Exploration of Information Privacy in Digital Ecosystems

Cumulative dissertation with the aim of achieving a doctoral degree

at the Faculty of Mathematics, Informatics, and Natural Sciences

Department of Informatics

Universität Hamburg

submitted by

Christian Kurtz

2022

Hamburg

Date of disputation

13 . 07 . 2022

Evaluators

First Evaluator: Prof. Dr. Tilo Böhmann

Second Evaluator: Prof. Dr. Paul Drews

Third Evaluator: Prof. Dr. Ali Sunyaev

Abstract

Motivation

Digital interaction has shifted from dyadic relationships between individuals and providers towards digital ecosystems that involve multiple actors, such as platform providers, service providers and third parties. All these actors gain access to data. This access can imply personal data creation, collection or sharing that is to some extent opaque for actors outside an organization and may not be expected, appropriate, or even legally permitted. The research gap exists on the movement, the processing, and the life cycle of personal data once it has been released by an individual. The lack of transparency concerning the inner workings of such digital ecosystems, coupled to their accompanying characteristics of complexity, emergences and dynamics, leads to the difficulty of articulating existing challenges and problems for information privacy. Thus, this dissertation uses the concept of digital ecosystems to study, in an exploratory manner, the new forms of socio-technical configurations processing personal data. For this, the dissertation moves beyond traditional approaches in the Information Systems (IS) discipline. Instead, it adopts a systemic perspective to address the research goals of understanding novel privacy-critical practices and proposing approaches to advance privacy in digital ecosystems. In this regard, the research questions address (1) the problems for privacy in digital ecosystems, (2) the creation of transparency, (3) the understanding of privacy-critical practices from a multi-actor and actor-centered perspective, and (4) the advancement of privacy in digital ecosystems.

Research Design

This cumulative dissertation adopts a highly explorative approach. The exploration refers to both the research field and to a novel mode of interdisciplinary collaboration. In this regard, an iterative and agile procedure paved the way for the dynamic development of knowledge regarding privacy in digital ecosystems. The research strategy employs both paradigms commonly used in the IS field: the design science paradigm and the behavioral science paradigm. This is supplemented by interdisciplinary research with the fields of law and ethics. In addition, disciplinary collaborations within the IS field made use of the dissertation's diverse connecting points into other research contexts.

Questionable or even negative phenomena resulting from organizational actions are difficult to study because perpetrators are reluctant to admit their existence. This dissertation studies 46 information privacy scandals published in the news, along with another ecosystem case. The cases provide the basis for the analysis of 1,330 documents (e.g., news articles, privacy policies, and party websites) in context of this dissertation. In this regard, qualitative methods are applied in the form of case studies, literature reviews, interdisciplinary assessments, archetype building, and parts of Design Science Research (DSR) and Value Sensitive Design (VSD).

Findings

The findings divide into two parts. The first addresses the creation of transparency and attempts to understand problems and practices affecting privacy in digital ecosystems. The second part includes approaches to advancing privacy in digital ecosystems.

Works on transparency and the understanding of ecosystems in relation to privacy are scarce. The investigation of eBay's complex ecosystem provides an exemplary benchmark of 906 involved partners and 132.3 hours needed to read related privacy policies. These numbers show the size of a single ecosystem and demonstrate how long it would potentially take for an individual to receive all information necessary to provide consent. In this dissertation, the analysis, illustration, and modelling of other ecosystems enabled a better understanding of privacy-critical practices. On the one hand, privacy scandals and related data flow and data processing steps in service ecosystems are represented in cross-impact matrices and illustrations. On the other, by building on disciplinary collaboration, architectural views enable decomposing data ecosystems to be seen in related illustrations that create different insights. In detail, privacy problems do not only exist between the user whose privacy is at stake and another actor but also between interacting actors in digital ecosystems, whose engagements affect the user's privacy. In this context, users are also affected by the actions of other users due to the interconnectivity inherent to digital ecosystems. In this regard, different archetypes characterize which organizational actor configurations can be critical to privacy. The reasons for this are wide-ranging.

This dissertation reveals that on the micro-level of an organization, crucial decisions regarding socio-technical components are made with ecosystem-wide privacy effects. This can result from a decision that carelessly integrates third-party code by a developer. Equally, privacy may also compete intraorganizational with other goals such as efficiency. On an ecosystem's macro-level, the involved actors in ecosystems may have information privacy understandings that are not always congruent, partially explicable due to the existence of interests that hinder or are opposed to privacy. Involved actors in digital ecosystems serve diverse aims and interests, and thus their activities are not necessarily related to the service's value proposition.

Consequently, this causes the user's created and shared personal data, intended for usage in the context of service provision, to be diffused into other service contexts and used for totally different reasons. In the vastness of ecosystems, this can create rebounding effects with unanticipated adverse effects for users. The findings of this dissertation reveal that Big Tech companies in particular make use of their involvement in diverse service systems. They proliferate in digital interaction with the user, as platform providers, service providers or third parties. These connections into diverse service contexts create a comprehensive ecosystem-connecting mechanism for accumulating personal data as involvement in digital interaction leads to personal data access. In consequence, Big Tech companies can decouple the data from the original value proposition and in the next step utilize them in other service contexts.

The second part of the findings proposes approaches to advance privacy in digital ecosystems. This dissertation shows that platform providers have a very influential role in designing the boundary resources of the platform and can manifest their perceptions throughout the platform ecosystem in ways that have implications for users, service providers and third parties. This can have detrimental effects on privacy. At the same time, it creates an opportunity, because this influence on ecosystems goes hand in hand with the possibility of advancing privacy. Thus, platform providers can be crucial actors in enhancing personal data protection in platform ecosystems.

In addition, design knowledge is developed to advance privacy. The design goals can improve the existing form of consent in digital ecosystems. Here, the reasonableness of the amount of time required to give informed consent is an important aspect to address by organizations and regulators. Finally, the knowledge created in another disciplinary research context addresses privacy-sensitive partnering and the limitation of data usage regarding the value proposition.

Research, Regulatory, and Practical Contributions

This dissertation makes research, regulatory and practical contributions that cover a broad spectrum due to the exploratory nature of this work.

The research contributions of this dissertation move beyond longstanding approaches and levels of analysis of privacy research in the IS field and adopt a systemic perspective to study privacy in digital ecosystems. This approach allows the contribution of diverse findings while considering actor-centered and multi-actor perspectives. The phenomena of diffusion and rebounding effects are identified across the data lifecycle and explained. The contributions of this dissertation fathom the currently prevailing practices related to privacy. These contributions take into account the multitude of actors across whom the steps of data creation, collection, and sharing in digital ecosystems are distributed.

In context of service research, the insights on privacy contribute to the understanding of value, value co-destruction, the connection to value propositions, and institutional arrangements in service ecosystems. With regard to data ecosystem research, this dissertation is one of the first works that addresses privacy and contributes knowledge concerning actors who have multiple roles. In terms of platform research, the boundary resource composition is described that allows different disciplines - in this case, the information systems, legal and ethical disciplines - to express their knowledge and foster fruitful discourses regarding privacy, actor's power and the application of existing data protection regulations.

Over and above the theoretical contributions, this dissertation provides three regulatory contributions that result from the intense interdisciplinary collaboration with the legal field. The first contribution reflects the design goals with the requirements for consent according to the General Data Protection Regulation (GDPR). Requirements defined in the GDPR do not yet cover the reasonableness of the amount of time required by users to be informed about data processing and thus provide consent. Two approaches are specified identifying how to deal with this. The second contribution highlights boundary resources for a data-protective regulation of platform ecosystems and the converse effects of boundary resources on regulations when applied and designed in a privacy-sensitive manner. This contribution has also been forwarded to the European Commission's relevant service to be considered in the GDPR's repeating evaluations. The third contribution reflects the GDPR's suitability to regulate data accumulation across service contexts and related rebound effects by Big Tech companies. Here, the isolated view on a single processing operation and the related juridical role according to the GDPR contrasts with the identified repeating practices including numerous data processing operations in diverse roles across service contexts. The results indicate that a new actor perspective and interpretation are needed for the GDPR to cope with companies' accumulation and rebound practices, especially for those of Big Tech companies.

In addition, this dissertation has practical implications for platform and service providers. Platform providers gain insights about why it is important to pay more attention to the complex and continuous effort to balance generativity, freedoms for services providers and included third parties, and individuals' information privacy. In addition, sweet spots are described that identify where to modify a platform ecosystem. In the case of service providers, it is important to differentiate a service provider's intentional or unintentional involvement in privacy-critical practices. In the case of unintentionality, providers can use the insights of this dissertation to ensure that the data processing operations of involved actors are mainly attributed to value proposition provision. Finally, the application of the architectural meta-model for data ecosystems could offer a fruitful starting point to deal with the complex and dynamic settings of partner involvement and related data processing operations.

Limitations

The limitations of this dissertation are divided into two categories: those that concern the results and those that concern the methodology.

The research results provide a very wide range of findings due to the exploratory research design of this dissertation. However, not all of them could be further developed and deepened. Furthermore, ecosystems are dynamic, which can lead to problems regarding the long-term accuracy of results. Nevertheless, the contributions of this dissertation are generally valid and remain unaffected. In addition, this dissertation considers the GDPR as the primary legal source of regulation. The potential difficulties of adopting this attitude are offset by acknowledging that GDPR is central to data protection and also applies to companies outside the European Union.

Methodological limitations include those that arise from the specific application of qualitative methods. Personal bias is minimized by involving multiple researchers in data collection and analysis, and by considering reliability measures.

Future Research

This dissertation identifies promising avenues for further research in the IS field regarding privacy in service ecosystems, platforms and data ecosystems. In future research, the IS field could develop a new understanding of information privacy. Thus, a shift from a definition only oriented on the individual in regard to controlling or restricting information towards an ecosystem-oriented definition of information privacy as personal data processing (in the context of the interests of the person to whom the data belongs) would be a prudent way forward. Such a definition would take into account the possibility that the actors involved in an ecosystem could have different, even conflicting, interests. Thus, this understanding could pave the way for research to understand how interests and values are currently considered. In addition, it would become possible to address the questions of how interests are actually balanced from a legal and ethical perspective and on the micro- and macro-levels of ecosystems.

In service research, a further investigation of actors in service interactions that do not limit personal data use in service systems is important. Studying the situations in which actors take multiple roles, or data practices repeat across service contexts, may be fruitful. The creation of transparency of the inner workings of service ecosystems should therefore be further considered. Modeling ecosystems with architectures could offer substantial contributions to this endeavor. In platform research, studies on boundary resources could consider how platform providers can design data access to limit privacy-critical practices. Research could address how to better realize the platform policy technically or how to improve app reviews. At the same time, the development of entirely new boundary resources may prove relevant. Future data ecosystem research could address how other companies use different roles to accumulate data. Since data is the fundamental resource of data ecosystems, the research focus on privacy seems promising.

Kurzfassung

Problemstellung und Ziel der Arbeit

Die digitale Interaktion hat sich von dyadischen Beziehungen zwischen Einzelpersonen und Anbietern[1] hin zu digitalen Ökosystemen verlagert, in denen eine Vielzahl von Akteuren wie Plattformanbieter, Dienstleister oder Drittparteien involviert sind - all diese Akteure erhalten Zugang zu Daten. Jener Zugriff kann hierbei die Erstellung, Sammlung oder Weitergabe personenbezogener Daten beinhalten, die für Akteure außerhalb einer Organisation in gewissem Maße undurchsichtig sind, möglicherweise nicht erwartet werden, nicht angemessen oder gar gesetzlich verboten sind. In diesem Kontext besteht eine Forschungslücke mit Blick auf den Fluss, die Verarbeitung sowie den Lebenszyklus von personenbezogenen Daten, sobald diese vom Individuum geteilt werden. Speziell die mangelnde Transparenz der inneren Vorgänge in digitalen Ökosystemen in Kombination mit den Merkmalen der Komplexität und der Dynamik führen zu Erschwernissen, existierende Herausforderungen in Hinblick auf Privatheit[2] präzise zu formulieren.

In der vorliegenden Dissertation wird das Konzept der digitalen Ökosysteme verwendet, um jene neuartigen Formen sozio-technischer Konfigurationen, in denen personenbezogene Daten verarbeitet werden, explorativ zu untersuchen. Damit geht diese Dissertation über die traditionellen und bisher angewandten Ansätze in der IS-Disziplin hinaus und nimmt stattdessen eine systemische Perspektive ein, um dem gesetzten Forschungsziel gerecht zu werden, ein Verständnis hinsichtlich neuartiger privatheitskritischer Praktiken zu entwickeln sowie darauf aufbauend Ansätze zur Förderung von Privatheit in digitalen Ökosystemen vorzuschlagen. In diesem Zusammenhang adressieren die Forschungsfragen dieser Dissertation die (1) Probleme für Privatheit in digitalen Ökosystemen, (2) die Schaffung von Transparenz, (3) das Verständnis privatheitskritischer Praktiken unter Berücksichtigung einer akteurszentrierten und -übergreifenden Perspektive sowie (4) die Förderung von Privatheit in digitalen Ökosystemen.

[1] Es wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

[2] In der deutschsprachigen Kurzfassung dieser Dissertation wird „Privacy" als „Privatheit" übersetzt. Dieser Begriff ist im Vergleich zum Begriff der „Privatsphäre" weniger mit einer räumlichen Konnotation beladen (Lindner, 2014).

Forschungsdesign und -methodik

Die vorliegende kumulative Dissertation basiert auf einem stark explorativen Ansatz. Hierbei bezieht sich die Exploration sowohl auf das Forschungsfeld an sich als auch auf eine neuartige Form der interdisziplinären Zusammenarbeit. Das hierbei herangezogene iterative und agile Vorgehen eröffnet den Raum für eine dynamische Entwicklung von Wissen in Bezug auf Privatheit in Ökosystemen. In der Forschungsstrategie findet dabei eine Berücksichtigung der beiden im IS-Bereich üblichen Paradigmen in Form des Design Science- sowie des Behavioral Science-Paradigmas statt. Interdisziplinäre und disziplinäre Kooperationen ergänzen diesen Ansatz. Die interdisziplinären Kooperationen beziehen in diesem Zusammenhang einerseits die rechtliche Perspektive und andererseits die ethische Perspektive mit ein, während die disziplinären Kooperationen in den jeweiligen Forschungskontexten auf den vielfältigen Anknüpfungspunkten dieser Dissertation aufbauen können.

Grundsätzlich sind fragwürdige oder negative Phänomene, die sich aus organisationalen Handlungen ergeben, oftmals nur schwer zu untersuchen, da die Verursacher ihre Existenz ungern eingestehen. Um diesem Umstand möglichst gerecht werden zu können, werden 46 in den Nachrichten veröffentlichte Privatheit-Skandale sowie ein weiterer Ökosystem-Fall untersucht. Jene Fälle bilden die wesentliche Grundlage für die Analyse von 1.330 Dokumenten (u. a. Datenschutzerklärungen, Nachrichtenartikel und Webseiten) im Rahmen der Dissertation. In jenem Zusammenhang findet eine Anwendung qualitativer Methoden in Form von Fallstudien, Literaturrecherchen, interdisziplinären Beurteilungen, Archetypenbildung sowie Bestandteile der Design Science Research (DSR) und des Value Sensitive Design (VSD) statt.

Forschungsergebnisse

Die Ergebnisse der Arbeit sind in zwei Teile gegliedert: Der erste Teil befasst sich mit der Entwicklung von Transparenz und Verständnis in Bezug auf privatheitsrelevante Probleme und Praktiken in digitalen Ökosystemen. Der zweite Teil umfasst darauf aufbauend Ansätze zur Förderung von Privatheit in digitalen Ökosystemen.

Transparenz über Ökosysteme in Bezug zu Privatheit existiert bisher lediglich in sehr geringem Maße. Vor diesem Hintergrund zeigt eine exemplarische Untersuchung des komplexen Ökosystems von eBay im Rahmen der Dissertation eine Anzahl von 906 Unternehmen auf, die an Datenverarbeitungsprozessen beteiligt sind. Für Nutzer ergibt sich hieraus in Konsequenz eine Lesedauer der entsprechenden Datenschutzerklärungen in Höhe von 132,3 Stunden. Diese Zahlen verdeutlichen das Ausmaß eines einzigen Ökosystems und die damit einhergehende zeitlich aufzuwendende Dauer, die eine Einzelperson benötigt, um eine informierte Einwilligung zur Datenverarbeitung zu erteilen.

Zur Schaffung von Verständnissen hinsichtlich privatheitskritischer Praktiken umfasst die vorliegende Dissertation die Analyse, Darstellung sowie Modellierung weiterer Ökosysteme. So werden einerseits Datenschutzskandale und die damit verbundenen Datenfluss- und Datenverarbeitungsschritte in Dienstleistungsökosystemen in Wechselwirkungsmatrizen sowie Abbildungen veranschaulicht. Andererseits ermöglichen auf Basis wissenschaftlicher Kollaborationen fußende architekturelle Ansichten die granulare Zerlegung von Datenökosystemen in ihre einzelnen Bestandteile.

Besonders hervorzuheben ist die Erkenntnis, dass im Einzelnen Problematiken hinsichtlich Privatheit nicht nur zwischen dem Nutzenden, um dessen Privatheit es geht, sowie einem weiteren Akteur existieren. Es bestehen gleichsam Konflikte zwischen weiteren Akteuren in digitalen Ökosystemen, die Auswirkungen auf die Privatheit des Nutzers haben. Darüber hinaus sind aufgrund der Vernetzung in Ökosystemen Nutzer zudem von den Handlungen anderer Nutzer betroffen. In diesem Kontext charakterisieren Archetypen die organisationalen Akteurskonfigurationen, welche negativ auf Privatheit wirken - die Gründe dafür sind vielfältig.

Vor diesem Hintergrund identifiziert die Dissertation, dass auf der Mikroebene einer Organisation wesentliche Entscheidungen bezüglich sozio-technischer Komponenten getroffen werden, die sich auf das gesamte Ökosystem auswirken. Dies kann zum einen aus einer Entscheidung im Zusammenhang mit der Third-Party-Code-Integration seitens eines Entwicklers ohne weitere Bedenken resultieren. Andererseits kann Privatheit auch intraorganisational in Konflikt zu anderen Zielen wie beispielsweise Effizienz stehen. Auf der Makroebene eines Ökosystems liegt ein Hauptgrund darin, dass die beteiligten Akteure in Ökosystemen über Verständnisse von Privatheit verfügen, die nicht immer kongruent zueinander sind – auch aufgrund der Existenz von Interessen, die Privatheit behindern oder ihr entgegenstehen. So verfolgen beteiligte Akteure in Ökosystemen Ziele und Interessen, die nicht zwingend nur dem Nutzenversprechen eines Dienstes zuzuordnen sind.

Folglich schafft dies den Raum dafür, dass die von Nutzern erstellten und geteilten personenbezogenen Daten, welche für die Anwendung im Rahmen der Erbringung von Dienstleistungen bestimmt waren, in andere Dienstleistungskontexte verlagert und für weitere Zwecke verwendet werden können. In den Weiten der Ökosysteme kann dies zu Rückpralleffekten mit unvorhergesehenen, nachteiligen Auswirkungen für Nutzer führen. In diesem Zusammenhang verdeutlichen die Ergebnisse der Dissertation, dass insbesondere Big-Tech-Unternehmen von ihrer Einbindung in diverse Dienstleistungssysteme Gebrauch machen. Sie treten in der digitalen Interaktion gegenüber den Nutzern als Plattformanbieter, Dienstleister oder Drittparteien auf. Jene Einbindung in diverse

Dienstleistungskontexte schafft einen hohen ökosystemverbindenden Mechanismus zur Akkumulation personenbezogener Daten, da Einbindung zum Zugriff auf personenbezogene Daten führt. Folglich können Big-Tech-Unternehmen die Daten vom ursprünglichen Nutzenversprechen entkoppeln, um die personenbezogenen Daten im nächsten Schritt in anderen Dienstleistungskontexten verwenden zu können.

Im zweiten Teil des Ergebnis-Kapitels werden Ansätze zur Förderung von Privatheit in digitalen Ökosystemen vorgeschlagen. Die Dissertation zeigt auf, dass Plattformanbieter eine einflussreiche Rolle bei der Gestaltung der Grenzressourcen der Plattform innehaben sowie ihre Auffassungen im gesamten Plattform-Ökosystem manifestieren können - mit Auswirkungen auf Nutzer, Dienstleister sowie Drittparteien. Dieser Aspekt kann sich nachteilig auf Privatheit auswirken. Gleichzeitig ergibt sich daraus eine Chance, da jene Einflussnahme mit der Möglichkeit einhergeht, Privatheit in Ökosystemen auszuformen. So können Plattformanbieter entscheidende Akteure zur Verbesserung von Datenschutz und Privatheit innerhalb von Plattform-Ökosystemen darstellen.

Darüber hinaus beinhaltet diese Dissertation Gestaltungswissen zur Förderung von Privatheit. Die Gestaltungsziele können hierbei die existierende Form der Einwilligung in digitalen Ökosystemen verbessern. In diesem Zusammenhang stellt die Zumutbarkeit hinsichtlich des Zeitaufwands, der für die Erteilung der Einwilligung benötigt wird, einen wesentlichen Aspekt dar, der von Organisationen und Regulierungsbehörden berücksichtigt werden sollte. Darüber hinaus wurde in einer weiteren disziplinären Kollaboration nutzbringendes Wissen hinsichtlich der Zusammenarbeit von Akteuren in Ökosystemen geschaffen, welches die Begrenzung der Datenverwendung innerhalb der Dienste in den Blick nimmt.

Beiträge für Forschung, Regulatorik und Praxis

Die vorliegende Dissertation leistet theoretische, regulatorische sowie praktische Beiträge, welche aufgrund des explorativen Charakters insgesamt ein breites Spektrum umfassen.

Die theoretischen Beiträge dieser Dissertation gehen über die langjährigen Ansätze und Analyseebenen der Privatheitsforschung im IS-Feld hinaus und berücksichtigen eine systemische Perspektive zur Untersuchung von Privatheit in digitalen Ökosystemen. Jener Ansatz ermöglicht es, vielfältige Erkenntnisse unter Berücksichtigung einer akteurszentrierten und -übergreifenden Perspektive zu gewinnen. Dabei werden neuartige Phänomene wie die Diffusion oder Rückpralleffekte identifiziert und eingeführt. Ferner ergründen die Beiträge der Dissertation die gegenwärtig vorherrschenden Praktiken in Bezug auf Privatheit. Dieser Ansatz trägt der Vielzahl von Akteuren Rechnung, über welche die

Schritte der Datenerstellung, -sammlung, und -weitergabe in digitalen Ökosystemen verteilt sein können.

Weiterführend leistet diese Dissertation einen Beitrag zur Dienstleistungsforschung. Neben den Ergänzungen zum Werteverständnis tragen die Forschungsbeiträge in Bezug zu Privatheit zum Wissen über Wertedestruktion, Nutzenversprechen sowie den in Dienstleistungsökosystemen existierenden, institutionellen Vereinbarungen bei. Hinsichtlich der Forschung im Themenfeld der Datenökosysteme ist die Dissertation hierbei eine der ersten Arbeiten, die sich mit Privatheit befasst sowie Erkenntnisse über Akteure liefert, die eine Vielzahl von Rollen einnehmen. In Bezug zur Plattformforschung wird die Zusammensetzung der Grenzressourcen dargelegt. Dies ermöglicht es, verschiedenen Disziplinen - in diesem Fall der IS-Disziplin, der Rechtswissenschaft und der Ethik - ihr Wissen zum Ausdruck zu bringen und Diskurse über Privatheit, die Macht von Akteuren sowie die Anwendung bestehender Datenschutzgesetze zu führen.

Neben den theoretischen Beiträgen bringt die Dissertation drei regulatorische Beiträge hervor, die aus der intensiven interdisziplinären Zusammenarbeit mit dem rechtlichen Feld resultieren. Der erste Beitrag reflektiert die entwickelten Gestaltungsziele in Hinblick auf die Anforderungen an eine wirksame Einwilligung gemäß der Datenschutzgrundverordnung (DSGVO). Insbesondere das Gestaltungsziel der Zumutbarkeit des Zeitaufwandes, welcher für eine informierte Einwilligung notwendig ist, stimmt mit keiner der in der DSGVO genannten Anforderungen überein. Resultierend werden zwei Ansätze genannt, welche geeignet erscheinen, diesen Aspekt zu adressieren.

Der zweite Teil schafft ein bislang nicht existierendes Verständnis von Grenzressourcen für eine datenschutzfreundliche Regulierung von Plattform-Ökosystemen und deren umgekehrten Auswirkungen auf die Regulierung bei privatheitsorientierter Anwendung und Gestaltung. Jener Beitrag wurde auch an die zuständige Dienststelle der Europäischen Kommission weitergeleitet, damit dieser bei den wiederholten Evaluationen der DSGVO berücksichtigt werden kann.

Der dritte Teil setzt sich mit dem Regulationspotential der DSGVO auseinander, insbesondere in Bezug zur Datenakkumulation über differente Dienstleistungskontexte hinweg sowie der damit verbundenen Rückpralleffekte speziell durch Big-Tech-Unternehmen. An dieser Stelle steht die isolierte Betrachtung eines einzelnen Verarbeitungsvorgangs und der damit einhergehenden rechtlichen Rolle gemäß der DSGVO den identifizierten Praktiken entgegen, die zahlreiche Datenverarbeitungsvorgänge in unterschiedlichen Rollen in verschiedenen Dienstleistungskontexten beinhalten. Hieraus resultiert als Beitrag, dass eine neue Akteursperspektive und -auslegung für die DSGVO erforderlich ist, um die Akkumulations- und Rückprallpraktiken von Unternehmen, vor allem die von Big-Tech-Unternehmen, adressieren zu können.

Darüber hinaus beinhaltet die Dissertation praktische Implikationen, die sich an Plattform- und Dienstanbieter richten. Plattformanbieter erhalten Einblicke, aus welchen Gründen es relevant ist, dem komplexen und kontinuierlichen Unterfangen zwischen Generativität, Freiheiten für Dienstleister und Drittparteien sowie der Privatheit von Individuen größere Aufmerksamkeit zu schenken. Ferner werden Anknüpfungspunkte erläutert, an denen Plattform-Ökosysteme privatsheitsfördernd verändert werden können. Bei Dienstleistern ist es hierbei wesentlich, zwischen der beabsichtigten und unbeabsichtigten Beteiligung an datenschutzkritischen Praktiken zu differenzieren. Im letzteren Fall können Dienstleister die Erkenntnisse der Dissertation nutzen, indem sie sicherstellen, dass die Datenverarbeitungsvorgänge der beteiligten Akteure in erster Linie auf die Bereitstellung des Nutzenversprechens zurückzuführen sind. Darüber hinaus kann die Anwendung des architekturellen Meta-Modells für Datenökosysteme vorteilhaft sein, um die komplexen und dynamischen Partnergeflechte und einhergehenden Datenverarbeitungsvorgänge besser handzuhaben.

Limitationen

Die Limitationen der vorliegenden Dissertation untergliedern sich in Aspekte bezüglich der Ergebnisse sowie der Methodik. Die Forschungsergebnisse umfassen ein sehr breites Spektrum an Erkenntnissen, die auf die explorative Vorgehensweise der Dissertation zurückzuführen sind. Nicht alle dieser vielfältigen Ergebnisse wurden jedoch weiterentwickelt oder vertieft. Darüber hinaus ist zu beachten, dass Ökosysteme dynamisch sind. Dies kann zu Beeinträchtigungen hinsichtlich der langfristigen Genauigkeit der Ergebnisse führen. Nichtsdestotrotz bleiben die Erkenntnisse und Beiträge dieser Dissertation aufgrund ihrer übergeordneten Aussagekraft davon unberührt. Zudem wurde die DSGVO als primäre Datenschutzregelung herangezogen. Jene ist eine der zentralsten Regulationen für den Datenschutz weltweit und ebenfalls anwendbar auf Unternehmen außerhalb der europäischen Union.

Weiterhin finden sich in dieser Dissertation methodische Einschränkungen, die sich aus der spezifischen Anwendung qualitativer Methoden ergeben. Durch die Beteiligung mehrerer Forscher an der Datenerhebung und -analyse sowie durch Berücksichtigung von Reliabilitätsmaßen wurden einhergehende Einschränkungen jedoch reduziert.

Ausblick

Die vorliegende Dissertation zeigt vielversprechende Wege für die weitere Forschung von Privatheit im IS-Feld sowie hinsichtlich der Erforschung von Dienstleistungs-, Plattform- und Daten-Ökosysteme auf.

In der künftigen Forschung im IS-Feld kann ein neues Verständnis von Privatheit entstehen. Eine Verlagerung von einer rein am Individuum orientierten Definition und dessen Möglichkeiten der

Kontrolle oder Einschränkung von Informationen hin zu einer ökosystemorientierten Definition des Datenschutzes als Verarbeitung personenbezogener Daten entsprechend den Interessen des Individuums, wäre ein geeigneter Ansatz für die Zukunft. Denn eine solche Definition würde berücksichtigen, dass die am Ökosystem beteiligten Akteure unterschiedliche, gar gegensätzliche Interessen aufweisen. Folglich könnte jener Ansatz den Pfad für Untersuchungen ebnen, wie Interessen und Werte derzeit Einzug in Ökosysteme halten und gewichtet werden. Darüber hinaus könnte sich den Fragestellungen gewidmet werden, wie Interessen aus rechtlicher und ethischer Sicht sowie auf der Mikro- und Makroebene von Ökosystemen auszutarieren sind.

Darüber hinaus kann die Dienstleistungsforschung den Fokus stärker auf Akteure in Dienstleistungsinteraktionen legen, welche die Nutzung personenbezogener und -beziehbarer Daten nicht auf Dienstleistungssysteme beschränken. Die Untersuchungen von Akteuren, welche multiple Rollen einnehmen oder aber von Datenpraktiken, die über differente Dienstleistungskontexte hinweg existieren, erscheint in diesem Zusammenhang perspektivisch ergiebig. In diesem Kontext sollte die Schaffung von Transparenz über Abläufe in Dienstleistungsökosystemen intensiviert werden. Die Modellierung von Ökosystemen mit Architekturen kann dabei wesentliche Beiträge leisten. In der Plattformforschung könnte zudem die privatsheitsfördernde Ausgestaltung der Grenzressourcen, die einen Datenzugriff in Plattformökosystemen ermöglichen, adressiert werden. Dies kann beinhalten, in welcher Weise eine technisch wirksamere Umsetzung von Plattformbestimmungen stattfinden kann oder aber welche Möglichkeiten hinsichtlich der Optimierung von App-Review-Prozesse bestehen. Gleichzeitig kann die Entwicklung gänzlich neuer Grenzressourcen von Bedeutsamkeit sein. Zukünftige Datenökosystem-Forschung sollte weitere Unternehmen in den Blick nehmen, die differente Rollen zur Datenakkumulation nutzen. Da Daten die grundlegende Ressource von Datenökosystemen darstellen, erscheint eine intensivere wissenschaftliche Auseinandersetzung mit Privatheit zukunftsträchtig.

Table of Contents

The articles' sections are not integrated in this table of content.

List of Figures

The articles' figures are not integrated in this list.

List of Tables

The articles' tables are not integrated in this list.

List of Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
DG	Design Goal
DSGVO	Datenschutzgrundverordnung
DSR	Design Science Research
ECJ	European Court of Justice
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
IS	Information Systems
PbD	Privacy by Design
RG	Research Goal
RQ	Research Question
SDK	Software Development Kit
VSD	Value Sensitive Design

The articles' abbreviations are not integrated in this list.

1 Introduction

The following section is divided into the motivation and problem statement, the research goal and research questions, and the thesis outline.

1.1 Motivation and Problem Statement

The value for humans of information privacy[3] is attributed to its great importance for democracy (Westin 1967) and its necessity for full human flourishing (Tavani 2008). This position is emphasized by the Data Ethics Commission instituted by the Germany's Federal Government. Their final report published in 2019 emphasizes that the protection of privacy is closely linked to the protection of human dignity and self-determination (Ethics Commission 2019). However, digital technologies occur in all spheres of life and affect information privacy. Given the present data deluge resulting from billions of people using IS extensively, personal data are created almost everywhere (Nissenbaum 2019; Zuboff 2015).

Digitized and smart services have become a central element of this interconnected world. Processing data relating to an individual is often essential for the provision of smart services that reflect that individual user's preferences and usage contexts (e.g., locations) (Peters et al. 2016). Data are used for diverse purposes. For example, in mobile applications, data are necessary for application performance management, security, monetization or service provision (Binns et al. 2018; Gopal et al. 2018; Razaghpanah et al. 2018). Diverse actors become involved in these previously described purposes and lead users and providers no longer to interact in a dyadic relationship but rather in co-creative networks that include service providers, platform providers and third parties. Thus, while service capability and digital user experiences improve with the involvement of specialized actors, the number of actors who process person-related data increases and user privacy can be affected. As a result, questions and challenges for information privacy emerge due to the novel use and sharing of personal data that is not expected, appropriate or even legally permitted.

In the IS field, an individual's ability to control the information they share with others dominates the understanding of information privacy (Acquisti et al. 2015; Bélanger and Xu 2015; Dinev et al. 2015; Kallemeyn and Chipidza 2021; Karwatzki et al. 2017; Smith et al. 2011). Here, the assumptions of

[3] In this dissertation, the word "privacy" is used to mean "information privacy".

unidirectional personal data flows and bilateral relationships underlie existing models (Benson et al. 2015; Conger et al. 2013; Karwatzki et al. 2017). However, the overwhelming frequency with which personal data is created, used, and shared between actors raises new questions about these privacy understandings and views (Nissenbaum 2019; Tavani 2008). The limitations of these conceptualizations of privacy as restricting others' access or controlling personal data led Nissenbaum (2004) to develop a new normative framework of privacy as *Contextual Integrity*. Recently, Nissenbaum also recognized that "[t]here was a time when [she] believed that privacy could be well enough protected atomically, that is, by astutely monitoring and characterizing data flows in terms of contextual parameters and divergences from norms and expectations, case by case. Although there certainly will be occasions when this approach successfully can identify sources of privacy breach, as a general approach, it is overwhelmed by the scale of the shadow data universe" (Nissenbaum 2019, p. 255). Thus, different information privacy concepts – including newer ones – struggle to cope with hidden data processing operations that exist on a systemic level. In this regard, systemic means the personal data creation, collection, and use of diverse actors which are involved in digital interaction. A research gap exists on the movement and life cycle of personal data once it has been released by an individual (Conger et al. 2013; Spiekermann and Novotny 2015). This gap motivates to use novel perspectives to articulate and address privacy-critical aspects.

In the IS field, research on ecosystems gained increasing attention to study the new forms of networks, with their related emergences and dynamics, from a systemic point of view. Digital ecosystems can be divided into different types, including service ecosystems (Vargo and Akaka 2012; Vargo et al. 2017; Vargo et al. 2015), data ecosystems (Aaen et al. 2021; Oliveira et al. 2019; Oliveira et al. 2018), platform ecosystems (Constantinides et al. 2018; Hein et al. 2019; Parker et al. 2017), business ecosystems (Moore 1996) and software ecosystems (Manikas 2016). The consideration of a specific ecosystem type depends on the research context. While, for example, some studies have used the ecosystem lens to explain digital transformation phenomena (Nischak et al. 2017; Vial 2019), there is a lack of research that studies personal data practices and information privacy.

1.2 Research Goal and Research Questions

This dissertation uses the lens of digital ecosystems to understand novel personal-data processing operations and upcoming problems for information privacy. Thus, the overarching research goal (RG) of this dissertation is:

> **RG: Understanding privacy-critical practices and proposing approaches to advance information privacy in digital ecosystems.**

The dissertation builds on a highly explorative approach. Exploratively refers both to the research field and to a novel mode of interdisciplinary collaboration. In the course of this dissertation, the newly created insights of one iteration determined the next iteration. Besides the IS discipline, the legal and ethical disciplines and their related perspectives and understandings were involved in addressing the research goal. The insights generated by this dissertation could be incorporated into other research contexts in the IS field, and revelations from these collaborations are integrated into this dissertation. All three facets had a very strong influence on this dissertation.

In the following paragraphs, the guiding research questions (RQs) are specified and briefly described.

RQ-1: What problems exist for privacy in digital ecosystems?

RQ-1 aims to identify what problems that are critical for information privacy exist in digital ecosystems. One central challenge for this dissertation is that negative phenomena arising from the actions of organizational actors are often hard to investigate because perpetrators are reluctant to acknowledge their existence. Thus, this dissertation considers the call to explore privacy violations as well as factors and problems that lead to actors' practices (Bélanger and Xu 2015). To address this, a large part of this dissertation includes the study of privacy scandals that involve certain kinds of transgressions regarding information privacy that became known to others and are sufficiently serious to elicit a public response.

RQ-2: How to create transparency about privacy-critical practices in digital ecosystems?

This RQ addresses the need to create transparency about privacy-critical personal data flows and related practices. Transparency is usually equated with qualities such as openness, insight or clarity (Christensen and Cheney 2015). Transparency and observation are essential for normative dealing: observers (such as researchers, practitioners or regulators) seeking to judge whether practices exist as intended and what changes may be required in them, will be better able to do so when they have more access to the facts describing the practices (Ananny and Crawford 2018). The more such observers know about the system's inner workings, the better it can be governed, and actors can be held accountable (Ananny and Crawford 2018). Transparency can be expressed in many different ways and be more or less helpful for a goal; it is formed by information generation and provision (Florini 2007).

To address RQ-2, a cross-impact matrix is used, a quantitative determination of transparency regarding the privacy policies of a large-scale ecosystem is created, and privacy scandals in ecosystems are visualized. Insights generated by this dissertation are also integrated into a data ecosystem architecture meta-model and related instantiations in another research context.

RQ-3: What are multi-actor and actor-centered privacy-critical practices in digital ecosystems?

Two foci are considered in RQ-3. An actor-centered view addresses the practices of Big Tech companies that span personal data practices across different service contexts. This view contributes to understanding a single company's data ecosystem and its data accumulation that derives from its multi-role function in diverse service contexts. Meanwhile, a multi-actor focus helps to understand the conflicting practices that arise from the interaction of multiple actors in ecosystems. In this regard, different archetypes are identified that set the basis for further investigation of actor arrangements.

RQ-4: How can privacy be advanced in digital ecosystems?

The knowledge generated about the different privacy-critical problems and practices is considered in RQ-4 in order to propose different approaches to advance privacy in digital ecosystems. First, platform providers' boundary resource composition and the provider's accountability from a legal and ethical point of view have been identified as areas particularly suitable for advancing information privacy in platform ecosystems. Second, this dissertation contributes design knowledge. Seven design goals are developed for consent in large-scale ecosystems. In addition, design knowledge from another collaboration addresses the limitations of data usage when considering a service's value proposition.

1.3 Thesis Outline

The structure of this dissertation is illustrated in Table 1. After this introduction, section 2 provides the theoretical foundations of digital ecosystems and information privacy. Section 3 characterizes the overall research design and specifies the research strategy and applied methods. Section 4 summarizes the articles that are considered in this dissertation. The overall theoretical contributions are discussed in section 5, while section 6 describes the regulatory and practical contributions. Section 7 reflects the limitations of the research findings and the research design, while Section 8 identifies avenues for further research. The last sections contain the nine published articles. One article under review is attached in the Appendix.

Table 1. Dissertation Outline

1.	**Introduction**
2.	**Theoretical Foundations**
3.	**Research Design**
4.	**Articles**
5.	**Theoretical Contributions**
6.	**Regulatory and Practical Contributions**
7.	**Limitations**
8.	**Implications for Further Research**
9. – 17.	**Publications**
9.	Article No. 1: Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors
10.	Article No. 2: Towards a Framework for Information Privacy in Complex Service Ecosystems
11.	Article No. 3: The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems
12.	Article No. 4: Design Goals for Consent at Scale in Digital Service Ecosystems.
13.	Article No. 5: Conceptualizing Design Parameters of Online Neighborhood Social Networks
14.	Article No. 6: Value sensitive design and power in socio-technical ecosystems.
15.	Article No. 7: Unraveling Privacy Concerns in Complex Data Ecosystems with Architectural Thinking
16.	Article No. 8: Accountability of platform providers for unlawful personal data processing in their ecosystems–A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR
17.	Article No. 9: Exploring Archetypes of Value Co-Destructive Privacy Practices
Appendix	**Manuscript under review**
A	Article No. 10: Multi-Role Actors and Rebounding Effects in Data Ecosystems – Exploring Big Tech's Privacy Scandals and GDPR Limitations

2 Theoretical Foundations

In the following section, the theoretical foundations are laid down.[4] The last subsection combines the streams of digital ecosystems and information privacy.

2.1 Digital Ecosystems

'Digital ecosystem' is used as an umbrella term, as this dissertation make use of specific types of service, platform and data ecosystems. The ecosystem concept emerged in diverse research contexts as a lens to investigate the complex emerging nature of intertwined interactions between actors. All three types share a conceptual core containing at least three common characteristics (Constantinides et al. 2018; Gelhaar et al. 2021; Hein et al. 2019; Oliveira et al. 2019; Vargo and Akaka 2012).

First, the ecosystems consist of socio-technical configurations. Second, actors are connected by interactions that include exchanges. While the primary focus of this dissertation addresses personal data exchanges and related flows, ecosystems can comprise other exchanges, such as money exchanges. Third, in these socio-technical ecosystems, actors' artifacts and interactions are dynamic and subject to constant change. Focusing on a specific type of ecosystem provides the opportunity to spotlight different characteristics essential to its function. Thus, each ecosystem type enables a particular perspective from which to study and understand information privacy in digital ecosystems.

The service ecosystem perspective allows to examine value co-creation in self-contained and self-adjusting networks (Vargo and Akaka 2012) by considering institutional arrangements, i.e., the assemblages of rules or norms that guide value co-creation. A platform ecosystem perspective creates the opportunity to study the specific actor arrangement of individuals, platform providers and service providers, including third parties. Existing research already addresses how platform providers define the rules in platform ecosystems and implement related governance mechanisms to facilitate value-creating mechanisms between the other actor groups (Hein et al. 2019). Compared to the service and platform ecosystem perspective, the data ecosystem perspective can help address the consumption, production or provision of data by or among a loose set of interconnected actors where one actor performs one or more roles (Oliveira et al. 2019). This last-mentioned aspect is essential for studying the effect on privacy

[4] The theoretical foundations are based on the articles included in this dissertation. Thus, text components are included here that are similar or identical to components of the articles' foundation and background sections.

had by an actor who has multiple roles. The following subsections address the different ecosystem types and related research contexts in more detail.

2.1.1 Value Co-Creation and Co-Destruction in Service Ecosystems

According to service logic, actors co-create value through interaction (Vargo et al. 2008b). The configurations of people, technologies and other entities, joint resource integration and service exchange can be viewed on different levels of abstraction (Vargo and Lusch 2004; Vargo et al. 2008a). Service systems can be characterized as the value-creation in interactive configurations of mutual exchange (Vargo et al. 2008a). This view of service systems allows the investigation of resource integration among the aforementioned configurations (Vargo and Lusch 2010). Service ecosystems can be characterized as "relatively self-contained self-adjusting systems of resource-integrating actors connected by shared institutional logics and mutual value creation through service exchange" (Vargo and Lusch 2011; Vargo and Akaka 2012, p. 207). In this regard, different perspectives exist in the literature on delimit service systems and service ecosystems. In this dissertation, service systems are seen as a subset of service ecosystems. A service ecosystem perspective can be helpful to address value co-creation among multiple service systems, as is also described in the literature (Vargo and Akaka 2012; Vargo and Lusch 2010).

From service research, it is known that institutional arrangements guide value co-creation by defining acceptable behaviors and enabling and constraining social action (Vargo and Lusch 2016). Nevertheless, actors might have divergent perceptions of institutions and institutional arrangements (Kleinaltenkamp 2018; Plé and Demangeot 2020). The effects remain relatively occluded, as a prevailing assumption in service research is that actors share an understanding regarding institutions (Mustak and Plé 2020). This gap also exists for information privacy.

Research on value co-destruction has shown that value co-creation is an optimistic ideal that is not always achieved (Lintula et al. 2018; Prahalad and Ramaswamy 2004). Value co-destruction can appear in the interaction of co-creating actors, resulting in a decline of value for at least one actor involved (Lintula et al. 2017; Plé 2017; Plé and Chumpitaz Cáceres 2010; Vartiainen and Tuunanen 2016; Worthington and Durkin 2012). The reason is that one actor integrates or applies the resources in a manner that is not expected or appropriate (Lintula et al. 2017). Not all actions are visible or even comprehensible to customers, as service blueprints clarify (Sampson 2012). Actions and related effects can be intended or unintended (Plé and Chumpitaz Cáceres 2010). In a situation of intended co-destruction, one actor makes use of the available resources and tries to gain more benefit. In case that value co-destruction becomes public, this may result in customer loss, dissatisfaction or a negative image for the value co-destructive actor. Novel studies have investigated value co-destruction in service ecosystems, taking into account the investigation of value co-destruction in the business-to-business context (Pathak et al. 2020), undesirable effects in the sharing economy (Buhalis et al. 2020) and smart city ecosystems (Pellicano et al. 2018).

2.1.2 Platform Ecosystems and Boundary Resources

Platform ecosystems can be a fruitful resource for investigations of personal data practices that involve the actor configurations of individuals, platform providers and service providers that include third parties (Barros and Dumas 2006; Riedl et al. 2009b; Van Alstyne et al. 2016). Platform providers embody an intermediary actor in the arrangement of multi-actor data processing (Gawer and Cusumano 2015; Hein et al. 2019). Research on digital infrastructures emphasized that platforms providers increasingly interpose their platforms between individuals and service providers and orchestrate the mode of interaction (Riedl et al. 2009a; Van Alstyne et al. 2016). In this context, "a digital platform ecosystem comprises a platform owner that implements governance mechanisms to facilitate value-creating mechanisms on a digital platform between the platform owner and an ecosystem of autonomous complementors and consumers" (Hein et al. 2019, p. 90).

Platform providers facilitate a platform and the set of digital resources that make value-creating interactions possible by providing resources such as an operating system or an app store (Parker et al. 2016). Service provider apps offer functionality, service or content (Constantinides et al. 2018), which can be accessed by the user in the platform ecosystem (Ghazawneh and Henfridsson 2013). Platforms differ in their architecture, which affects the nature of module provision and platform governance. In closed platforms, the provider controls which modules can be accessed by controlling the distribution of modules, typically using app stores (Hein et al. 2019; Schreieck et al. 2016; Tiwana et al. 2010). Platform providers do not control this distribution in open platform architectures, thus leaving more freedom on how actors can interact via the platform (de Reuver et al. 2018; Tiwana et al. 2010). Hybrid architectures, in which platform providers control distribution channels while simultaneously making provisions for open distribution channels and interactions, also exist.

The interaction between service providers and the platforms has been central to platform boundary resource research (Constantinides et al. 2018; Tiwana et al. 2010). Platform providers enable external developers to contribute to the ecosystem by providing boundary resources (Constantinides et al. 2018; Tiwana et al. 2010; Tiwana et al. 2013). Designing and implementing boundary resources requires retaining control while allowing service providers to implement independent platform innovation (Eaton et al. 2015). Platform providers maintain balance by changing boundary resources over time.

Boundary resources can – but do not have to – emerge from a kind of negotiation process between the platform provider and the service providers that Eaton et al. (2015) describe as "tuning."

Boundary resources can contribute to diverse functions (Karhu et al. 2018). Examples of functions include resourcing or securing the platform (Ghazawneh and Henfridsson 2013). Platform resourcing can be defined as the mechanisms and tools by which the scope and the diversity of a platform are enhanced, such as software development kits (SDKs) or application programming interfaces (APIs) (Ghazawneh and Henfridsson 2013; Hagiu and Wright 2015; Van Alstyne et al. 2016). The function of securing the platform can include application review processes or mandatory developer agreements (Ghazawneh and Henfridsson 2013). To sum up, boundary resources can help to study platform providers' means to influence personal data processing operations in platform ecosystems.

2.1.3 Data Ecosystems

Data ecosystems is a novel concept that has emerged in the last years in the literature. Research on data ecosystems is still in its infancy and is perceived as "new and undertheori[z]ed" (Aaen et al. 2021, p. 3), especially regarding the theory, models and engineering (Oliveira et al. 2019). So far, no common agreement exists regarding the definition of this concept (Oliveira et al. 2019). Existing literature shows that data ecosystems can be characterized as "the cross-actor generation, processing, and use of data to create added value for all actors involved" (Gelhaar et al. 2021, p. 6114). In this regard, Oliveira et al. (2019) highlight (in a systematic study of data ecosystems) the "loose set of interacting actors that directly or indirectly consume, produce, or provide data and other related resources (e.g., software, services, and infrastructure). Each actor performs one or more roles and is connected to other actors through relationships, in such a way that actors by collaborating and competing with each other promote [d]ata [e]cosystems" (p. 604).

Aaen et al. (2021) investigated data ecosystems as they relate to the topic of information privacy. In this study, the authors contributed the knowledge that data reuse can undermine the legitimacy of data analytics initiatives relating to an ecosystem. However, other existing papers "are focused on some component or technology that reflects only a small fragment of the whole research area" (Oliveira et al. 2019, p. 590). Thus, there is a lack of research applying the data ecosystem perspective to different contexts, especially to study information privacy (Oliveira et al. 2019).

2.2 Information Privacy and Personal Data Protection

In the following subsection, the specifics concerning the development of information privacy, information privacy in the IS field and data protection by the GDPR are explained.

2.2.1 The Development of Information Privacy

Given the increased number of personal-data sharing and processing practices in modern societies, the "end of privacy" is thought by some to be at hand (Tavani 2008; Zuboff 2019). However, collecting and using personal information is a long-established activity, with records going back to at least the Roman era (Tavani 2008). Over the centuries, privacy has evolved in response to the specific (and changing) political and technological situations of different societies (Moor 2006; Regan 1995; Solove 2002; Tavani 2008). At the end of the last century, two streams of thought about privacy were predominant in the literature (Tavani 2008). One, the understanding of privacy as "restricted access", postulated that one has informational privacy when one is able to limit or restrict the access of others to one's personal information. The other, which understood privacy as "control", postulated that one has privacy when one controls information about oneself (Tavani 2008).

These perspectives' shortcomings in the face of new or imminent information practices led Nissenbaum (2004) to develop a new understanding of privacy as *Contextual Integrity*. The main idea behind this normative framework is that information flows must be appropriate, so as not to violate privacy. This aim is achieved if contextual-information norms are met (Nissenbaum 2004). According to Contextual Integrity, personal data flows are appropriate and consider user's expectations if context norms relating to the specific types of personal data in a specific scenario are taken into account and not violated by actors processing and sharing personal data (Nissenbaum 2011). This concept has been applied to numerous technologies and novel information practices (Barth et al. 2006; Jia et al. 2017).

Nevertheless, Nissenbaum (2019) herself recognizes that "[g]iven a technological landscape that includes vast data holdings, data analytics, AI, machine learning, IoT, mobile devices, and other computational capacities, there is a dire need for systemic principles that will expose the material risks of the current data policy anarchy" (Nissenbaum 2019, p. 255). The strength of Contextual Integrity in assessing data flows on a very fine, granular level goes hand in hand with the weakness that it struggles to cope with systemic effects caused by interconnected personal-data sharing and processing. Nissenbaum (2019) calls for making these hidden practices "available for inspection" and creating transparency across data chains but notes that what this means in detail is an open question, one that remains critically important to answer (Nissenbaum 2019).

2.2.2 Information Privacy in the IS Field

Information privacy research in the IS field often persists in using the definitions of the ability to control or limit access to the information about oneself (Bélanger and Xu 2015; Dinev et al. 2013; Kallemeyn and Chipidza 2021; Xu et al. 2008). Some design-oriented studies exist in this field (Callegati et al. 2015; Greenaway and Chan 2013; Kühl et al. 2020; Sjöström et al. 2022). However, a major part of IS research in the context of information privacy focuses primarily on individual actions and motivations and is most relevant to behavioral economics and psychology (Acquisti et al. 2015; Dinev et al. 2015; Kallemeyn and Chipidza 2021; Kehr et al. 2015). For example, researchers address individuals' intentions to disclose data (and the privacy concerns that relate to that intention) (Gopal et al. 2018; Steinbart et al. 2017); the motivating or discouraging factors (Thiebes et al. 2017); or the privacy paradox, which is a gap between the intention to disclose personal data and the disclosure behavior (Acquisti et al. 2015; Norberg et al. 2007).

In this context, privacy concerns refer to individual beliefs about personal data sharing and usage by, for example, other companies or unauthorized persons (Smith et al. 1996). Studies divide privacy concerns into the collection, secondary usage, errors, improper access, and control of data (Hong and Thong 2013; Smith et al. 1996). Secondary usage encompasses personal data processed by actors for a specific purpose, but which is then used for another secondary purpose without an individual's authorization (Smith et al. 1996). Improper access describes the situation where personal data are available to an actor who is not authorized to use or process them (Smith et al. 1996). The violation of information privacy and actors' unauthorized access to an individual's personal data can trigger adverse consequences (Karwatzki et al. 2017).

Besides physical, social, legal and career-related consequences, consequences provoked by corporate parties may be psychological, freedom-related or resource-related (Karwatzki et al. 2017). Psychological consequences include the negative impact on one's peace of mind owing to potential surveillance, unknown ramifications or loss of control (Karwatzki et al. 2017). Freedom-related consequences include the loss of freedom of opinion and behavior owing to organizational access to an individual's personal data; this can result in manipulations of opinion and behavior to influence an individual's decision and direct restrictions on behavior (Karwatzki et al. 2017). Resource-related consequences include loss of time, material losses and financial losses (e.g., price discrimination) (Karwatzki et al. 2017).

So far, privacy research at the group level remains scarce (Kallemeyn and Chipidza 2021). A few articles modeled personal data access in multi-party constellations (see exemplary Figure 1) (Benson et al. 2015; Conger et al. 2013; Karwatzki et al. 2017). However, "[n]o known research focuses on the data themselves, i.e., their existence, movement and life cycle once released by the individual." (Conger et al. 2013, p. 412f.).

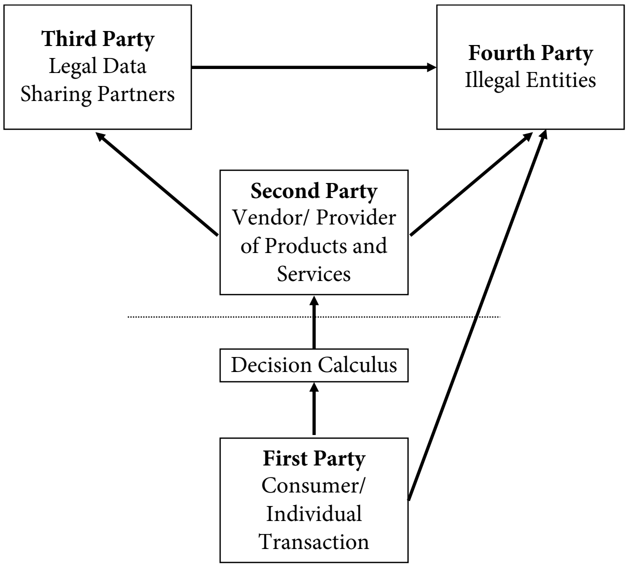


Figure 1. Model of Personal Data Sharing - Based on Conger et al. (2013)

Bélanger and Xu (2015) emphasized that for the future of information privacy research, it is necessary "to move beyond the existing theoretical frameworks, levels of analysis and traditional approaches to information privacy research" (p. 575). In this regard, privacy by design, privacy across levels of analysis, and the contextual nature of privacy are listed as three of five potential areas for future privacy research in the IS field (Bélanger and Xu 2015). In addition, the authors call to explore privacy violations as well as factors and problems that lead to actors' practices (Bélanger and Xu 2015).

2.2.3 Personal Data Protection under the GDPR

The General Data Protection Regulation (GDPR 2016) was implemented in May 2018. In the European Union (EU), the GDPR aims to protect the personal data of persons by preventing it from being unlawfully processed (GDPR 2016, Art. 1 (1)). The GDPR as a directive is applicable and binding for all EU member states. Compared to the previous Data Protection Directive, one of its important changes is its expanded applicability, even binding organizations outside of the EU when they process EU citizens' personal data (GDPR 2016, Art. 3 (2)). The GDPR also serves as a template for data protection regulation throughout the world, such as the California Consumer Privacy Act 2018 (de la Torre 2018). Under the GDPR, regulators can invoke substantial penalties of up to 4% of companies' annual worldwide annual turnover and award compensation claims to affected persons (GDPR 2016, Art. 82) when data protection clauses have been violated (GDPR 2016, Art. 83 No. 5).

In the context of the GDPR, the term “personal data” is defined as “any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (GDPR 2016, Art. 4 No. 1). An organization must take several technical and organizational measures to safeguard the rights and interests of the persons to whom the data in question relates. Every act of collecting, transmitting, using or otherwise processing personal data must be have a legal basis (GDPR 2016, Art. 6) and be compatible with a predefined purpose (GDPR 2016, Art. 5).

The GDPR offers a framework allowing affected individuals as well as regulators to assess personal data practices regarding their lawfulness or otherwise. However, the application of the law is not fixed and unilateral, and in the end the case-specific application of the GDPR by authorities and courts specifies what is lawful and what is not. Primarily, the GDPR enforces data protection by offering a binary approach to two opposing actors: a controller (the actor that processes the personal data and is responsible for the lawfulness of the processing) and a data subject (the affected individual or user). However, just as digital ecosystems include a more complex reality of actors and roles, so the GDPR is not limited to this approach and offers further roles that delineate responsibility and obligations for data processing operations.

2.3 Novel Personal-Data Practices in Digital Ecosystems

In digital ecosystems, intertwined interactions between actors and novel resource applications lead to new forms of personal data practices. However, a major part of privacy research in the IS field still focuses on the individual (Bélanger and Xu 2015; Kallemeyn and Chipidza 2021) and the concept of information privacy as one’s ability to control personal data about oneself. In this regard, dyadic interactions between an individual and a company have been investigated in depth (Acquisti et al. 2015; Kallemeyn and Chipidza 2021). However, research from systemic perspectives addressing novel multi-actor practices critical for information privacy has been much less emphasized. Thus, the research gap exists on the movement, the processing, and the life cycle of personal data (Conger et al. 2013; Spiekermann and Novotny 2015). “[N]obody knows for sure who shares which [personal data] with whom, in what form and on what occasions” (Spiekermann and Novotny 2015, p. 2).

Information privacy can be safeguarded when information flows are appropriate (Nissenbaum 2019). A central element of this concept is the determination of what is understood by a society as “appropriate.”

However, the opacity of ecosystems creates the need for knowledge and transparency to be able to apply the framework. Transparency gives researchers, practitioners, and regulators the ability to “see” a system—an ability often equated with understanding its underlying mechanisms (Ananny and Crawford 2018). Transparency also creates a basis from which to judge whether parties and related practices exist as intended; therefore, it is the key to governance and protection (Ananny and Crawford 2018) and opens the room for consideration of data practices in a society (Nissenbaum 2019).

To explore privacy in digital ecosystems, the first steps are to create different types of transparency and to identify which problems exist. Subsequent steps include investigating the different forms of personal-data practices from actor-centered and multi-actor perspectives. Building on the previous findings, the last step involves identifying and developing potential solutions that will advance privacy in digital ecosystems.

3 Research Design

This section outlines the overall research design to address the RQs (cf. 1.2). The research strategy offers 'high level' guidance while the research methods provide guidance at a more detailed level (Johannesson and Perjons 2014).

3.1 Research Strategy

To study privacy in digital ecosystems, this dissertation uses a highly explorative approach. In the course of this dissertation, each iteration's newly created insights determine the next iteration's direction. An iterative and agile study of privacy scandals allows the dynamic development of knowledge and transparency that includes identifying areas where ecosystems' privacy advancement would be both feasible and useful. However, this explorative approach and related openness unavoidably limit detailed planning and a controlled research procedure. Consequently, this strategy differs from other dissertations in the IS field, where works often position themselves in accordance with one of the two common paradigms (Bichler et al. 2016).

This dissertation adopts a research strategy inspired by both existing paradigms common in the IS field. The behavioral science paradigm originates from natural science research methods (Hevner et al. 2004). The research uses theories that explain or predict interactions among people, organizations and information technologies (Hevner et al. 2004). Alternatively, the design science paradigm originates from the fields of engineering and the sciences of artifice. Research under this paradigm seeks to create useful artifacts and design knowledge through information systems and related design (Hevner et al. 2004; Smith et al. 1996).

One central part of this dissertation is to propose approaches to advance privacy in digital ecosystems. Such advances are typically addressed in design-oriented studies (March and Smith 1995). However, the author is aware that the traditional design understanding of advancement is of limited applicability in this dissertation. This is for several reasons. First, not all aspects of digital ecosystems can be designed and thus, advanced. Second, the dissertation's proposals for advancement also draw from other disciplines and related possibilities for improving privacy, e.g., regulation. Essentially, the dissertation's research strategy is supplemented—indeed, underpinned—by interdisciplinary research. The goal of this dissertation is not confined to the single discipline of IS, and other disciplines are directly connected to it (cf. Figure 2). Because hard regulations exist that frame the digital realm by forcefully obligating its actors to behave in a certain way, and soft values guide actors and their behavior more subtly, this dissertation must consider the disciplines of law and ethics from the outset.

Furthermore, the knowledge generated by this work was always going to be very compatible with other research contexts. Thus, the author of this dissertation, Christian Kurtz, integrated his knowledge into additional research projects that addressed partnering in digital ecosystems. The discoveries made as a result of these collaborations regarding partnering in ecosystems have been reflected in, and contribute to, this dissertation.

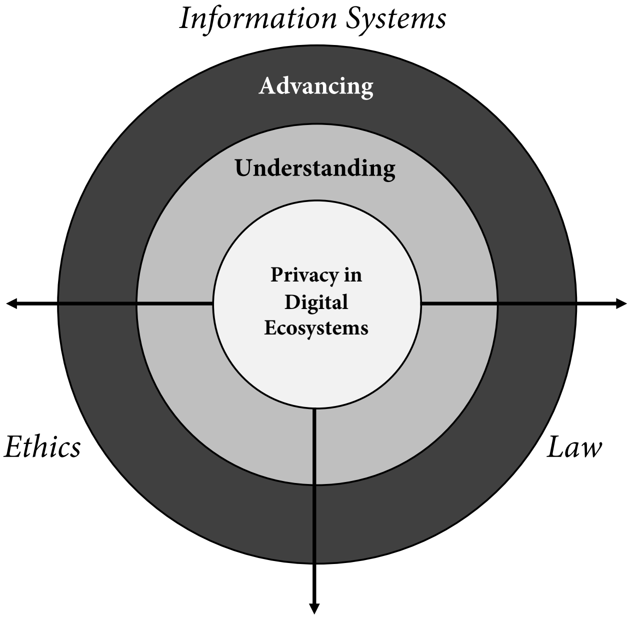


Figure 2. Research Process

The context of this dissertation made it difficult to easily access data material, which is of course essential for a research effort (Johannesson and Perjons 2014). Questionable or even negative phenomena resulting (for example) from organizational actions are often difficult to investigate because the perpetrators are reluctant to admit their existence. Given this problem, information privacy scandals published in the news have been identified as basic sources. This dissertation draws on Thompson's (2013) definition of 'scandal.' A privacy scandal refers to a scandal in privacy-critical personal-data practice in a digital ecosystem.

A scandal has the following characteristics: first, its occurrence or existence involves an element of secrecy or concealment. Second, its occurrence or existence involves a transgression related to information privacy. Third, individuals disapprove of the practices and may be offended by the transgression. Fourth, reporters express their disapproval by publicly denouncing the practices. Fifth, the disclosure and condemnation of the practices may damage the reputation of the party responsible for them (Thompson 2013).

3.2 Research Methods

This dissertation builds primarily on qualitative methods (cf. Figure 3). A large part of this dissertation builds on case studies of privacy scandals. The research methods of interdisciplinary assessments, archetype building, DSR, and VSD are combined with the case studies to address the research questions in the articles. In addition, literature reviews were conducted in the context of the articles. In addition, a systematic literature review also constitutes an individual publication. In the following subsections, the methods are briefly introduced and described.

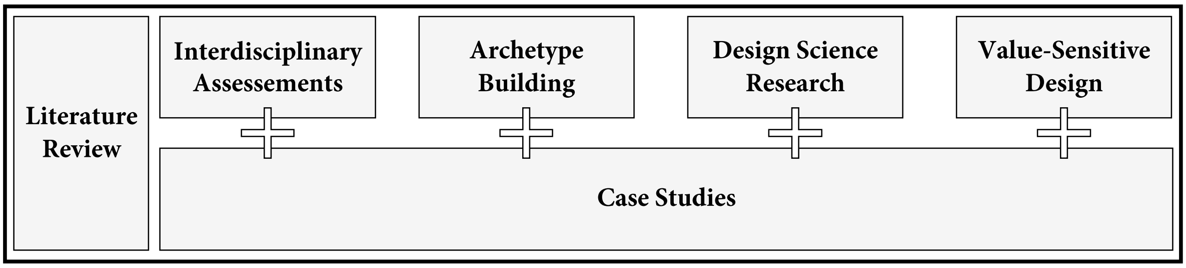


Figure 3. Applied Research Methods

3.2.1 Case Study

The case study method is appropriate when research is at an early, formative stage and when the research focus takes into account contemporary events (Benbasat et al. 1987). However, while a single case study approach may be appropriate to explore a phenomenon that occurs in rare or extreme circumstances, multiple cases offer more robust theory-building due to the greater variety and breadth of empirical evidence (Eisenhardt and Graebner 2007; Yin 2009). Moreover, multiple cases allow "comparisons that clarify whether an emergent finding is simply idiosyncratic to a single case or consistently replicated by several cases" (Eisenhardt and Graebner 2007, p. 27). In addition, heterogeneous sampling enables cross-case results to be more representative (Seawright and Gerring 2008). According to Yin (2009), news articles published in media can serve as sources of evidence in the context of case research.

In this dissertation, 47 cases are studied, of which 46 (C1 – C46) refer to privacy scandals (see Table 2). Some cases have been investigated in multiple publications, but not all case studies have yet been published in articles. The cases from as-yet unpublished manuscripts have been studied in depth in the course this dissertation and have provided important insights. Case C47 is an extreme case that provides insights about the complex ecosystem of eBay and related partners. The links in Table 2 lead to more information about the cases. Table 3 itemizes the nature of the sources and documents related to each case study.

Table 2. Overview of Investigated Cases

No.	Case Description	Exemplary Link	Paper No.
C1	Facebook, This Is Your Digital Life, and Cambridge Analytica.	cnet.co/2Vx3Ith	2, 3, 7, 8, 9, 10
C2	Weather app AccuWeather and third-party track user locations	zd.net/2IIZSW5	2, 3, 8, 9
C3	Android is sharing more data by inferring data through passive means.	cnet.co/2wkmNxv	9, 10
C4	Facebook sued over the collection of call and text data.	cnet.co/3oHJ4is	9, 10
C5	Restaurants use waitlist apps to collect personal data from customers.	cnet.co/2I32PA2	7
C6	Device fingerprints collected by the spyware Red Shell	bit.ly/355nhcM	7
C7	Healthcare app Ada transmitted data to companies like Amplitude or Facebook	bit.ly/2zREn0y	7
C8	Amazon's smart speaker Alexa makes unexpected recordings	nyti.ms/2IBbF93	9
C9	Smart TVs install tracking software ex-works	nyti.ms/36IhzNB	9
C10	Facebook SDK accessed device data by integration in Zoom	zd.net/32Tzz6u	9
C11	Facebook receives data (e.g., heart rates) from popular apps.	cnet.co/3mPi1jq	10
C12	VPN service Onavo Protect shared user data with Facebook.	cnet.co/3oVcrhl	10
C13	Up to 17,000 apps tracked individuals via their advertising IDs.	cnet.co/2Bx97Sf	10
C14	Facebook gathers personal data from Pregnancy+ and other apps.	cnet.co/2SZlxZv	10
C15	YouTube collects data on child viewers younger than 13.	cnet.co/2NqbjTB	10
C16	Google tracked individuals' locations without consent.	cnet.co/2GxsMVr	10
C17	Facebook shared user data with dozens of companies.	cnet.co/2Mimd2v	10
C18	Cambridge Analytica gathered Facebook data via "sex compass" quiz.	cnet.co/2HxGucc	10
C19	Thousands of Android apps are tracking children.	cnet.co/2IHKLK1	10
C20	Facebook uses "like" buttons to collect data on individuals.	cnet.co/2qEPbqB	10
C21	Facebook app CubeYou collected data through personality quizzes.	cnet.co/2IHLOcV	10
C22	Google was accused of secretly collecting data via its Nest Secure hub.	cnet.co/2TFdwvj	10
C23	Facebook tracks users and ex-employees who are potential threats.	cnet.co/3kTY5Lu	10
C24	Google monitors people via Screenwise Meter in exchange for gifts.	cnet.co/2JarzH5	10
C25	Facebook paid teens to access their browsing history and phone.	cnet.co/3kIayC8	10
C26	Google had a deal with Mastercard to receive data about retail sales.	cnet.co/3oEM8vJ	10
C27	Facebook, Google, and Microsoft use "dark patterns" to trick people.	cnet.co/3emckql	10
C28	Australian sports event sought to offer Wi-Fi to receive Facebook data.	cnet.co/3egZA43	10
C29	Facebook's SDK integration into Zoom accesses diverse data	cnet.co/3ujew9c	10
C30	Instagram may have used iPhone cameras to spy on users	cnet.co/3t98Ehe	10
C31	Google still tracks users in private web browser modes	cnet.co/3ecjI92	10
C32	iPhone apps record the actions of individuals without permission.	cnet.co/2thrkPu	-
C33	The Weather Channel app collects and shares location data.	cnet.co/2Qrew1Q	-
C34	App GasBuddy sold location data to Third Party Reveal Mobile.	cnet.co/2U51Vub	-

C35	Smart TVs are tracking viewers' data.	cnet.co/2UJhPIX	-
C36	Mail app developers might be reading personal e-mails.	cnet.co/2DkJ69H	-
C37	Verizon, AT&T, and Sprint had location data-sharing contracts.	cnet.co/2Zm8y8m	-
C38	Uber drivers have access to all users' pick-up and drop-off locations.	cnet.co/2KcInsW	-
C39	Yahoo and AOL read the e-mails of individuals.	cnet.co/2qxTBjB	-
C40	Grindr shared sensitive information like HIV status with third parties.	cnet.co/3ereRzj	-
C41	MoviePass tracks the locations of individuals.	cnet.co/2IHeCSV	-
C42	Fitness tracker Strava gives away sensitive military information.	cnet.co/2Xr5FRS	-
C43	Twitter is under investigation about its tracking practices.	cnet.co/387MDbZ	-
C44	GP booking service HealthEngine shared patient data with a law firm.	cnet.co/3kL4vge	-
C45	Several iOS apps shared location data with third parties.	cnet.co/2HEJd5G	-
C46	The social video app TikTok collected the personal information of children.	cnet.co/2vduG6M	-
C47	eBay involves 906 partner policies on the platform	ebay.com/gdpr	4

The news articles reporting the cases were used as a starting point to conduct a backward search to extend the data material to enable an in-depth investigation. A total of 1,330 documents were studied (Table 3). The collected and analyzed documents include news articles, blog articles, scientific studies, legal documents (e.g., court decisions), privacy policies and party websites, government press releases, and further documents such as technical studies.

Table 3. Overview of Data Collected and Analyzed Across the Cases

No.	News Articles	Blogs	Studies	Legal Documents	Privacy Policies	Party Websites	Government Press Releases	Further Documents	Σ
C1	81			1	1	1	2	1	87
C2	1	2				2		1	6
C3	4	1	1						6
C4	7					1	2		10
C5	9	1			1	1		1	13
C6	18	2						1	21
C7	10	1						1	12
C8	5					2			7
C9	2	1		1		3			7
C10	5					2			7
C11	3						1		4
C12	12					1			13
C13	14	2	1		1			1	19
C14	6				1			2	9
C15	12				1	1	2		16
C16	9	1			1	2		1	14
C17	13	1				1	1		16
C18	4						1		5
C19	3		1			1	1		6

C20	4	1							5
C21	10								10
C22	8	1				1	1	3	14
C23	4								4
C24	5							1	6
C25	7						1		8
C26	3								3
C27	4						1		5
C28	2					1			3
C29						1			1
C30						1			1
C31						1			1
C32	6	1							7
C33	3			1					4
C34	5		1						6
C35	4						1		5
C36	5	2							7
C37	11					1	2		14
C38	2								2
C39	6				3				9
C40	6				1				7
C41	3								3
C42	2	2							4
C43	2								2
C44	2					1			3
C45	4								4
C46	2			1		2	1		6
C47					828	80			908
Σ	328	19	4	4	838	107	17	13	1330

3.2.2 Literature Review

As Vom Brocke et al. (2009, p. 1) emphasize, "[s]cience is a cumulative endeavor as new knowledge is often created in the process of interpreting and combining existing knowledge." Webster and Watson (2002) highlight that a central part of a research effort is to review the existing literature. This dissertation incorporates different literature reviews that are considered in the articles. In addition, a systemic literature review was conducted to investigate the current state of existing Privacy by Design (PbD) studies (Vom Brocke et al. 2009; Webster and Watson 2002). The focus was on the research outcomes and applications of PbD to create an overview of existing literature and identify contexts that have been studied.

3.2.3 Interdisciplinary Assessment

In interdisciplinary assessments, the IS perspective has been connected to the legal and ethical fields. The iterative and dynamic process of interdisciplinary assessment is conducted in several research iterations and includes the constant re-evaluation and development of findings within and across manuscripts. In combination with the case studies, each of the disciplines involved came with particular methods, paradigms and terminology that resulted in the need to turn towards *other* disciplines to fully contextualize an appreciation of them. For example, one important question was how legal norms and their requirements could be interpreted or applied to validate their fulfillment, shape, and develop the legal interpretation. This was especially true of the GDPR – a legal framework that includes obligations that are, by design, very abstract and open to interpretation, offering obligated actors a chance to shape their meaning via real-life application. They thereby lend themselves perfectly to interdisciplinary assessment.

3.2.4 Archetype Building

Archetypes are promising for the investigation of patterns or sets of structures as they create systematic descriptions of structural arrangements (Schilling et al. 2017). Thus, the identification of archetypes lays the foundations for a subsequent theory-driven investigation of configurations and their inherent dynamics by highlighting new opportunities (Guillemette and Paré 2012). The taxonomy development developed by Nickerson et al. (2013) can provide guidance to the process of archetype building. This approach is widely used in the IS field and provides guidance for a structured, iterative process to identify archetypes. This approach has already been successfully applied in IS research for archetype building in different research contexts (Möller et al. 2019; Vogel et al. 2020; Weking et al. 2018). In this context, this dissertation considers archetype building to identify systemic resource integration patterns in actors' arrangements that violate information privacy.

3.2.5 Design Science

The core of the design science paradigm seeks to enhance human and organizational capabilities by creating useful artifacts. In this regard, the focus is on the analysis, design or use of information systems to determine how these aspects can effectively be accomplished (Hevner et al. 2004; Smith et al. 1996). DSR posits that design is a search process (Hevner et al. 2004) and thus typically progresses through iterations (Peffers et al. 2007). A common approach in DSR is to adapt the incremental phases of "problem identification", "objectives of a solution", "design and development", "demonstration", "evaluation" and "communication" in multiple iterations (Peffers et al. 2007).

A design theory therefore describes the construction of an artifact (Walls et al. 1992). For example, design goals specify the purpose and scope of a design theory (Gregor and Jones 2007). When design goals are generalized, they can enable application detached from a particular setup. (Horlach et al. 2019). Thus, creating design knowledge is fundamental for DSR (Gregor and Jones 2007; Kuechler and Vaishnavi 2008; Legner and Löhe 2012). However, guiding methods for the development of specific types of design knowledge exist only rarely (Baskerville and Pries-Heje 2010; Fischer et al. 2010; Legner and Löhe 2012). In this dissertation, identified problems that point out the main difficulties for achieving consent in a meaningful way were used to develop design goals. In other research contexts, further design knowledge has been developed.

3.2.6 Value Sensitive Design

Technology is not neutral or divorced from human values (Brey 2010; Simon 2016; Simon 2017) because human values are embedded, embodied or built into technology. In this regard, VSD increasingly attracts researchers in the IS field (Gebken et al. 2021a; Gebken et al. 2021b; Mueller and Heger 2018; Winkler and Spiekermann 2018). The VSD method promotes actively accounting for human values in developing technological artifacts by providing a framework for analyzing, weighing and operationalizing values into technology (Friedman and Hendry 2019; Friedman et al. 2008). According to Friedman and Hendry (2019), VSD can guide "researchers, designers, engineers, policymakers, and anyone working at the intersection of technology and society […], it provides theory, method, and practice to account for human values in a principled systematic manner throughout the technical design process." (p. 3)

The VSD method is divided into three phases to account for values in the design process of technical artifacts: technical, conceptual, and empirical investigations. The three phases of VSD repeat iteratively and are intended to influence each other throughout the iterations (Friedman and Hendry 2019). The approach does not prescribe specific methods to each phase, allowing users to select methods appropriate to the respective context of the application (Friedman and Hendry 2019; Friedman et al. 2008). In context of this dissertation, the impact of platform providers' power on actors in ecosystems that apply VSD was examined. In addition, aspects of VSD were incorporated in studies that considered the value of privacy.

4 Articles

The following section details the articles included in this cumulative dissertation.

4.1 Overview

This cumulative dissertation is based on nine peer-reviewed publications: two journal articles and seven articles published in conference proceedings (Section 9 to 17). Article no. 3 was nominated as the best paper at the Hawaii International Conference on System Sciences (HICSS) and was invited for an extended version submission to the Journal of Management Information Systems (JMIS). The extended version of the article was instead published in the Journal of Responsible Technology (JRT) (article no. 8). In addition, the Editor-in-Chief of the Pacific Asia Journal of AIS (PAJAIS) invited the authors of article no. 9 in February 2022 to submit an extended version of the article to the journal. Article no. 10 is under review (Appendix A). The article was accepted in 2019 to a workshop by the European Journal of Information Systems. The article was submitted to the related outlet's special issue on the dark side of analytics and artificial intelligence. The article passed the first round of the special issue but was rejected after the second round and did not make it in this outlet for publication (article no. 10).[5]

Table 4 provides an overview of all included articles ordered by publication time. The articles have been reformatted to ensure a consistent appearance as part of this dissertation (Section 9 to 17, Appendix A).

Table 4. List of Included Publications

No.	Article	Section
1	*Kurtz, C., Semmann, M., and Böhmann, T. (2018)* **Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors** Proceedings of the 24th Americas' Conference on Information Systems (AMCIS), New Orleans (USA).	9
2	*Kurtz, C., Semmann, M., and Schulz, W. (2018)* **Towards a Framework for Information Privacy in Complex Service Ecosystems** Proceedings of the 39th International Conference on Information Systems (ICIS), San Fransisco (USA).	10

[5] The article 'Gebken, L., Kurtz, C., Drews, P., Schirmer, I., and Böhmann, T. 2021b. "Human-Value-Oriented Digital Social Innovation: A Multilevel Design Framework," Proceedings of the 42nd International Conference on Information Systems (ICIS), Texas (USA)' was very valuable to the dissertation's author, Christian Kurtz. It offered insights on the formation of value-sensitive service ecosystems. However, this manuscript is not included in this dissertation.

3	*Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. (2019)* **The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems** Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), Hawaii (USA).	11
4	*Kurtz, C., Wittner, F., Vogel, P., Semmann, M., and Böhmann, T. (2020)* **Design Goals for Consent at Scale in Digital Service Ecosystems** Proceedings of the 28th European Conference on Information Systems (ECIS) - A Virtual AIS Conference.	12
5	*Vogel, P., Grotherr, C., Kurtz, C., and Böhmann, T. (2020)* **Conceptualizing Design Parameters of Online Neighborhood Social Networks** In Proceedings of the 15th International Conference on Wirtschaftsinformatik, Potsdam (Germany), 2020.	13
6	*Jacobs, M., Kurtz, C., Simon, J., and Böhmann, T. (2021)* **Value sensitive design and power in socio-technical ecosystems** Journal: Internet Policy Review (IPR).	14
7	*Burmeister, F., Kurtz, C., Vogel, P., Drews, P., and Schirmer, I. (2021)* **Unraveling Privacy Concerns in Complex Data Ecosystems with Architectural Thinking** Proceedings of the 42nd International Conference on Information Systems (ICIS), Austin (USA).	15
8	*Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T.(2021)* **Accountability of Platform Providers for Unlawful Personal Data Processing in their Ecosystems – A Socio-Techno-Legal Analysis of Facebook and Apple's iOS according to GDPR** Journal of Responsible Technology (JRT).	16
9	*Kurtz, C., Vogel, P., and Semmann, M. (2022)* **Exploring Archetypes of Value Co-Destructive Privacy Practices** Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS), Hawaii (USA).	17

Table 5 provides an overview of the manuscript in the Appendix that is currently under review.

Table 5. Paper under Review

No.	Manuscript	Section
10	*Kurtz, C., Burmeister, F., Semmann, M., and Böhmann, T.* **Multi-Role Actors and Rebounding Effects in Data Ecosystems – Exploring Big Tech's Privacy Scandals and GDPR Limitations** Under Review: 43rd International Conference on Information Systems (ICIS), Copenhagen (Denmark).	Appendix A

4.2 Descriptions

This section details the nine publications (cf. Table 4) and the manuscript in the Appendix (cf. Table 5). The following tables include the author names, article title, publication year, ranking of the outlet, type of publication, the aim of the publication, the applied methodology, the research contribution, and the co-authors' contribution to the respective article. If this dissertation's author, Christian Kurtz, is not the first author, his contribution to and learning from the related article are described.

Table 6. Summary of Article No. 1 (Kurtz et al. 2018a)

Citation	Kurtz, C., Semmann, M., and Böhmann, T. Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Proceedings of th 24th Americas' Conference on Information Systems (AMCIS), New Orleans (USA), 2018.
Ranking	WKWI: B, VHB-JQ 3: D, CORE: A
Type	Completed research paper
Track	Information Systems Security and Privacy
Methodology	Systemic literature review
Research question	What is the current state of research regarding the Privacy by Design-implementation of third-party data processors?
Research contribution	The GDPR raises novel requirements for companies regarding the personal-data processing of involved external data processors. One requirement addresses the companies' consideration of PbD. Given this regulatory obligation, this article creates the first rigorous and systematic literature review of PbD. In this regard, the article focuses on manuscripts that seek a third-party involvement in multi-actor arrangements. The results show a surprising dearth of research in this field.
Co-authors' contribution	Martin Semmann and Tilo Böhmann co-authored this publication. Both contributed to the methodological design, advised conducting a literature review, and provided overall feedback.

Table 7. Summary of Article No. 2 (Kurtz et al. 2018b)

Citation	Kurtz, C., Semmann, M., and Schulz, W. Towards a Framework for Information Privacy in Complex Service Ecosystems. Proceedings of the 39th International Conference on Information Systems (ICIS), San Fransisco (USA), 2018.
Ranking	WKWI: A, VHB-JQ 3: A, CORE: A*
Type	Short paper
Track	Conference Track: Bridging the Internet of People, Data and Things
Methodology	Case study, Interdisciplinary Assessment
Research question	How to study privacy-critical issues in service ecosystems?
Research contribution	This paper proposes an analytical framework for analyzing cases in complex service ecosystems. This framework includes a cross-impact matrix to identify privacy-critical issues helpful for both researchers and practitioners. In this paper, the cross-impact matrix is applied to the cases of AccuWeather and RevealMobile, and Facebook and Cambridge Analytica. Based on the application of the cross-impact matrix, various privacy-related problem propositions that exist in ecosystems are identified. These propositions serve as the basis for future studies of related practices. It became apparent that problems in digital ecosystems do not only exist between the user whose privacy is at stake and another actor but also between interconnected actors in digital ecosystems, which has consequent effects on users' privacy.
Co-authors' contribution	Martin Semmann and Wolfgang Schulz co-authored this publication. Martin Semmann provided overall feedback for the paper and contributed to its discussion section. Wolfgang Schulz contributed to the research design and proposed a high-level overview of the research framework.

Table 8. Summary of Article No. 3 (Kurtz et al. 2019)

Citation	Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems. Proceedings of the 52nd Hawaii International Conference on System Sciences, Hawaii (USA), 2019.
Ranking	WKWI: B, VHB-JQ 3: C, CORE: A (Best-Paper-Nominee)
Type	Completed research paper
Track	Privacy and Economics
Methodology	Case study, Techno-legal analysis (interdisciplinary assessment)
Research question	How can and should actors in service ecosystems be classified according to the GDPR?
Research contribution	With the GDPR taking effect, this article seeks to understand both the implications and opportunities the regulation affords privacy in ecosystems. In this article, a novel techno-legal analysis is applied to two cases that show that novel requirements arise for platforms as key actors in service ecosystems. The authors conclude that besides the role of service providers and third parties, the two major platform providers, Apple and Facebook, have to be classified as joint controllers for data processing operations within their ecosystems. Based on this analysis, the article discusses where privacy-preserving obligations in such ecosystems need to be positioned.
Co-authors' contribution	Florian Wittner, Martin Semmann, Wolfgang Schulz and Tilo Böhmann co-authored this publication. Florian Wittner contributed a legal perspective to the techno-legal analysis and the discussion that includes the description of obligations. Martin Semmann, Wolfgang Schulz, and Tilo Böhmann contributed to its discussion section and provided overall feedback for the paper.

Table 9. Summary of Article No. 4 (Kurtz et al. 2020)

Citation	Kurtz, C., Wittner, F., Vogel, P., Semmann, M., & Böhmann, T. Design Goals for Consent at Scale in Digital Service Ecosystems. In Proceedings of the 28th European Conference on Information Systems (ECIS) – A Virtual AIS Conference, 2020.
Ranking	WKWI: A, VHB-JQ 3: B, CORE: A
Type	Completed research paper
Track	Security and Privacy Research in Information Systems
Methodology	Case study, Techno-legal analysis (interdisciplinary assessment), Design science
Research question	What design goals address the problems of consent in digital ecosystems?
Research contribution	Privacy policies are important when personal data processing is based on user consent. The policies specify the purposes and details of data processing in a legally binding way. In a study of the extreme case that is eBay, with its large-scale and massively interconnected ecosystem partnerships, 18 problems are identified that demonstrate the main difficulties and problems for achieving consent in a meaningful (i.e., informed and voluntary) way. Based on these problems, design goals are developed, which can guide organizations, researchers and regulators to design meaningful consent in digital service ecosystems. The developed design goals are compared with the requirements for effective consent specified in the GDPR. The design goal of reasonableness regarding the time needed to be informed to provide consent, compared to the usage time of the service, is so far not taken into account in regulatory requirements and shows a crucial shortcoming.
Co-authors' contribution	Florian Wittner, Pascal Vogel, Martin Semann and Tilo Böhmann co-authored this publication. Florian Wittner supported the legal perspective to the techno-legal analysis and contributed the description of requirements for valid consent according to the GDPR. Pascal Vogel supported the data collection. Martin Semmann and Tilo Böhmann provided overall feedback for the paper.

Table 10. Summary of Article No. 5 (Vogel et al. 2020)

Citation	Vogel, P., Grotherr, C., Kurtz, C., & Böhmann, T. Conceptualizing Design Parameters of Online Neighborhood Social Networks. In Proceedings of the 15th International Conference on Wirtschaftsinformatik, Potsdam (Germany), 2020.
Ranking	WKWI: A, VHB-JQ 3: C, CORE: C
Type	Completed research paper
Track	Social Media in Business and Society
Methodology	Taxonomy development, Archetype building
Research question	What are the conceptually and empirically validated design parameters of neighborhood social networks?
Research contribution	This paper presents a taxonomy of design parameters of neighborhood social networks. Based on a literature review and an internet analysis, implications regarding the nature of neighborhood social networks are derived, and the importance of information privacy within the ecosystem is particularly highlighted. A further-developed taxonomy serves as a classification scheme for researchers and practitioners analyzing, selecting and designing neighborhood social networks.
Authors' contribution	Pascal Vogel, Christian Grotherr, Christian Kurtz, and Tilo Böhmann authored this publication. Pascal Vogel contributed the major part to the article. Christian Grotherr contributed to the research design and advised on the taxonomy dimensions. Christian Kurtz assisted regarding methodological questions and provided his knowledge on the discussions around the design parameters that consider privacy. The findings on the importance of privacy within the borders of a service system and related value proposition are integrated into this dissertation. Tilo Böhmann provided overall feedback for the paper and contributed to its discussion section.

Table 11. Summary of Article No. 6 (Jacobs et al. 2021)

Citation	Jacobs, M., Kurtz, C., Simon, J., and Böhmann, T. Value sensitive design and power in socio-technical ecosystems. Internet Policy Review, 2021.
Ranking	Not listed in IS Rankings.
Type	Completed research paper
Track	-
Methodology	Interdisciplinary assessment, Case study, Value sensitive design
Research question	RQ1: How and to what extent does the "grand challenge" of accounting for power in VSD get exacerbated by the integration of technical artifacts in increasingly vast and complex socio-technical ecosystems? RQ2: How does the organizational structure of socio-technical ecosystems affect the challenge of accounting for power in VSD? RQ3: How can this challenge be addressed? RQ4: Are there positive effects for VSD if the approach is applied in settings in which the power to make design decisions is distributed over various actors?
Research contribution	This paper examines how the distribution of power within socio-technical ecosystems poses a challenge in regard to the application of VSD and the value of privacy. For platform ecosystems, the paper shows that developers are required to interpret and realize a concept of privacy that is predefined by platform providers and manifests in the platform's boundary resource design. The article specifies four factors that determine the distribution of power: first, the level of decentralization of the ecosystem; second, whether VSD is applied at the core or the periphery; third, the temporality when power can be exercised; and fourth, the phase of VSD. The paper subsequently outlines how the challenge of accounting for power can be addressed to consider and advance values and especially privacy in ecosystems.
Authors' contribution	Mattis Jacobs, Judith Simon, and Tilo Böhmann co-authored this publication. Mattis Jacobs contributed the great part to the article. Christian Kurtz contributed to the study of platform-based ecosystems and supported the findings, discussion and conclusion. He provided his knowledge on ecosystems, platform providers' influence, boundary resources and privacy cases. The findings that platform providers define a privacy conceptualization for the ecosystem, and the aspects of power differences that exist within ecosystems, are also considered in this dissertation. Judith Simon contributed to the understanding of VSD and power as well as providing overall feedback. Tilo Böhmann contributed to the discussion and implications and provided overall feedback.

Table 12. Summary of Article No. 7 (Burmeister et al. 2021)

Citation	Burmeister, F., Kurtz, C., Vogel, P., Drews, P., and Schirmer, I. Unraveling Privacy Concerns in Complex Data Ecosystems with Architectural Thinking. Proceedings of the 42nd International Conference on Information Systems (ICIS), Austin (USA), 2021.
Ranking	WKWI: A, VHB-JQ 3: A, CORE: A*
Type	Completed research paper
Track	General IS Topics
Methodology	Case study, Expert interviews
Research question	RQ1: What are key concerns of business and regulatory stakeholders about privacy in data ecosystems? RQ2: Which elements and relations should be integrated in a data ecosystem architecture meta-model to address the identified concerns and leverage architectural thinking in the privacy context?
Research contribution	This paper specifies architectural thinking as a systematic approach to decomposing data ecosystems. Key privacy concerns of business and regulatory stakeholders were collected to build the foundation for the development of a data ecosystem architecture meta-model. The different instantiations of the model demonstrate its ability to disassemble privacy-critical practices. The article extends the scope of architectural thinking to the privacy context and builds a foundation for creating transparency in privacy-critical practices in ecosystems.
Authors' contribution	Fabian Burmeister, Pascal Vogel, Paul Drews and Ingrid Schirmer authored this publication. Fabian Burmeister contributed the major part of the article. Christian Kurtz contributed to developing the architectural meta-model for data ecosystems based on the knowledge of boundary resources in platform ecosystems. In addition, he contributed to clustering the concerns and instantiating the meta-model. The findings from this article how to create fine-granular transparency in ecosystems and the importance of organizational micro-processes that can lead to ecosystem-wide privacy effects are also considered in this dissertation. Pascal Vogel contributed to the instantiation of the meta-model. Paul Drews provided overall feedback. Ingrid Schirmer provided overall feedback and supported the development of the meta-model and its instantiation.

Table 13. Summary of Article No. 8 (Kurtz et al. 2021)

Citation	Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. Accountability of platform providers for unlawful personal data processing in their ecosystems–A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR. Journal of Responsible Technology, 2021.
Ranking	Not listed in common Information Systems Rankings.
Type	Completed research paper
Track	-
Methodology	Case study, Socio-techno-legal analysis (interdisciplinary assessment)
Research question	Are Major Platform Providers accountable for Personal Data Diffusion in their Ecosystems?
Research contribution	The platform providers influence their platform ecosystems to promote the service providers' contribution and exercise control by utilizing boundary resources. This study uses two high-profile cases and the GDPR to show that the boundary resource design, the arrangement and the interplay affect information privacy and shape the role of platform providers according to the GDPR. Companies accountable for unlawful personal data processing must fulfill obligations as otherwise they face possible fines of up to 4% of their annual worldwide revenues. Thus, a platform provider's accountability can have a huge impact on future platform design and the protection of individuals' information privacy in platform ecosystems.
Co-authors' contribution	Florian Wittner, Martin Semmann, Wolfgang Schulz and Tilo Böhmann co-authored this publication. Florian Wittner supported the legal perspective to the socio-techno-legal analysis and the discussion and implication sections. Martin Semmann, Wolfgang Schulz, and Tilo Böhmann contributed to the discussions and implications of the article and provided overall feedback.

Table 14. Summary of Article No. 9 (Kurtz et al. 2022)

Citation	Kurtz, C., Vogel, P., and Semmann, M. Exploring Archetypes of Value Co-Destructive Privacy Practices. Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS), Hawaii (USA), 2022.
Ranking	WKWI: B, VHB-JQ 3: C, CORE: A
Type	Completed research paper
Track	Digital and Cybernized Services and Digitalisation of Services
Methodology	Case Study, Archetype Building
Research question	Which resource integration patterns lead to value co-destruction violating information privacy?
Research contribution	In service research, value co-destruction emerged as a perspective from which to study undermined value co-creation. The article makes use of this lens to analyze information privacy. The article builds on a multi-case analysis of information-privacy violations reported in the news and elucidates seven archetypes of value co-destruction. The archetypes enable an understanding of the underlying mechanisms and effects of actor arrangements in service ecosystems. The article shows that understandings regarding privacy are not congruent between actors in ecosystems and can affect users' privacy. Other actors in addition to the user can be affected by privacy-critical actions in the ecosystem. The article highlights which roles can potentially advance privacy in related archetypes. The paper also elaborates on the assumption of service research that actors share institutional arrangements. The paper clarifies that this sharing only refers to a sense of having the same parameters, e. g. the same laws, and not to a sharing in the sense of having the same understandings.
Co-authors' contribution	Pascal Vogel and Martin Semmann co-authored this publication. Pascal Vogel contributed to the research design and advised on archetype building. Martin Semmann contributed to the introduction and discussion and provided overall feedback for the paper.

Table 15. Summary of Article No. 10 (Kurtz et al. 2022 (under review))

Citation	Kurtz, C., Burmeister, F., Wittner, F., Semmann, M., and Schirmer, I. Multi-Role Actors and Rebounding Effects in Data Ecosystems – Exploring Big Tech's Privacy Scandals and GDPR Limitations. 43rd International Conference on Information Systems (ICIS), Copenhagen (Denmark), 2022 – under review.
Ranking	WKWI: A, VHB-JQ 3: A, CORE: A*
Type	Completed research paper
Track	-
Methodology	Case Study, Techno-legal analysis (interdisciplinary assessment)
Research question	(1) What are the roles and effects of key actors in data ecosystems exposed by privacy scandals? (2) Can the GDPR be applied to regulate these roles and effects in data ecosystems?
Research contribution	This article shows that Big Tech companies take various roles across services contexts opposed to a user. In this regard, Big Tech companies' roles enable the data accumulation, diffusion and rebounding effects on users in a plethora of service contexts typically hidden for the user. Taking into account the GDPR, the article indicates that the GDPR's scope is too limited to regulate such personal data practices efficiently. Thus, a specific regulatory role for companies, tailored to their spheres of influence and the totality of their data processing operations, could prove necessary for ecosystem regulation.
Co-authors' contribution	Fabian Burmeister, Florian Wittner, Martin Semmann and Ingrid Schirmer co-authored this publication. Fabian Burmeister supported the methodological section, case collection and analysis, discussion, and the article's editing. Florian Wittner supported the legal analysis and the discussion. Martin Semmann and Ingrid Schirmer supported in case analysis, discussion, and provided overall feedback for the paper.

5 Theoretical Contributions

This section specifies the theoretical contributions made by this dissertation. The results do not always build directly on each other in a linear fashion due primarily to the strongly exploratory nature of this work in the research field.

The first part of this section focuses on understanding privacy-critical practices in ecosystems. It is divided into identifying existing problems, creating transparency of personal-data practices, and considering actor-centered and multi-actor perspectives. The second part comprises contributions regarding the advancement of privacy in digital ecosystems. The design knowledge developed for consent in digital ecosystems is included and the contribution of platform providers and related boundary resource composition is characterized. The third part details the contributions of other research contexts and specifies which findings contributed to this dissertation, both in terms of understanding and advancing privacy in ecosystems. Summing up, the fourth part specifies the overall theoretical framework by taking an integrated view of the contributions described.

5.1 Understanding Privacy-Critical Practices in Digital Ecosystems

Kurtz et al. (2018b) specified an analytical framework valuable for the exploration of privacy in digital ecosystems that has been adopted by most of the articles of this dissertation. The main idea of this analytical framework is that the analysis of privacy scandals can help to characterize privacy-critical issues in ecosystems. This then builds the basis for identifying and deriving problem propositions. These problem propositions in turn build the starting points for developing options for action regarding policymakers, industry and users. In this context, Kurtz et al. (2018b) used the term "ecosystem" for the first time to indicate that actors interact not only with information systems where everything is designed in detail but also in 'systems of systems'. Parts of these systems are dynamic and evolve in the interaction among actors. Actors make decisions that affect other actors, which affect (for example) the scope of subsequent (design) decisions. In literature, only a few models touch upon multi-party interactions involving access to personal data (Benson et al. 2015; Conger et al. 2013; Karwatzki et al. 2017). Kurtz et al. (2018b) created an overview of personal data flows that can potentially exist among actors with the roles of user, platform provider, service provider and third party in a ecosystem (Figure 4).[6]

[6] The tables and figures in this section have been slightly (linguistically) revised compared to their publications in the articles. For example, the actor names are modified in this figure for a consistent naming of involved actor groups across the dissertation. The "third party" was originally named "backend service", but it characterizes the same actor group.

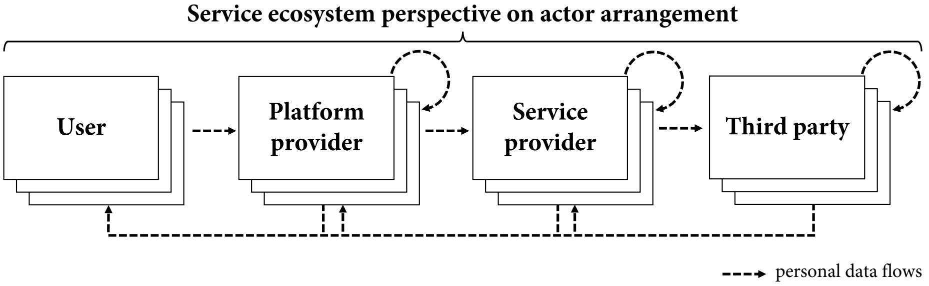


Figure 4. Data Flows in Service Ecosystems – Based on Conger et al. (2013) (Kurtz et al. 2018b)

Compared to the existing models in IS literature (Benson et al. 2015; Conger et al. 2013; Karwatzki et al. 2017), Figure 4 highlights that multiple actors related to a single role can appear and process or share personal data within an ecosystem. For example, multiple third parties can appear in a digital interaction. Personal data flows exist between actors with the same role and related actors in other roles. In addition, a central element of this model is that it highlights that personal data also flows back to a user. Multiple users can be seen to be affected by data flows and practices within a service ecosystem.

5.1.1 Problems for Information Privacy

Different critical issues for privacy became visible when cases taking place in digital ecosystems were examined. Kurtz et al. (2018b) developed and applied a cross-impact matrix to make aspects transparent and to describe the problems existing for privacy in two cases (cf. Table 16). In this regard, the privacy problems exist in the relationships of two actors that do not necessarily include the user. Instead, problems between actors in ecosystems can affect an individual's privacy. These findings emphasize that the dyadic view on the relationship between a user and another actor - dominant in the IS literature - is too limited to address all the problems that exist in digital ecosystems involving multiple actors.

In total, nine problem propositions have been identified based on the analysis of two cases. One problem proposition highlights the issue for platform providers that service providers do not consider user decisions properly. The interaction of service providers and third parties can also create problems for users' information privacy. For example, a third party may not deal with the personal data according to the user's interests. Another problem proposition highlights that users have only limited knowledge about ecosystems, especially regarding the third parties and their practices involving their personal data. The problem of a missing "Overview of Backend Service" was identified in the literature review on third-party data processors by Kurtz et al. (2018a) and highlights the problems that exist regarding opacity within service ecosystems. The problem proposition "Format of Transparency" emphasizes that if a user gives consent to a service's privacy policy, the privacy policies of third parties are also accepted. From a legal perspective, the question remains whether such a form of consent is valid.

Table 16. Derived Privacy-Related Problem Propositions (Kurtz et al. 2018b)

		Impact on			
		Users	**Platform Providers**	**Service Providers**	**Third Parties**
Action by	**Users**	Check of Privacy Statements and Settings	Careful Use of Platforms		
	Platform Providers	Default Settings for Privacy Protection		Implementation of User Decisions, Control when Data leave Platform	Control when Data leave Platform
	Service Providers	Format of Transparency			Interaction with Backend Services
	Third Parties	Overview of Backend Services			

The two analyzed cases particularly highlighted the necessity to create transparency of personal data processing in digital ecosystems and to investigate the actors' connections to third parties in digital ecosystems. A literature review by Kurtz et al. (2018a) aimed to identify the current state of research regarding the privacy-sensitive involvement of actors serving as third parties. The authors proposed a research agenda based on the state of knowledge (Table 17). The first points highlight the necessity of more connected works, given that publications have been scattered across the field. The second point highlights the need to consider the privacy regulation of the GDPR, which at the time was new. The third, fifth and sixth points propose the development of solutions that are helpful for embedding and monitoring third parties, while the fourth point emphasizes the need for ensuring transparency within and between organizations. This aspect is addressed in the next subsection (5.1.2).

Table 17. Research Agenda for Privacy by Design regarding Third Parties (Kurtz et al. 2018a)

Research Agenda
I. Consolidate research perspectives to establish common foundations for Privacy by Design
II. Derive and validate the core requirements for Privacy by Design to comply with GDPR
III. Expand design science research efforts beyond the derivation of requirements
IV. Develop concepts to ensure transparency in and between organizations
V. Develop benchmarking for the evaluation of data processors
VI. Develop decision support tools to enable developers to carefully decide on integrating data processors in the form of third parties and the resulting consequences regarding being compliant with the GDPR

This section contributes to RQ-1. In the initial articles of this dissertation, the ecosystem perspective is used first to access the research context and then to characterize the privacy problems that exist. A depiction has been developed that illustrates potential personal data flows in service ecosystems across the actors involved. The model includes novel aspects such as personal data flows back to the user and the diversity of actors related to one role. A cross-impact matrix highlights that information privacy problems in an ecosystem do not necessarily exist between the user and another actor. Instead, problems between actors in other roles can affect a user's privacy. As a result, both the study of two high-profile cases and a subsequent literature review highlight the necessity of transparency regarding data processing and practices.

5.1.2 Transparency of Data Practices in Digital Ecosystems

For this dissertation, four different approaches have been developed and used to make personal data practices in digital ecosystems transparent. Besides the usage of cross-impact matrices, quantitative and illustrative forms of transparency have been created. A fourth type is contained in the section that specifies contributions in other research contexts (5.3.2). Burmeister et al. (2021) developed an architectural lens on data ecosystems (cf. 5.3.2).

Although in practice privacy policies create a kind of transparency, their applicability is doubtful, as the following contribution emphasizes. Kurtz et al. (2020) created a quantitative transparency analysis to examine the potential complexity when many actors and their related policies are involved in an ecosystem. The study of the extreme case of eBay's ecosystem revealed that the platform lists six purposes with a total of 2,740 partner entries (Table 18). A partner can be listed in multiple purpose categories on eBay's website. A data clean-up of the 2,740 partner entries resulted in 906 unique organizations to which a user is exposed in eBay's ecosystem (Table 19).

Table 18. Partner Entries on eBay (Kurtz et al. 2020)

Purpose category	Number of partner entries
'Content selection, delivery, and reporting	315
'Website Improvement'	421
'Google Advertising'	645
'Storing and accessing information on your devices'	502
'Ad selection, delivery, and reporting	460
'Personalizing advertising based on your behavior'	397
	2,740

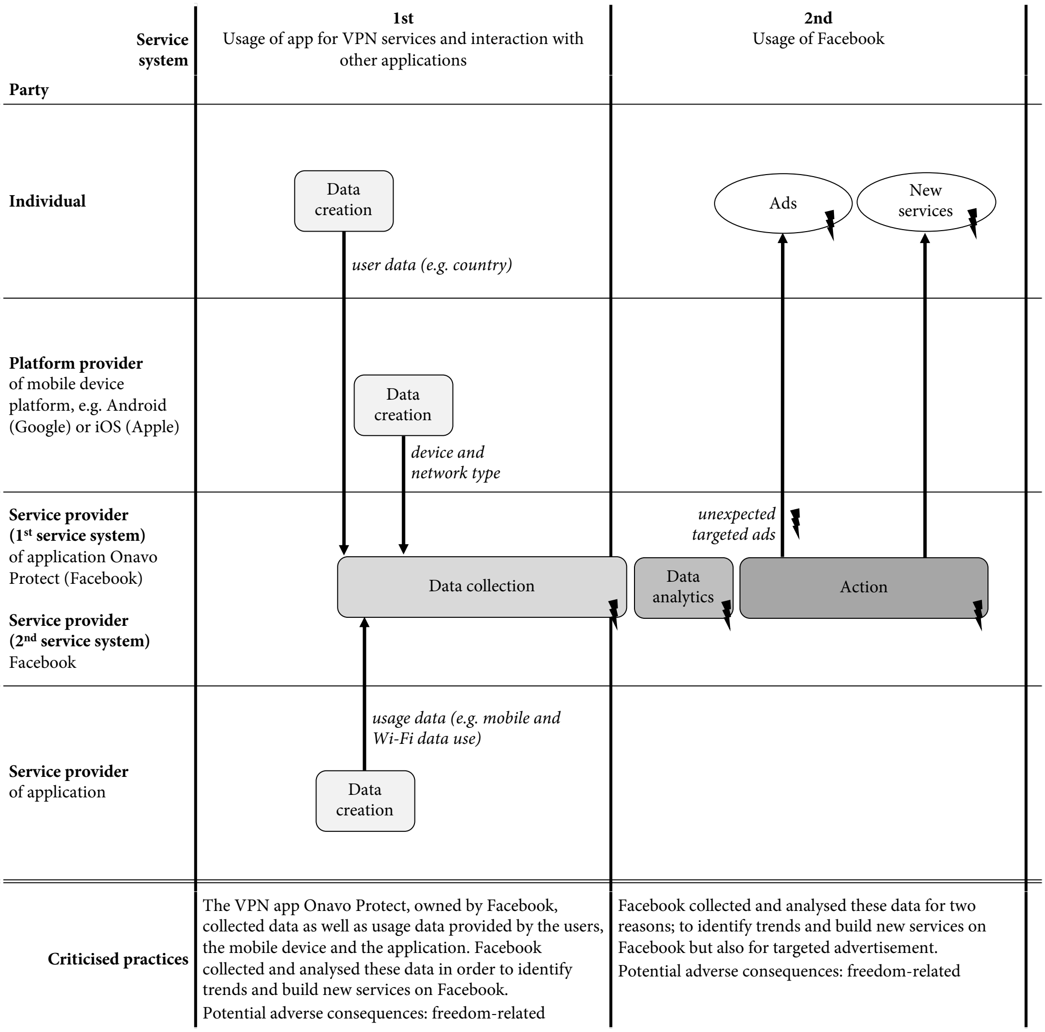
Kurtz et al. (2020) performed a data collection and analysis to obtain detailed insights. It is important to note that practices such as removing duplicates or crawling data are not typically performed by users. In addition to the names of partners, the related privacy policies are referenced on eBay's website. The authors identified 827 privacy policies of 906 third parties that could be accessed. Of the 827 accessible privacy policies, 735 are in English. The other 92 policies were in 16 other languages: Bulgarian, Chinese, Czech, Danish, Dutch, German, Finnish, French, Italian, Japanese, Polish, Portuguese, Russian, Slovak, Spanish and South Korean. On those companies' websites, no option existed for users to change the language of the policy. Finally, 79 privacy policies were not accessible at all.

Table 19. eBay Partners' Privacy Policies in Numbers (Kurtz et al. 2020)

Partners	Count	Word count
Unique	906	-
Privacy policies not accessible	79	-
Privacy policies accessible	827	2,221,079
Privacy policies accessible in English	735	1,984,823
Privacy policies accessible in other languages (16 languages)	92	236,256

The average reading time has been calculated to determine how long it would take to be informed to provide consent to the data practices in eBay's digital ecosystem. 7,940 minutes are required to read the accessible privacy policies in English for eBay's digital service ecosystem. This is equivalent to 132.3 hours. That's 16.5 working days (assuming 8 hours per day) or 5.5 24-hour days. 171 partners whose policies are in languages other than English or are inaccessible are not considered in this result. This calculation only relates to reading time, which might not necessarily correspond with the time required for the average user to fully understand the content and implications of the policies. The period of 5.5 days conflicts with some of eBay's auction durations, which can last one, three, or five days. This quantitative transparency for an ecosystem shows the massive number of actors who would be allowed to access and process personal data based on a single digital interaction.

Besides the quantitative form of transparency, another form of transparency has been used in the course of this dissertation. In literature, transparency on modeling the movement and life cycle of personal data once it has been released by an individual, such as who shares this personal data with whom and on what occasions, is scarce (Conger et al. 2013; Spiekermann and Novotny 2015). Kurtz et al. (2022 (under review)) illustrated exemplary data flows and the data processing steps of privacy scandals. An example is given in Figure 5 that illustrates practices related to the app "Onavo Protect", which is owned by Facebook. This app collected data about users' activities and diffused these data into a second service system, where Facebook's internal-market researchers collected and analyzed them to identify trends for building new services on Facebook and providing targeted advertisements. Figure 5 illustrates processing steps as elements to describe the sequential actions conducted by multiple parties. These steps include data creation, data collection, data analytics and insight-based action. The figure describes criticized practices and related potential adverse consequences from actors having access to personal data (Karwatzki et al. 2017). Analytics-process steps and data flows that have been criticized in a scandal are marked with flash symbols. Multiple service systems are considered, to underline that actors execute service-system crossings into systems not dedicated to the same value proposition. The crossing involves moving personal data created in the initial service system to another service system. The interaction of two service systems can be characterized as a service ecosystem.


Service system
Party
1st
Usage of app for VPN services and interaction with other applications
2nd
Usage of Facebook
Individual
Data creation
user data (e.g. country)
Ads
New services
Platform provider of mobile device platform, e.g. Android (Google) or iOS (Apple)
Data creation
device and network type
Service provider (1st service system) of application Onavo Protect (Facebook)
Service provider (2nd service system) Facebook
unexpected targeted ads
Data collection
Data analytics
Action
usage data (e.g. mobile and Wi-Fi data use)
Service provider of application
Data creation
Criticised practices

The VPN app Onavo Protect, owned by Facebook, collected data as well as usage data provided by the users, the mobile device and the application. Facebook collected and analysed these data in order to identify trends and build new services on Facebook.
Potential adverse consequences: freedom-related

Facebook collected and analysed these data for two reasons; to identify trends and build new services on Facebook but also for targeted advertisement.
Potential adverse consequences: freedom-related

Figure 5. Illustration of a Privacy Scandal (Kurtz et al. 2022 (under review))

The analysis and illustrations of various privacy scandals enabled the identification of two privacy-relevant phenomena (Kurtz et al. 2022 (under review)). First, the phenomenon of personal data diffusion characterizes practices that exceed service system borders. Service systems can be tailored regarding the value proposition, which is the reason why a user uses a platform or service from a particular company. However, personal data are not always used for activities regarding the value proposition, and they may leave service systems. The cases show that an organization's diffusion of personal data can create rebounding effects that are likely to be unanticipated by the users due to their diverse origins. Thus, rebounding effects are privacy impacts on individuals involving personal data appearing in other service contexts. These effects may create adverse consequences (Karwatzki et al. 2017). Information about these practices is rarely typically available; this opacity hinders attempts to make detailed statements regarding the existence and depth of such consequences.

In this section, RQ-2 is addressed by creating forms of transparency. Transparency has to be seen in the context of related necessities. One form highlights the overview of partners and policies in a single digital ecosystem. This form of transparency contributes to the understanding that providing informed consent in digital ecosystems can make unreasonable temporal demands of individuals. The analysis and illustration of privacy scandals generates insight into two privacy phenomena. First, diffusion explains personal data practices that exceed system borders. Second, rebounding effects characterize unanticipated privacy impacts with adverse consequences for individuals derived from prior personal data diffusion.

5.1.3 An Actor-centered Perspective on Big Tech Companies

This dissertation uses an actor-centered perspective to address the personal-data practices of Big Tech companies in ecosystems (Kurtz et al. 2022 (under review)). Unlike actors assuming a single role concerning an individual, Big Tech companies take on multiple different roles. These companies assume the roles of platform provider, service provider or third party to accumulate and use personal data. These roles help the companies establish access to personal data in various service contexts (see Figure 6).

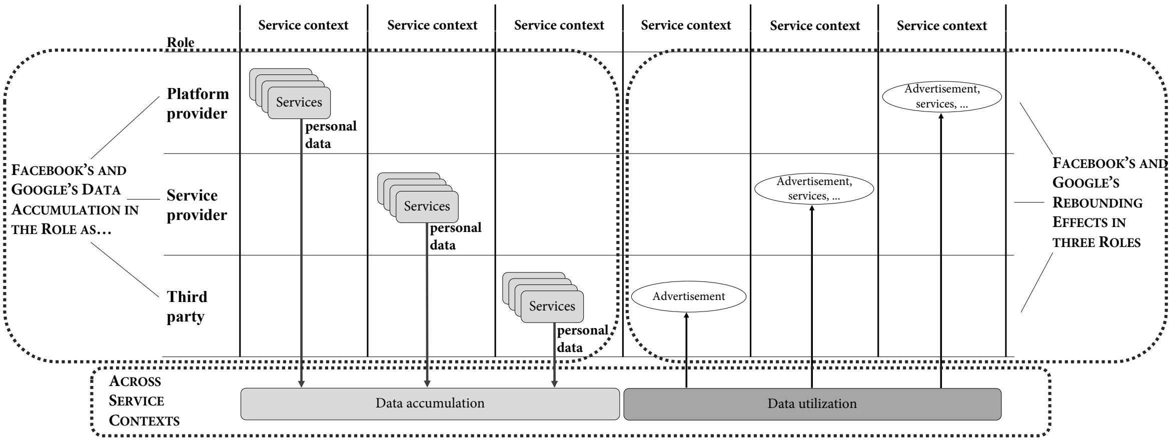


Figure 6. Privacy-Critical Multi-Role Companies (Kurtz et al. 2022 (under review))

Big Tech companies such as Google and Facebook use different roles and adopt practices under different names to accumulate and diffuse personal data across service contexts. The companies appear in diverse service contexts but do not limit themselves and their data usage to those service contexts. Big Tech companies use the existing consent limitations and link all personal data accumulation and utilization practices across their roles to a single privacy policy. Here, the personal data accumulation and usage of various personal data across diverse sources – no matter the role or service context used to acquire it – are summarized under one umbrella for diverse purposes. The data accumulation across service contexts leads to individuals' and regulators' uncertainty about data practices in ecosystems. Here, only the data-accumulating companies have detailed insights. Big Tech companies create rebounding effects in other service contexts that are likely to be unanticipated by the users. Rebounding effects can be characterized as information privacy violations for individuals in ecosystems that base on the opaque data accumulation from one or multiple service contexts (Kurtz et al. 2022 (under review)). Rebounding effects involve the processed data flowing from actors in ecosystems to individuals and can produce adverse consequences. Big Tech companies particularly create rebounding effects because of their various roles in service contexts. The companies take on the same or different roles that lead to the rebounding effects. In this regard, individuals no longer have control over their data and related life cycle in digital ecosystems.

This section addresses RQ-3 and highlights that Big Tech companies proliferate in digital interactions as platform providers, service providers or third parties. Big Tech companies are often referred to as platforms, which does not reflect the extent of their roles in data ecosystems. Their connections into diverse service contexts create an efficient ecosystem-connecting mechanism for accumulating personal data, as involvement in digital interactions leads to personal data access. The companies systematically embed digital ecosystem configurations that decouple data from the original value proposition and cross service system boundaries to utilize personal data in other service contexts. This usage of diffused data in other service contexts leads to unanticipated rebound effects in the vastness of data ecosystems. The connection between data accumulation and rebound effects is difficult to uncover due to the secrecy established around the inner workings of companies' data ecosystems.

5.1.4 A Multi-Actor Perspective on Value Co-Destructive Archetypes

Besides an actor-centric view, a multi-actor perspective has been added to the analysis conducted by this dissertation. Kurtz et al. (2022) use the concept of value co-destruction derived from service research. Seven archetypes of resource integration patterns have been identified that include privacy violations (cf. Table 20). The archetypes reflect organizational actor configurations where one or multiple actors violate information privacy by integrating—intentionally or unintentionally—users' personal data in ways that are not expected or appropriate. The archetypes show that other actors in addition to the user may be affected by value co-destruction. (This fact has already been noted in the section that specifies problems in ecosystems (cf. 5.1.1).)

Table 20. Seven Privacy Co-Destructive Archetypes (Kurtz et al. 2022)

No	Description	Value Co-Destruction by			Value Co-Destruction for			
		Platform provider	Service provider	Third-party	User	Platform provider	Service provider	Third-party
I	The platform provider is the only actor in the value co-destruction process that causes a negative value outcome for an individual in the form of an information privacy violation. On a device platform, the provider can exploit the device data interface.	x			x			
II	The platform provider co-destroys value together with a service provider. The role of the platform provider in the design of data access may be crucial.	x	x		x			
III	The platform provider interacts with a third party not visible to a user in an interaction. A user cannot replace a third party. In this archetype, the third party acts as a platform extension. The service provider may also be affected.	x		x	x		x	
IV	This archetype has a service provider using their data access (in certain cases provided via the platform). A user has the option to replace one service with another.		x		x			
V	The value for a user is co-destroyed by a service provider in combination with a third party. Third-party integration in a service can be opaque for a user. However, with the knowledge of value co-destruction, the user can replace one service with another.		x	x	x	x		
VI	In this archetype, the third party takes advantage of their integration into a service. Value is co-destroyed by the third party's data processing, which is often opaque to the service provider, platform provider and user.			x	x	x	x	
VII	This archetype includes the roles of a platform provider, service provider and third party that are involved in the value co-destruction that a user faces. No counterbalancing actor group exists in this archetype that could serve as a corrective.	x	x	x	x			

The platform provider is involved in four of the seven archetypes. Since the platform provider is a powerful actor and can prescribe the practices in the platform ecosystem (cf. 5.2.1), no actor group can act as a corrective in these four archetypes. When market mechanisms cannot generate corrective functions due to the absence of competition because of a prevailing oligopoly or monopoly (for example, for iOS or Android), privacy intervention for these archetypes through regulation is the most plausible way to prevent value co-destruction. In the archetypes in which a service provider or a third party is involved, users typically have more opportunities to switch services and related providers. In such archetypes, a platform provider can act as a corrective to protect users' privacy.

The literature already indicates that interactions may include value co-destruction in a service ecosystem due to the actors' goals being non-congruent, or the actors trying to maximize benefits without heeding the consequences for subsequent actors (Mele et al. 2018). Service research indicates that institutions define acceptable behavior and enabling and constraining social action (Vargo and Lusch 2016). However, Mustak and Plé (2020) emphasize that not all actors might have the same understandings and perceptions of institutional arrangements (Kleinaltenkamp 2018; Plé and Demangeot 2020). Kurtz et al. (2022) contribute to the knowledge on information privacy highlighting the importance of the meaning of "shared" in different institutional arrangements. Sharing can be understood in many ways. Thus, if divergent interpretations of institutions and institutional arrangements exist, this can create value differences.

This section addresses RQ-3 and contributes insights on the actor configurations that may be involved in privacy-critical practices. The archetypes set the foundations for further investigations. Other actors besides the users can be affected. Actors in the form of platforms or service providers can hinder other actors from creating privacy violations, while users can choose other services that have other third parties involved. This can be difficult if platforms have to be replaced, and alternatives rarely exist—in such circumstances, regulations can be valuable. Finally, this section contributes to understanding the important differentiation between shared and joint institutional arrangements.

5.2 Advancing Privacy in Digital Ecosystems

After understanding different aspects and practices affecting information privacy in digital ecosystems, this subsection specifies the contributions that advance information privacy in digital ecosystems. First, platform providers' roles and related boundary resources are investigated. Second, design knowledge for consent at scale in digital ecosystems is specified.

5.2.1 Platform's Boundary Resource and Their Role for Privacy

A large part of digital interaction is conducted over a platform (Lusch & Nambisan, 2015). In this context, boundary resources are socio-technical manifestations of the ways in which a platform provider controls the platform and involved actors. Kurtz et al. (2021), based on their previous study (Kurtz et al. 2019), identified that the concept would be valuable in connecting the IS field and legal field regarding data protection in digital ecosystems. Table 21 describes how boundary resource categories, which include data access, distribution, policies, and related boundary resources such as data interfaces and the app review process, are privacy-crucial (see also Figure 7).

Table 21. Overview of Boundary Resources Relevant to Information Privacy (Kurtz et al. 2021)

Category	Boundary Resource	Description
Data Access	Data Interfaces	Enable service providers and third parties to access data via the platform
	User-Centered Configuration	Enables users to set configurations of the data accessible to service providers and third parties
Distribution	Access to App's Privacy Statement	Describes the access to the policies that explain how the app wants to collect, use, share and manage the transmitted data
	App Review Process	Reviews app compliance with the platform policies and guidelines
	App Store	Provides the distribution channel for service providers
Policies	Platform Policies and Guidelines	Defines terms and conditions for service providers in developing, testing, distributing, maintaining and running an app

Kurtz et al. (2021) define the boundary resource composition in a platform ecosystem as a configuration of boundary resources that are interdependent. A focus on a single boundary resource can help to create specific effects. However, reviewing the entire composition is required for a holistic view of the resource's (joint) effects and non-effects in the ecosystem and (for example) their effects on an individual's privacy. Boundary resources can be designed to act in a protective or a violative manner. Thus, boundary resources and related composition can raise or lower the bar to information privacy in a platform ecosystem.

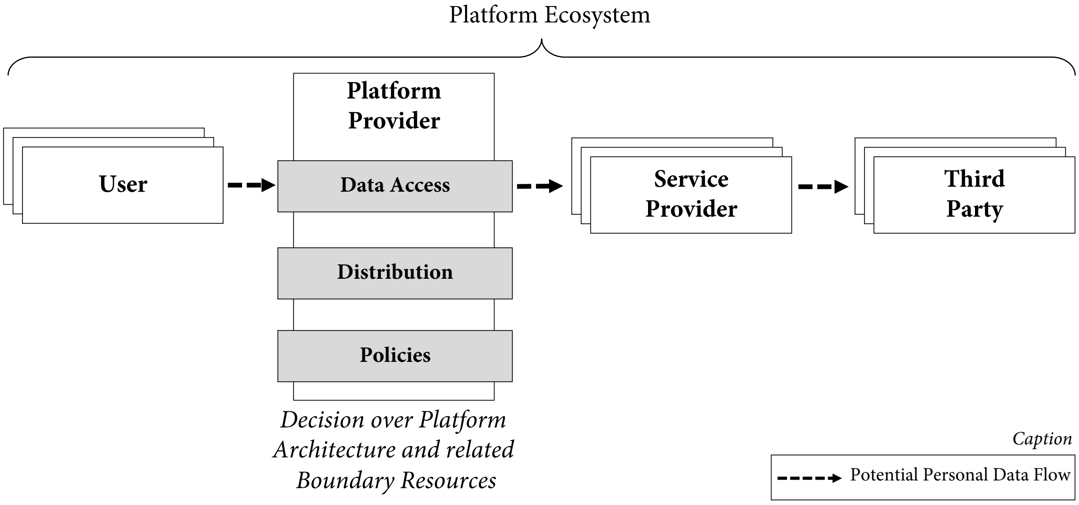


Figure 7. Privacy-Related Boundary Resources in Platform Ecosystems (Kurtz et al. 2021)

The knowledge regarding boundary resources and their effects on privacy has been used in three further contexts. It contributed conceptually to create an architectural meta-model of data ecosystems (cf. 5.3.2). It assisted in the ethical understanding of the power relationships in digital ecosystems (cf. 5.3.1). Finally, it facilitated at the intersection of IS and law to assess actors and related processing operations in platform ecosystems according to a regulation (cf. 6.1.2).

This section highlights that boundary resources have a huge impact on personal data processing and, consequently, on privacy in platform ecosystems. In this regard, the composition of boundary resources is introduced, showing how boundary resources depend on each other. Considering the composition is important for raising the level of information privacy in platform ecosystems. The knowledge about boundary resources and information privacy is used in the three research contexts of ecosystem architectures, actors' power relations, and regulatory assessments based on the GDPR.

5.2.2 Design Goals for Consent at Scale

Kurtz et al. (2020) show in their case study of eBay the potential scope of a single digital ecosystem. In such a context, fulfilment of the regulatory purpose of requiring users' consent is highly questionable. Digital ecosystems also include the recursive challenge that privacy policies refer to third parties, who themselves refer to other parties. Given this problem, the consequences of a user providing data become unpredictable. The current form of consent ultimately leads to users (justifiably) not comprehending personal data processing in related ecosystems.

Kurtz et al. (2020) derived seven design goals (DGs) as a basis for advancing the act of consent for data processing in digital ecosystems (cf. Table 22). 17 problems faced by users were classified and served as the basis for deriving DGs. The DGs are generalized and can be applied to various digital ecosystems. The design goals DG1 – DG4 consider the outset and the diversity of policies and related content in a digital ecosystem. DG5 addresses the dynamics within an ecosystem that must be addressed. The sixth goal, DG6, considers that actors integrate numerous data processing operations and purposes in a single policy detached from the specific use of a particular service offered by an actor. While DG1 to DG6 are helpful to concretize the abstract requirements for valid consent according to the GDPR, DG7, the reasonableness of the time required to provide consent in relation to the usage time of the service, is so far neither covered in practice nor by regulation. However, this design goal will be increasingly important for consent as digital ecosystems and associated data practices grow concomitantly.

Table 22. Design Goals for Consent in Digital Ecosystems (Kurtz et al. 2020)

No.	Design Goal
DG1	No personal data processing before providing consent
DG2	Accessibility of information concerning data processing and purposes
DG3	Uniformity of information concerning data processing and purposes
DG4	Consistency in information concerning data processing and purposes
DG5	Notifications about changed information of data processing, purposes, or involved actors
DG6	Transaction-specific consent to data processing
DG7	Reasonableness of the time required to provide consent in relation to the usage time

This section describes design knowledge that can advance consent at scale in digital ecosystems (RQ-4). Companies and regulators can consider these design goals in diverse ecosystem types. This is particularly true of DG7 as it is not yet covered by regulation. This should be considered in future design and regulatory discussions, because consent should continue to serve as a tool for information privacy in digital ecosystems.

5.3 Contributions in Other Research Contexts

This subsection emphasizes contributions based on collaboration and acknowledges the applicability of this dissertation's contributions and knowledge to other research contexts. Findings from these contexts informed this dissertation, assisting the acts of both understanding and advancing privacy in digital ecosystems.

5.3.1 The Accountability and Power of Platform Providers

This subsection looks at platform providers. The interdisciplinary collaboration at the intersection of law and IS by Kurtz et al. (2021) highlights that platform providers can be held accountable for personal data processing in the platform ecosystem that is unlawful according to the GDPR. The findings show that platform providers influence boundary resources in their respective configurations and interplay. In so doing, they determine the behavior of actors on the platform and they ways in which they can process personal data. The existing boundary resource composition and related designs need to be considered to specify the need for, as well as the legal design of, accountability for information privacy violations in the ecosystem. For example, the findings support that the platform provider must be classified as the data controller when the platform provider determines the only possible methods of offering applications for the service provider and accessing them by the users.

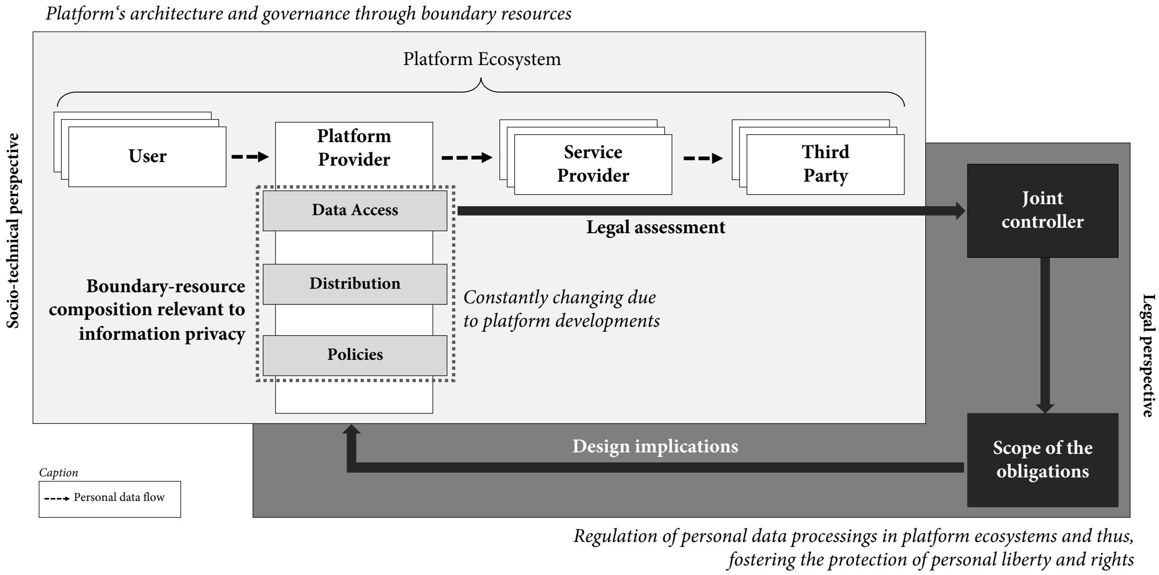

Platform‘s architecture and governance through boundary resources
Platform Ecosystem
User
Platform Provider
Service Provider
Third Party
Data Access
Distribution
Policies
Boundary-resource composition relevant to information privacy
Constantly changing due to platform developments
Legal assessment
Joint controller
Scope of the obligations
Design implications
Socio-technical perspective
Legal perspective
Caption
Personal data flow
Regulation of personal data processings in platform ecosystems and thus, fostering the protection of personal liberty and rights

Figure 8. Socio-Legal Assessment of the Boundary Resource Composition (Kurtz et al. 2021)

As Kurtz et al. (2021) highlight, the relationship between the boundary resources, the controllership according the GDPR, and related obligations is reciprocal (Figure 8). The relationship includes the fact that the boundary resource composition can trigger controllership. Conversely, the platform’s architecture and related boundary resource design affect the scope of obligations for platform providers in their role as controllers. It is important to note that the obligations depend on the individual case, taking into account the platform provider’s orientation and limitations. As a result, the platform providers can be accountable for data processing operations carried out by any actor within the platform ecosystem. An example would be when a platform’s design facilitated certain unlawful behavior. The findings show that a closed platform architecture leads presumably to the platform providers’ classification as a joint controller, which in turn can advance information privacy protection in digital ecosystems, as penalties of up to 4% (GDPR 2016, Art. 83 No. 5) of the platform provider’s annual worldwide revenues create a significant business risk.

In addition, Jacobs et al. (2021) show in joint work that platform providers are able to exercise power in ecosystems by determining the design of boundary resources and thereby influencing the behavior and practices of service providers and third parties in the platform ecosystem. This study builds on previous works on platform providers and their influence in platform ecosystems (Kurtz et al. 2019; Kurtz et al. 2021) and elaborates Mattis Jacobs’ perspective on the concept of power.

The exercise of power in platform ecosystems varies considerably in temporality (Jacobs et al. 2021). Jacobs et al. (2021) highlight that power can function *ex-ante*, i.e., platform providers can prevent design decisions from being implemented. Illustrations are the technical interface design that predetermine how actors can access data, and, more generally, which requirements service providers have to consider on the platform. Here, the provided boundary resources can constrain the application's design process. As platform providers mainly determine boundary resource design independently, they determine the app design of developers as well as developers' possible applications of VSD. Platform providers impose their ideas of the conception, weighting and operationalization of values, which they directly control, on to the whole platform ecosystem. These values obstruct or compel decisions that promote or demote the realization of information privacy. Thus, platform providers predetermine how human values like privacy are conceptualized and how privacy is operationalized by others in the ecosystem. In addition, another mode of exercising power functions *ex-post*. One example is the app review and approval process that platform providers use to include or exclude services.

This section contributes to understanding the platform provider's accountability and power. The boundary resources, in their respective design, configuration and interplay, show the platform provider's influence over determining actors' behavior regarding personal data processing in the ecosystem. Thus, they can either obstruct or force decisions that promote or hinder the realization of information privacy. At the same time, assessing the boundary resource composition can show whether platform providers are accountable for unlawful personal data processing in their platform ecosystems and, if so, to what extent.

5.3.2 Architectures of Data Ecosystems

Kurtz et al. (2021), in their research on platform ecosystems, identified that boundary resources are central objects that influence digital ecosystems' data flows and practices. Findings from the interdisciplinary collaborations on boundary resources in platform ecosystems contributed to the development of the architectural meta-model for data ecosystems (Burmeister et al. 2021). The conceptualization of a boundary architecture with related boundary objects is a central component of the meta-model for data ecosystems. The meta-model draws also on early considerations by Drews and Schirmer (2014). In the research process, Burmeister et al. (2021) jointly identified and positioned different model components. Concern areas and the categories of different stakeholder concerns have been discussed and developed to build the foundations for the meta-model.

The contributions of the meta-model and the architectural views on data ecosystems are helpful to understanding and breaking-down intertwined personal-data processing in complex data ecosystems. They allow the granular differentiation of those aspects and permit a flexible classification across the different architectures of individuals, boundaries and enterprises. For example, an instantiation that has been developed and improved visualizes the potential privacy impacts regarding a design decision to implement a third-party service. Integrating address autofill functions would use personal data for various purposes, meaning that a developer's decision to integrate a socio-technical component would have unintentional ecosystem-wide consequences regarding information privacy.

This section highlights the usefulness of developing an architectural lens with which to view data ecosystems in order to create transparency. The intersection of actors can be detailed using the introduced boundary architecture. Boundary architectures are helpful for modeling boundary objects not assignable to one actor. The instantiation of the architecture allows for much detail to be included and appraised. The architectural instantiation of a developer's design decision shows that the ease with which a third-party component with rich functions can be integrated can result in personal data diffusion with huge privacy implications.

5.3.3 Partnering in Digital Ecosystems

Discussions in context of two studies (Burmeister et al. 2021; Vogel et al. 2020) resulted in learning that privacy competes in a company with other aims or values, leading to ecosystem-wide privacy effects. It can, for example, be more efficient for a developer to implement software code from a third party than writing parts of the software code. Therefore, a design parameter was developed in the research context of online social networks. It characterizes privacy advances in relation to the prevention of personal data access and usage by actors outside the service system (Vogel et al. 2020). Thus, an organization's consideration of this design parameter—regardless of the case context—can prevent the diffusion of personal data by restricting data access only to actors and their activities if they are related to the service system's value propositions.

This section describes partnering in digital ecosystems. Crucial decisions regarding information privacy are already made on the micro-level of a company that can nevertheless cause ecosystem-wide effects. Limiting personal data usage to an organization's value proposition can result in the advancement of privacy.

5.4 Overall Theoretical Contribution

Different aspects of privacy-critical practices in digital ecosystems are highlighted in this dissertation, which also adopts interdisciplinary perspectives from ethics and law. In the following subsection, the contributions that are located on a broad spectrum are connected to each other. This subsection is divided into two parts: understanding privacy in digital ecosystems and the approaches to advancing privacy in digital ecosystems (cf. Figure 9). Besides these theoretical contributions, this dissertation includes regulatory and practical contributions to advance information privacy in digital ecosystems (see section 6).

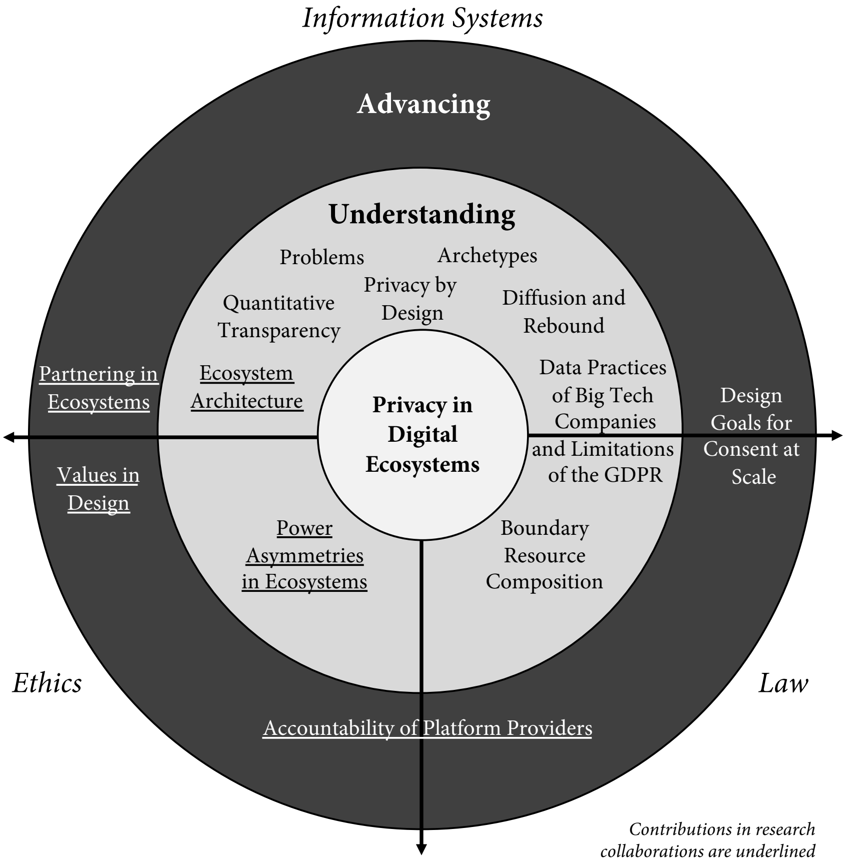

Information Systems
Advancing
Understanding
Problems
Archetypes
Privacy by Design
Quantitative Transparency
Diffusion and Rebound
Partnering in Ecosystems
Ecosystem Architecture
Privacy in Digital Ecosystems
Data Practices of Big Tech Companies and Limitations of the GDPR
Design Goals for Consent at Scale
Values in Design
Power Asymmetries in Ecosystems
Boundary Resource Composition
Ethics
Law
Accountability of Platform Providers
Contributions in research collaborations are underlined

Figure 9. Contributions in Context of This Dissertation

5.4.1 Understanding Privacy in Digital Ecosystems

The complexity and dynamics of digital ecosystems are linked to the sheer difficulty involved in generating transparency and understanding regarding data practices. This is true for individuals as much as organizations, as data processing in digital ecosystems is not necessarily visible or comprehensible. The investigation of eBay's ecosystem and its partners shows the size of a single ecosystem facing a user and how long it would take to read the available policies for providing informed consent.

Illustration of privacy-critical practices existing in digital ecosystems provided opportunities to make certain facts transparent and, at the same time, enabled researchers from a variety of disciplines to engage in dialogue. This approach allowed the exchange of information in diverse forms, such as using cross-impact matrices; illustrations of actors, processing activities and related data flows in service ecosystems; and the application of the architectural meta-model. It soon became apparent that problems in digital ecosystems do not only exist between the user whose privacy is at stake and another actor but also between interconnected actors. These aspects demonstrate the limits of unidirectional personal data flow and bilateral relationship models that dominate existing analyses and theories of information privacy research in the IS field (Benson et al. 2015; Conger et al. 2013; Karwatzki et al. 2017). They create the necessity to understand privacy in ecosystems from a systemic perspective that considers both a multi-actor and an actor-centric view.

In the multi-actor view, two important realizations are connected to each other. First, different archetypes characterize actor configurations that do not consider privacy according to the users' interests and possibly not according to other actors' interests in the ecosystem. One reason for this is that the understanding of information privacy does not have to be equal for all actors in an ecosystem, who may be driven by other and conflicting interests. In service research, Mustak and Plé (2020) highlighted that actors in ecosystems might have not congruent understandings of institutional arrangements (Kleinaltenkamp 2018; Plé and Demangeot 2020). This dissertation contributes knowledge to the case of privacy. Second, directly related to this is the insight that in these actor arrangements, different power structures prevail. In platform ecosystems, platform providers have a very influential role in the actor structure of individuals, platform providers, service providers, and third parties. Platform providers determine the design of boundary resources and related composition largely independently. They can assert their conception, weighting and operationalization of values, which they directly control, on to the whole platform ecosystem. Thus, while different understandings and interests of actors exist, powerful actors in ecosystems can support or inhibit values that affect their interests in digital ecosystems.

In the actor-centric view, there are three factors to consider. First, looking into an organization, crucial decisions are made regarding embedded socio-technical components. These decisions can have ecosystem-wide privacy effects. From an inter-organizational point of view, decision outcomes can be unintended and result, for example, from a developer's careless design decision. In addition, inter-organizational values such as privacy have also been seen as competing with other aims such as efficiency, which is improved by implementing third-party functions rather than developing the functions and write related code in-house.

Second, this dissertation shows that an actor’s connections to multiple service contexts generate an efficient ecosystem-connecting mechanism for accumulating personal data. Involvement in digital interaction leads to personal data access. As a result, companies embed configurations in digital service systems and decouple data from the original value proposition. The data then crosses service system boundaries for utilization in another service. The value proposition seems suitable as a possible spot for identifying actors that have amplifying effects on the diffusion of personal data in digital ecosystems. The consequence for information privacy is that personal data is used in different service contexts for totally different reasons. Data accumulation across service contexts is often opaque and only the company itself has detailed insights. Big Tech companies in particular systematically fostered involvement in diverse service systems. They proliferate throughout digital interactions as platform providers, service providers or third parties. At the same time, they provide many different value propositions in different contexts and relate these processing operations only to one privacy policy (for example, Google with the services of Google Maps, Android, Crashlytics, etc.).

The beginning of this dissertation highlighted that Contextual Integrity faces companies' overwhelming and systemic personal data practices (Nissenbaum 2019). As a framework, Contextual Integrity is excellent for focusing on single data processing operations, but it is less able to cope with unclear systemic personal data practices. This dissertation provides insights about systemic established paths of data aggregation and recontextualization, especially for Big Tech companies. These paths are deeply embedded in the proliferation of service-system crossings. However, it remains to be seen how well Contextual Integrity can take these systemic practices throughout the data's life cycle into account.

Third, access to personal data may result in adverse consequences (Karwatzki et al. 2017). This possibility is intensified by the fact that actors can use personal data in analytics and artificial intelligence, enabling powerful inferential transitions to information of interest (Nissenbaum 2019). The previously described personal data diffusions create opportunities for organizational rebound effects that are likely to be unanticipated by users. Accumulated data used in other service contexts thus lead to rebound effects on individuals in data ecosystems. The granularity of personal data can have an impact on the sensitivity of data and rebound effects. For instance, the more often location data are available to a company, the more accurate are their insights about the individual lives, hobbies or medical treatments of users (Martin and Nissenbaum 2019). Nevertheless, the connections between data accumulation and rebound effects are difficult to reveal due to the secrecy established around the companies' ecosystems.

In conclusion, this dissertation shows that individuals do not have full control or influence over what happens with their personal data in digital ecosystems. These findings suggest that individuals can rarely act with comprehensive self-interest regarding their privacy in ecosystems. Advancing privacy in ecosystems can, however, mitigate the problems and challenges found there.

5.4.2 Advancing Privacy in Digital Ecosystems

Having understood the different aspects of information privacy in digital ecosystems, the question of how to advance privacy in digital ecosystems emerges. This dissertation proposes different approaches to doing so. On the one hand, the accountability of platform providers from an ethical and legal point of view is highlighted. On the other hand, design knowledge regarding consent at scale and partnering in ecosystems is specified. These proposed approaches respond to the call for novel forms of privacy solutions in the IS field (Bélanger and Xu 2015).

Given the power asymmetries in ecosystems, powerful actors can promote or obstruct values. More specifically, powerful actors prescribe certain values and effects for their operationalizations and for service providers using VSD. This dissertation shows that platform providers have a very influential role in connecting users and service providers while applying their ideas to the whole platform ecosystem. The boundary resource composition creates a 'sweet spot' for privacy adjustment and regulation in ecosystems. By designing privacy-sensitive boundary resources, platform providers define privacy for involved actors and related personal-data practices. The regulatory implications show why platform providers are accountable for personal data processing in their ecosystems according to the GDPR (cf. 6.1). Various obligations can arise from this accountability and can thus raise the bar for privacy protection in the ecosystem. In this way, a platform provider that creates a balanced boundary resource composition can contribute to setting standards. In the long run, this practice can influence the GDPR's definition and range of constraints. Ultimately, platform providers can be crucial actors for advancing personal data protection within platform ecosystems.

Design knowledge can also mitigate privacy problems in digital ecosystems. In this regard, the new design goals for consent in digital ecosystems can improve the existing forms of consent. The reasonableness of the time needed to give consent, and transaction-specific data processing, are two design goals that contribute to revise the form of consent and regulatory requirements. The transaction-specific design goal is also able to address and prevent personal data diffusion into other service contexts. This is also addressed by a design principle concerning partnering in ecosystems. The consideration of the design principle in companies' decisions on actors' data access could assure the conformation of data usage to the value proposition of the service context.

6 Regulatory and Practical Contributions

The following section specifies the regulatory contributions made by this dissertation (specifically, the contributions that could further develop the GDPR and its application) and the practical contributions it makes to platform and service providers.

6.1 Regulatory Contributions Concerning the GDPR

The following contributions result from interdisciplinary collaborations with experts in the legal field and lead to valuable discoveries about data protection in multi-actor constellations (Kurtz et al. 2022 (under review); Kurtz et al. 2019; Kurtz et al. 2021; Kurtz et al. 2020). These regulatory contributions are divided into three parts.

The first describes important lessons about the limitations and future requirements of consent in digital ecosystems. The second identifies the contributions made concerning the roles proposed by the GDPR. (These contributions have been forwarded to the relevant service of the European Commission to be considered in the GDPR's repeating evaluations.) Finally, the third considers the GDPR's potential to regulate the service system-crossing practices, related data accumulation, and rebound effects by Big Tech companies.

6.1.1 Consent at Scale in Digital Ecosystems

The GDPR specifies the validity of consent when it is 1) freely given, 2) unambiguously stated, 3) for a specific purpose or set of purposes, and 4) based on an informed decision (GDPR 2016, Art. 4 (11)). So far, no precise interpretations of these requirements, especially in multi-actor-constellations, exist, as court decisions are mostly outstanding. In consequence, existing practices may under-apply GDPR’s specifications. However, it is only when privacy policies enable individuals to truly understand the specifics and potential consequences of offering up their data do they successfully serve their purpose. Kurtz et al. (2020) demonstrated that to give consent to use eBay involved providing consent to 906 partners, requiring individuals to spend 132.3 hours reading their policies. Nobody can claim that this level of temporal sacrifice is appropriate for providing consent—it leaves individuals *de facto* uninformed. Based on this analysis, Kurtz et al. (2020) suggest seven design goals that can guide organizations, researchers and regulators to reshape consent in digital service ecosystems. (Kurtz et al. 2020) compared the design goals with the requirements for effective consent specified in the GDPR

(GDPR 2016, Art. 4 (11)). While six of the seven design goals can be mapped to the requirements of consent, the design goal of reasonableness is not covered by the requirements.

Kurtz et al. (2020) show that two approaches can be helpful for addressing this design goal. First, the law can attempt to limit the sizes of digital ecosystems and thus the number of actors involved in data processing operations. While this approach could be helpful in limiting personal data sharing in ecosystems, specifying ecosystem limits would be extreme difficult, as this specification would need to consider the legitimate interests and fundamental rights of actors such as service providers and third parties. Second, to address "reasonableness", the design goal of uniformity may be helpful as it promotes machine-readable information for data processing operations. This approach would enable a new, technically supported form of consent. On this basis, automation appears plausible that would be able to achieve the different design goals. The reactivation of the "Platform for Privacy Preferences Project" would allow the quicker standardization of processing information and could establish machine-readable forms of consent, thereby simplifying privacy policies. In conclusion, because neither the design goals nor the GDPR-defined requirements are fixed, realizing the design goals efficiently could also raise the bar for what is expected by other companies (GDPR 2016, Art. 40).

6.1.2 Platform Providers as Joint Controllers

The GDPR specifies additional roles besides the two opposed parties (GDPR 2016, Art. 26-29). The regulatory idea behind this is to allocate responsibility to several parties at once. This is because multiple parties play important contextual roles in the sharing and use of personal data and so the risk of a responsibility vacuum arises. Joint controllership between multiple actors attempts to address this issue by allocating responsibility to all parties sufficiently involved in influencing personal-data processing (GDPR 2016, Art. 29).

As this dissertation and especially two of its component articles make clear (Kurtz et al. 2019; Kurtz et al. 2021), platform providers determine and control through their boundary resource composition the general ways in which personal data is processed in their ecosystems. The boundary resources' design influences the classification of a platform provider according to the terms of the GDPR. As Kurtz et al. (2021) make clear, the boundary resources, in their configuration and interplay, determine the platform provider's influence over the actors' behavior on the platform. As such, the boundary resources are central to the classification of platform providers as controllers. This classification identifies a role with different obligations, and Kurtz et al. (2021) concretize the abstract obligations of the controller role according the GDPR. The relationship between platform architecture, the included boundary resources and the level of control is central. This dissertation therefore contributes to the understanding both of boundary resources for a data-protective regulation of platform ecosystems and the effects of boundary resources on GDPR compliance when platform providers design them in a privacy-sensitive manner.

6.1.3 GDPR Limitations Regarding Big Tech Companies

The GDPR's and functions and roles may give the impression that every company and related personal data practice may be sufficiently regulated. However, the dangers stemming from the processing of personal data can vary greatly. Not all of them are related to the individual processing operation itself or its immediate environment (i.e., the personnel or the technical architecture surrounding it). In principle, regulators would dissect and analyze data processing operations independently according to the GDPR. However, as the paper on the practices of Big Tech companies emphasizes (Kurtz et al. 2022 (under review)), a danger can arise from the sum of different processing operations and the quantity of processed data. In this circumstance, a regulatory vacuum could occur for two distinct reasons.

Firstly, under the GDPR, an entity processing different types of personal data in various stages and situations is a controller at each of these instances and for each process. However, as indicated, the real danger may result from more than the sum of its (data processing) parts. The danger of privacy violations can be enhanced by combining the processing operations or the variety of contexts from which the affected data stem. The GDPR tries to consider this heterogeneity of sources of danger by placing obligations on data controllers that account for the broader processing environment. Secondly, not every critical participation act is necessarily covered by the GDPR. Big Tech companies tend to influence other data controllers in ways that shape and evolve the accumulation and proliferation of personal data. They enter data processing circumstances as platform providers or third parties due to their market power, exhibiting a privacy-affecting behavior that is not taken into account by the GDPR's traditional roles and their obligations.

These points show that despite modernization efforts on the legislative and judicial levels, a legal vacuum remains that is inhabited by Big Tech companies that do not fit the 'single individual role' model pursued by the GDPR. The isolated view of a single processing operation and its related legalities as defined by the GDPR contrasts with the repeating practices identified in this research. Those practices involve countless numbers of data processing operations in diverse roles and by diverse actors across service contexts. For the GDPR to cover these phenomena, a new actor perspective and interpretation is needed to cope with companies' accumulation and utilization practices, particularly when Big Tech companies are participants. Regulators can consider these results in three ways. First, through court decisions and data protection authorities interpretating and concretizing the GDPR on an EU or national level. Judgments by the European Court of Justice (ECJ) already show the legal ramifications of joint controllership and its related obligations. Second, through constant re-evaluation, development and improvement of the GDPR and its obligations and roles informed by feedback from different stakeholders. The GDPR itself endorses such endeavors, as seen in its provisions regarding regular evaluations (GDPR 2016, Art. 97 No. 1). Third, by applying other regulatory frameworks from outside data protection that follow a similar goal, thus bringing their regulatory toolbox to the table. Antitrust law is one field in particular that offers valuable insights.

6.2 Practical Contributions

This section describes the practical contributions this dissertation makes for platform providers and service providers. Platform providers can use these insights to pay more attention to the complex and continuous effort to balance the aspects of platform generativity, services provider and third party freedoms, and users' information privacy. Privacy-related obligations stemming from regulations can foster the 'securing' function of the boundary resource and can cause platform providers to design resources in a privacy-friendly manner. The inclusion of user interests and rights must be considered and weighed against other aims. Limited consideration of a single aim or group would be counterproductive, and compromise other groups' aims or requirements when developing a balanced platform architecture. Conversely, finding innovative and efficient solutions can shape the content and scope of regulatory obligations by demonstrating best practices.

When indications of privacy-critical behavior by service providers or third parties exist, tuning boundary resources can help prevent information-privacy violations. For example, the data access boundary resource can be developed to limit the processing operations on a technical level according to the requirements of the platform policy. Alternatively, the app review process can be tuned to verify whether an app's code violates the platform policies at any point. Boundary resource composition is important in increasing the overall efficiency of information privacy. Platform providers can therefore advance privacy by design in platform ecosystems. This advance could be supported by boundary resources that predefine how developers account for other human values in their applications. Doing so would shape value-sensitive ecosystems proactively and comprehensively.

This dissertation also has implications for service providers. Due to their partnering with other actors, service providers must address users' privacy interests far more often than would occur in a dyadic relationship. If a service provider unintentionally involves a party in privacy-critical practices, the provider must identify the reason why this happens. This dissertation shows different possibilities, such as conflicting values or aims within a company. If a company wants to advance its ecosystem in a privacy-sensitive way, the different types of design knowledge or the architectural meta-model may prove useful in handling the complexities of actor involvement. With the help of the model, transparency can be created that reveals involved third parties, related data processing and defined purposes. A subsequent assessment could prove whether the practices of third parties fit the service providers' privacy understandings or not. In this regard, data protection impact assessments would be extremely relevant. They could first assess the impacts when new partners become involved, and later could be repeated to assess partner dynamics in such aspects as their practices, acts or purposes.

7 Limitations

There are limitations to the findings and the methodology of this dissertation. The individual articles may incorporate further limitations, but those are specified in the respective texts.

First, ecosystems evolve dynamically over time, and that evolution may occur very quickly. For example, in the study of eBay's ecosystem (Kurtz et al. 2020), the ecosystem and its related partners changed while the authors were writing the article. Such dynamic changes can lead to problems regarding the long-term accuracy of some results. However, the generalized findings remain intact as they are detached from the specifics of numbers of actors etc. Second, the GDPR is primarily considered privacy regulation. Nevertheless, the GDPR is currently the most central regulation for data protection in the EU and it also applies to companies outside the EU when they process the personal data of EU citizens. Further studies could consider other regulations to develop a more intercontinental view of data protection. Third, one central aspect of this dissertation is the investigation of privacy scandals involving multiple individuals and actors that have been published in the media. However, research shows that individuals' perceptions of privacy differ (Kumaraguru and Cranor 2005; Westin 1991). On an individual level, not every investigated personal data practice is perceived as critical for privacy. However, due to the cross-media treatment of various scandals and the interviews with affected persons that were examined, it is assumed that the criticized practices are considered deserving of criticism by individuals as well as society more generally. Fourth, this dissertation offers a broad set of findings resulting from its explorative strengths. This breadth leads to the limitation that some determinations have been insufficiently studied. In future research, using the DGs during a design science process and with the involvement of regulators to enable consent at scale seems promising. However, adopting a more specific focus would have limited the explorative process and limited the breadth of the results that arose.

This dissertation also has methodological limitations. The studies that comprise this dissertation build on qualitative research and thus, as Myers (2019) makes clear, they depend upon the researchers' skills in applying relevant methodologies. They may also be subject to personal biases. To address these concerns, multiple researchers were involved in the collection and analysis of data, and reliability measures were considered. Secondary data was used to explore the cases that demonstrated personal data practices critical for information privacy. The accuracy of the description of the cases may be affected by the news editors' or authors' understandings, interests, and conscious or unconscious biases. Thus, different media outlets and diverse data sources and types were used to triangulate data. While a wide range of document types have been used, future research could attempt to gain greater access to internal data from companies, to better understand (for example) boundary resource development.

8 Implications for Further Research

This dissertation identifies promising avenues for further research regarding information privacy in the IS field, and in service, platform and data ecosystems. In addition, as this dissertation shows, interdisciplinary studies can help researchers to understand and assess novel socio-technical phenomena. However, interdisciplinary studies on information privacy are still scarce in the IS discipline. With the concept of boundary resources, a sweet spot has been identified at the intersection of the IS, legal and ethical fields. Here, the interaction of researchers across disciplines resulted in novel solutions to problems that are not confined to the IS field. In the future, most spheres of human activity will contain personal data; new questions will arise regarding the rules that govern societal and individual well-being in the digital realm. Interdisciplinary research can contribute to addressing the challenges of fostering human values in digitized societies.

8.1 Information Privacy in the IS Field

Research on information privacy in the IS field should continue to consider digital ecosystems that include diverse personal-data practices. One possible way to do this would be to consider a new understanding of information privacy that reflects the conclusions of this dissertation. Shifting from a solely individual-oriented definition of controlling or restricting information about oneself to an ecosystem-oriented one may offer a prudent way forward. A novel definition of information privacy could be “the processing of personal data according to the interests of the person to whom the data belongs”. Using this definition, actors in ecosystems would have to identify and consider individuals' interests so as not to violate their privacy. Interests are appropriate because individuals are not always able to comprehend what happens with their personal data in digital ecosystems. An individual may not expect third-party actors and actions. However, individuals could easily identify and express what they prefer, such as a smoothly running application. This definition would acknowledge that different, even conflicting, interests exist among the diverse actors involved in ecosystems when compared with the interests of the individuals to whom the personal data belongs. This new approach would pave the way for research on investigating questions of how to take privacy into account in multi-interest settings, from technical, legal and ethical perspectives and on micro- and macro-levels. On the micro-level, questions could address the issues around the developer's decision to incorporate third-party services. On the macro-level, research could address platform providers’ pursuit of generativity in the design of the platform’s boundary resources.

In addition, investigations of individuals' actions, motivations, behavioral economics or psychology that consider the ecosystem in which they operate may prove a fruitful line of inquiry. Research questions might address whether individuals are willing to share personal data used across service contexts in ecosystems or whether individuals can cognitively comprehend and assess the privacy risks and rebound effects in digital ecosystems.

Finally, information privacy and digital ecosystems could factor in design-oriented research. The newly developed design goals for consent at scale are the first step in such a direction. Other studies can use these goals and instantiate and evaluate them in different ecosystem contexts. Researchers who use the new understanding of privacy described above can make substantial contributions to design science solutions.

8.2 Service Ecosystems

This dissertation identifies diverse problems in service ecosystems concerning information privacy, showing important possibilities for future research. First, practices concerning personal data are not transparent. Thus, methods to create transparency in, and understanding of, the inner workings of ecosystems should be further considered in future research. Modeling personal data practices from architectural perspectives (Burmeister et al. 2021) can create important foundations for future research. Further development of the illustrative privacy scandals using service or data blueprint could be helpful. While an individual’s visibility of data processing practices has already been established, the visibility possessed by other actors involved in the ecosystem could be addressed. For example, service providers' practices are not necessarily transparent to platform providers. This is also true for the relationship between service providers and third parties.

Second, different actors interacting in service ecosystems share institutional arrangements but do not necessarily share the same value understandings. Thus, service research needs to address that actors in service systems do not limit their personal data usage to providing the value proposition but also use the data across service systems. Investigating actors who have multiple roles or service context crossings may be productive for future research. Research is also needed on how to advance values in ecosystems. On the micro-level, understanding and supporting important processes such as software developers’ decisions to embed third-party plugins may be vital in understanding values adopted in (and by) service ecosystems.

Third, the power in digital ecosystems is not necessarily equally distributed. Researchers could investigate the power relations between actors in digital ecosystems that can affect the advance or hindering of information privacy and other human values. Here, platform providers are key actors that decide boundary resources in platform ecosystems. Power differences also exist between service providers and third parties. Finally, the power of Big Tech companies acting as third parties should be addressed. For example, the integration of buttons provided by Big Tech companies offers an interesting case regarding power differences with ecosystem-wide consequences that researchers could investigate.

8.3 Platform and Data Ecosystems

This dissertation shows that the design of a platform and related boundary resources can have a fundamental effect on users' privacy. Platform research already contributes to understanding platform providers' governance mechanisms by using the concept of boundary resources (Eaton et al. 2015; Ghazawneh and Henfridsson 2013). Further investigations are required to determine the connection of more open and hybrid platform architectures to information privacy.

From the perspective of a platform provider, privacy regulations such as the GDPR can affect boundary resources design in platform ecosystems. Platform providers must take into account the regulations when designing their platform in order to abide by these regulatory constraints. Thus, studies could address how platform providers can better design the boundary resource of data interfaces to prevent privacy-violating processing operations. In addition, studies could address how to tune the app review process to assess whether an app's code conforms to or conflicts with the privacy statement or platform policies. Big Tech companies acting as platform providers could potentially be obligated to advance information privacy protection in their platform ecosystems. Research on the possibility of platform providers restraining other Big Tech companies acting as service providers or third parties seems promising. In addition, the development of entirely new boundary resources could be relevant for future studies. Studies could contribute to understanding the balance between generativity on one side and the interests of users on the other.

In recent studies on data ecosystems, the ability of an actor to have multiple roles has been identified (Oliveira et al. 2019). The results of this dissertation extend the knowledge regarding the roles of Big Tech companies. Future research might address how other, smaller companies use different roles for data accumulation in data ecosystems. In addition, third parties base their business model on their involvement in many services. Future research on data ecosystems could study such actors and the consequences of their practices on information privacy in data ecosystems.

9 Article No. 1 (Kurtz et al. 2018b)

Kurtz, C., Semmann, M., and Böhmann, T. Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Proceedings of the 24th Americas' Conference on Information Systems, New Orleans, 2018.

Abstract

As the General Data Protection Regulation (GDPR) within the European Union comes into effect, organizations need to cope with novel legal requirements regarding the processing of user data and particularly how other, in the service integrated, organizations can process these. Information systems (IS) and their design as mashing up services of various providers (ecosystems) is state of practice. The GDPR raises for companies the question of how they can ensure that operations conform with external data processors according to the regulation. The approach of Privacy by Design (PbD), which is also included in the GDPR, offers for organizations a way to operationalize these legal requirements. Therefore, we conduct the first, rigorous, and systematic literature review of PbD. Specifically, we focus on works that seek implementation of PbD in organizations, located in ecosystems. The results show a surprising dearth of research in this field, although GDPR explicitly emphasizes this critical issue.

9.1 Introduction

The GDPR, enforced in May 2018, is a regulation on data protection in the European Union. The regulation serves for the protection of the human right to privacy in the digital world. The accumulation of numerous data about an individual and the resultant data processing can have negative consequences on individual privacy. Therefore, the new regulation aims to protect data in order to protect privacy (Danezis et al. 2015). The GDPR integrates the concept "Data protection by design and by default" (Regulation, 2016, Chapter 4 Article 25). In this article, it is stated that the data controller must implement in the context and within the given conditions technical and organizational measures for data regulation by default. The pre-existing approach of PbD points out that privacy should be a proactively paramount consideration at the design stage of IS Cavoukian (2009). Using this approach, the goal can be achieved of protecting users' privacy. The framework of PbD suggests that such an approach can be subdivided more specifically. Basically, it proposes the following seven foundational principles (Cavoukian, 2009):

1. Proactive not Reactive; Preventative not Remedial: By proactively adopting strong privacy practices, events which have an invasive effect on privacy are anticipated and prevented.
2. Privacy as the Default Setting: Personal information is by default protected without the need for the user to take any action. The fair information practices – "Purpose Specification", "Collection Limitation", "Data Minimization", and "Use, Retention and Disclosure Limitation" – are taken into account.
3. Privacy Embedded into Design: Privacy is considered in the design and architecture of IT systems and business practices as a core functionality. It should be embedded holistically in terms of considering the context, integrative as respecting all stakeholders, and creative as re-defining previous designs.
4. Full Functionality – Positive-Sum, not Zero-Sum: All legitimate objectives of an organization are achieved with full functionality. A multi-functional solution is investigated where no trade-off is performed to the detriment of privacy.
5. End-to-End Security – Full Lifecycle Protection: Strong security actions are taken throughout the entire lifecycle. The management of personal information and included principles are carried out, such as destroying data at regular intervals.
6. Visibility and Transparency – Keep it Open: All stakeholders in business practices and technologies operating according the promises and objectives. For this, visibility and

transparency are needed for establishing accountability and trust. In this principle, the three fair information practices – "Accountability, "Openness", and "Compliance" – are considered.

7. Respect for the User – Keep it User Centric: The design should always consider the interests and needs of users. This principle implies the four fair information practices: "Consent" – users' consent regarding collection, usage, and disclosure of personal information; "Accuracy" – the need for complete, correct, and actual personal information; "Access" – providing user access to their data; and "Compliance" – interpreted as organizations having to take actions and communicating them regarding users' privacy.

Taking these principles into account, the approach of PbD Cavoukian (2009) has already been used as a method to implement privacy in organizational actions. Thus, the concept was already in place before the GDPR came into force. As described above, "Data protection by design and by default" (Regulation, 2016, Chapter 4 Article 25) is now legally binding. Therefore, this review aims to examine the state of implementation of PbD because it is a way to operationalize the legislation (Regulation, 2016, Chapter 4 Article 25). Another aspect of data regulation in the GDPR is to regulate data processing (Regulation, 2016, Chapter 4 Article 28). It is specified that organizations bear responsibility with regard to actions taken by "processors". These can be both internal and external actors of an organization who process data (Regulation, 2016, Chapter 4 Article 25). This regulation is important for organizations because the ongoing dissemination of interconnected service systems contain several organizations in the value chain in terms of ecosystems (Ostrom et al., 2015; Peters et al., 2016). Also, research on service has shifted from focusing on single services towards systems of services (Spohrer et al. 2007, Vargo and Lusch 2011, Chandler and Lusch 2015, Böhmann et al. 2014). This systemic ecosystem perspective implies a dynamic configuration across multiple actors that jointly integrate resources to create value for the beneficiary (Lusch and Vargo 2014). Due to these structures, there is a need for solutions and ways that companies can ensure that the embedded, external data processors act according the GDPR. In this article, we aim to determine whether the above-mentioned PbD principles have been a guidance so far for organizations. Therefore, we conduct the first, rigorous and systematic literature review of the application of PbD, where we focus on studies that seek implementation of PbD in organizations. In doing so, we concentrate on Principle 6 of the PbD framework. This principle calls for all stakeholders, whether internal or external, to act in accordance with the framework of PbD. This is in line with our focus on the regulation regarding data processors (Regulation, 2016, Chapter 4 Article 25). In this respect, the introduction is followed by the data collection section. In this passage, the characteristics of this literature review are specified, followed by the data analysis. Building on the findings, we analyze the literature with a focus on Principle 6 of PbD regarding the handling of data processors. It is followed by a discussion where a research agenda is derived. The paper finishes with a conclusion and aspects for future research.

9.2 Data Collection

In this paper, we explore the articles on PbD (Cavoukian, 2009) with the focus placed on studies which deal with the implementation of Principle 6. We aim to inform researchers about the current state of existing PbD studies by following a rigorous review process (Webster and Watson, 2002; Vom Brocke et al., 2009).

In Table 1, the characteristics of this literature review are highlighted: The focus (1) lies on the research outcomes and applications in the context of PbD with the goal (2) to clarify central issues which have been worked on so far. A conceptual and methodological organization (3) is chosen to cluster works that relate to the touch points in the ecosystem. We take up an espousal position (4) which is reasoned because the purpose is to summarize the studies and also to synthesize the research outcomes. Our review and findings address the entire IS community (5) but also researchers of other fields, bridging the gap between philosophers, lawyers, and IT researchers' results in interdisciplinary work. Furthermore, practitioners in terms of organizations are also addressed. The level of coverage (6) is exhaustive with selective citations, considering relevant sources regarding PbD but describing only one sample.

Table 1. Taxonomy of the literature review (following (Cooper, 1988, p. 109))

<table>
<tr><th>Characteristics</th><th colspan="6">Categories</th></tr>
<tr><td>focus</td><td>[✓ research outcomes]</td><td colspan="2">research methods</td><td colspan="2">theories</td><td>[✓ applications]</td></tr>
<tr><td>goal</td><td colspan="2">integration</td><td colspan="2">criticism</td><td colspan="2">[✓ central issues]</td></tr>
<tr><td>organization</td><td colspan="2">historical</td><td colspan="2">[✓ conceptual]</td><td colspan="2">[✓ methodological]</td></tr>
<tr><td>perspective</td><td colspan="3">neutral representation</td><td colspan="3">[✓ espousal of position]</td></tr>
<tr><td>audience</td><td>[✓ specialized scholars]</td><td colspan="2">[✓ general scholars]</td><td colspan="2">[✓ practitioners/ politicians]</td><td>General public</td></tr>
<tr><td>coverage</td><td>exhaustive</td><td colspan="2">[✓ exhaustive and selective]</td><td colspan="2">representative</td><td>central/ pivotal</td></tr>
</table>

To explore the state of research regarding PbD, we conducted an in-depth review of the literature in several stages. We constructed a rigorous literature review in five steps:

1. We identified the databases ACM Digital Library, AISeL, EBSCO Business Source Complete, EBSCO EconLit, IEEEXplore, ProQuest, and ScienceDirect. With the selection of these databases, we covered a broad set of research areas.

2. In the search terms, the concept of PbD is considered. The method of "privacy enhancing technologies" is not considered as a keyword - it deals with the technical method of implementing privacy (Koops and Leenes, 2014). The method of "Privacy Impact Assessments" for evaluating the effects of a project on privacy is also not used as a keyword (Wright and De Hert, 2012; Kung et al., 2015). Overall, PbD stretches the frame across them due to the application in technologies, architectures, business operations, and networked information ecosystems (Cavoukian, 2009).

3. The identified databases have been queried on the basis of a search. All articles were scanned, which take the search term "Privacy by Design" into account in the title, abstract or keywords. In addition, peer-reviewed articles should be considered already as high-quality classified which was not possible for three databases. Table 2 shows the number of articles per database that have resulted.

Table 2. Articles per Database

Database	ACM Digital Library	AISeL	EBSCO Business Source Complete	EBSCO EconLit	IEEE Xplore	ProQuest	Science Direct
Peer Reviewed	No	Yes	Yes	Yes	No	Yes	No
Hits	39	2	48	5	74	38	20

4. The next step included delete duplicate articles, which resulted in 188 articles being reviewed (Table 3).

5. The 188 articles were checked in the title, abstract, keywords, as well as for whether the concept of PbD (Cavoukian, 2009) was taken into account. The articles that were only descriptive regarding the concept and take no form of implementation into account, were removed. This resulted in 96 studies (Table 3).

Table 3. Selection Process

Hits	To review	Reviewed (Full-Paper)	To analyze
226	188	96	39

6. Out of the 96 articles, a deeper analysis was carried out where the entire article was checked. In addition, the articles from which another picture existed after determining that the title, abstract, and keywords were removed. This removal process also included works which only incidentally dealt with the concept in the article. Also, papers were excluded which indicated that they considered

PbD, however focused on Security by Design. Furthermore, studies were sorted with respect to unsuitable format (e.g. one-sided or workshop descriptions). In this literature review a backward and forward search was not carried out due to the fact that the focus was on articles which emphasize designing or implementing PbD artifacts. After completion of the above selection procedures, 39 articles remained (Table 3) which are analyzed below.

9.3 Data Analysis

Based on the papers identified as relevant, we conducted a thorough analysis. We applied four categories to differentiate the 39 papers. First, the sector was taken into account. We identified the sectors “Advertising”, “Health”, “Infrastructure”, “Security”, “Social”, and “Transport”. Furthermore, the category “Multiple” is assigned if more than one sector is considered in the article. Moreover, studies which considered no sector are assigned to the category “General”. Second, the research background which the authors refer to is presented. This classification is divided into the categories “Application and Platform Design”, “Application Design”, “Architecture Design”, “Platform Design”, “Service Design”, “Software Development”, “Software Engineering”, “System Design”, and “Technology”. The category “Technology” contains the articles which do not consider the implementation from a technical, computer science point of view, but rather from a social or legal viewpoint. The third category represents the artifacts developed within the papers. In doing so, we refer to the common categories of artifacts in designing science research (March and Smith 1995): “Concept” (Con.), “Model” (Mod.), “Method” (Met.), and “Instantiation” (Ins.).

Table 4. Categorization of relevant articles

Article	Sector	Artifact				Coverage Principle 6				
		Con.	Mod.	Met.	Ins.	PI	OS	DD	De	Ev
Aïvodji et al. (2016)	Transport				X					
Bier and Krempel (2012)	Multiple		X	X						
Caiza et al. (2017)	General		X	X						
Callegati et al. (2015)	Transport		X	X						
Cavoukian et al. (2012)	Security		X	X	X	X	X			
Cavoukian and Kursawe (2012)	Infrast.			X	X	X	X			
Colesky et al. (2016)	General		X	X		X	X			
Degeling et al. (2016)	General		X	X						
Diamantopoulou et al. (2017)	General			X	X	X	X			
Diver and Schafer (2017)	General			X						
Hartzog and Stutzman (2013)	Social		X	X		X				
Jaime et al. (2015)	Security				X	X	X			
Jutla et al. (2013)	General			X	X	X	X			
Jutla and Bodorik (2015)	General		X	X	X	X	X			
Kroener and Wright (2014)	General			X		X				
Kung et al. (2011)	Transport			X		X				

Kung et al. (2015)	Security		X	X		X				
Liegl et al. (2016)	Infrast.		X	X	X	X				
Martín et al. (2014)	General		X	X						
Métayer (2013)	Transport			X						
Milutinovic and De Decker (2016)	Health		X	X		X				
Mohammad et al. (2015)	Infrast.				X					
Morizio (2016)	General		X							
Morton and Sasse (2012)	General		X	X	X	X				
Nordgren (2015)	Health		X			X				
Notario et al. (2015)	General			X		X	X			
O'Connor et al. (2017)	Health			X		X	X			
Perera et al. (2016)	General			X	X	X	X			
Popescu and Baruh (2013)	Advertising		X	X		X				
Romanou (2017)	Multiple		X	X		X				
Rowan and Dehlinger (2014)	General			X		X	X			
Rubinstein and Good (2013)	Multiple		X	X		X				
Schoonmaker (2016)	Transport		X			X				
Siljee (2015)	General			X		X				
Sun et al. (2013)	Transport		X	X	X					
Vallez et al. (2017)	Social				X					
Van Der Sype and Maalej (2014)	General			X		X	X			
van Lieshout et al. (2011)	Infrast.			X		X				
Ye et al. (2014)	Social				X					

An article could include more than just one artifact. The fourth classification determines how the above-mentioned sixth principle, respectively the data processing of third parties, is considered in an article. For identifying the categories, we take the Design Science Research Methodology Process Model into account (Peffers et al., 2007). Here, five of the six common design process elements (excluding "Communication") are regarded as a possibility to determine the consideration dealing with third parties in an article. The first category "Problem Identification (PI)" points out if in articles an awareness in respect of operating with third parties is mentioned. The second category "Objectives of a Solution (OS)" is assigned when authors derive requirements for the integration of data processors in their study. An article belongs to the third category "Design and Development (DD)" when the requirements are modeled and developed in the form of, for example, system design or software development. The fourth category "Demonstration (De)" represents that in an implementation, the handling to data processors is regulated. This can be done by a proof of concept or a demonstrating a prototype. The fifth category "Evaluation (Ev)" is allocated to an article if the regulated interaction with third parties is implemented in a continuous real scenario.

In the following, we will provide an overview of the articles, their classifications, and connections between them (see Table 4). First, we delve into the sectors of the articles to analyze which are covered. It is noticeable that 16 articles are classified as not sector specific ("General"). In contrast to this, the other articles take different sectors into account, including sector-specific requirements. This is necessary because no one PbD artefact fits all sectors' solutions. Three of the articles consider several sectors. In total, the coverage of sectors is very specific and areas such as insurance are not covered by the 39 articles at all. Thus, because GDPR is independent from sectors, general approaches seem worthwhile developing.

The second classification indicates what type of artifact respectively has been covered in an article. The majority of papers – 26 of the 39 – propose at least two artefacts. It should also be noted that 14 studies include instantiations in the form of, for example, proof of concepts or prototypes. Unsurprisingly, none of the papers propose concepts, because PbD is considered as a guiding concept in the papers. Nevertheless, this shows that no further conceptual development has taken place since the initial publication of PbD.

We analyzed the coverage of principle 6 as the responsibility for actions taken by third parties, referred to in the GDPR as data processors, in the last category. Surprisingly, 13 papers do not take third parties into account and instead focus solely on internal stakeholders. Because the aim of this research is to explicitly focus on design-oriented research, DSRM helps to identify to what extent the papers contribute to research on PbD. The results show that 16 papers address the issue of data processing by third parties as relevant and potentially impacting privacy. An additional 12 papers extend this problem and derive requirements on how to deal with third parties as data processors. None of the existing research efforts currently go beyond these requirements. Consequently, no artifacts resulting in a design and development phase are proposed, nor are demonstrations or structured evaluations.

Based on this initial analysis, we further analyzed all papers that explicitly dealt with the problem identification (Table 5) as well as objectives of a solution (Table 6) for third-party data processors. The articles which relate to "Problem Identification" mainly involve the research background "Technology" (8 of 14). The reason for this is that the category "Technology" represents the above-mentioned social or legal viewpoint of the studies, where the focus is not on specific technical implementation. Due to this focus, the classification of the articles within the DSRM process do not go beyond the problem identification. Overall, it can be said that the listed articles give mainly an indication that the interaction with third parties should be regulated without adding more details on how such regulation should be implemented (Table 5).

Table 5. Problems identified regarding principle 6

Article	Research Background	Problem Identification regarding Principle 6
Hartzog and Stutzman (2013)	Technology	Design of four principles for protecting online information, the problem of third party requests in the context of social technologies are mentioned
Kroener and Wright (2014)	Software Engineering	Addressing of implementation guidelines for software engineers in which the accountability of third parties has to be regarded

Kung et al. (2011)	Application Design	Examination of three principles within the PbD concept in the context of intelligent transport service applications; transparency mechanisms for handling third parties
Kung et al. (2015)	System Design	Development of a surveillance system with several third parties, requirement is raised that certifiers to proof third parties and their data protection mechanisms
Liegl et al. (2016)	Technology	Approaches for ethical, legal, and social issues in information technology are addressed in a case study, call for considering third parties in this context
Milutinovic and De Decker (2016)	System Design	System proposal in eHealth sector, third parties are included in the system design
Morton and Sasse (2012)	Technology	Framework of activities for effective privacy practice, problem identification regarding the transfer of customer information to third parties without permission
Nordgren (2015)	Technology	Analysis and discussion of ethical implications in personal health monitoring, transmission of data to third parties is addressed as critical
Popescu and Baruh (2013)	Technology	Description of two privacy-aware proposals advancing the mobile marketing ecosystem, consideration of third parties processing user data
Romanou (2017)	Technology	Demonstration of the need to implement the PBD concept, problem of third parties respectively in the industry of data selling is depicted
Rubinstein and Good (2013)	Technology	Derivation and illustration of several privacy principles, modular software which originates a variety of third parties is criticized
Schoonmaker (2016)	Technology	Assessment to the area of autonomous vehicles, problem of third parties is indicated who collect and use data in the context of location-based services
Siljee (2015)	Software Engineering	Examination of two privacy transparency patterns, possibility to depict in these patterns third parties and which data they process
van Lieshout et al. (2011)	System Design	Conducting a case study to explore the potential impact of PbD. The authors name third-party services as potential privacy risks

The articles which contain "Objectives of a Solution" go one step further in the design process than the articles in the category "Problem Identification" mentioned in the above section. These articles take into account the identification of practical objectives and requirements that must be met (Table 6). However, several requirements are named that correspond to the fact that several objectives can be derived from the seven principles of PbD. It becomes apparent that solely one paper focuses on the consequences for the protection of users' data when implementing third parties in software development (Van Der Sype and Maalej, 2014). All other papers tackle the issue of third parties besides general design of systems. Accordingly, derived requirements do not extensively cover privacy issues.

Table 6. Objectives of solutions regarding principle 6

Article	Research Background	Objectives of a Solution regarding Principle 6
Cavoukian et al. (2012)	System Design	Design of a biometric encryption system, description of a control which enables the anonymity of users in the context of data processing in third-party databases
Cavoukian and Kursawe (2012)	System Design	Requirements in the case of smart meters are presented, objectives how to handle third parties are derived
Colesky et al. (2016)	Software Engineering	Exploration of PbD strategies, strategies describe the handling of third-party organizations implemented in systems

Diamantopoulou et al. (2017)	System Design	Proposal and Description of privacy process patterns, requirements regarding third parties are derived in these patterns (e.g. unlinkability and undetectability)
Jaime et al. (2015)	System Design	Design of a privacy-aware surveillance system, access limitation and disclosure of data to third parties are listed as requirements for the system design
Jutla et al. (2013)	Application Design	Description of privacy extensions for visualizing privacy requirements, requirement is listed to identify and to handle third parties
Jutla and Bodorik (2015)	Architecture Design	Description of a privacy architecture, techniques are listed and examined for preventing third-party injection
Notario et al. (2015)	System Design	Examination of a methodology for privacy engineering, risk-based privacy analysis, impact assessment as solution to create transparency with regard to third-party risks
O'Connor et al. (2017)	Technology	Practical approaches for designing IoT technologies within the health domain, appointment of a user agreement requirement to provide third parties with user data
Perera et al. (2016)	Application and Platform Design	Set of guidelines to assess privacy capabilities and gaps of IoT app. are proposed, problem claims that third parties can combine personal details through the aggregation from multiple sources - objectives of a solution are as a guideline derived
Rowan and Dehlinger (2014)	Software Development	Overview of the tool for the privacy policy auto-generation, data collection, and procedures in the interplay with third parties are included
Van Der Sype and Maalej (2014)	Software Development	Derivation of requirements and guidelines for app developers on how to contribute to the protection of users, examination with focus on implementation of third parties

By taking the other classifications in the context of the coverage of principle 6, different findings are examined. In the classification of sectors, it is evident that in all mentioned sectors, the category “Problem Identification”. Thus, in all mentioned sectors exist the relevance of solutions taking third parties into account. There are two findings in the classification of the research focus regarding the regulation of third-party processing. First, nine articles which have the research focus “Technology” cover principle 6. More precisely, eight of them are categorized as articles which respond to the “Problem Identification”. This means that the articles which have the research focus “Technology” are rather descriptive works, which can be assigned less to the implementation and realization in computer science. Furthermore, articles with the focus “Service Design” or “Platform Design” do not cover the handling regarding third parties at all.

9.4 Discussion

At the beginning of this article, we discussed the GDPR with which the goal is to be achieved to protect privacy in the form of data regulation. In the main focus of our review stands the involvement of external data processors in organizations. The question was whether the above-mentioned principles of PbD, particularly in consideration of principle 6, have been an operational guidance so far for companies? An effort was made to answer this question with the help of the Design Science Research Methodology Process Model. According the results of the analysis, none of the reviewed articles go beyond the second process step "Objectives of a Solution (OS)". This means that the process steps “Design and Development”, “Demonstration”, or “Evaluation” have not yet been covered. Thus, based on the PbD approach exist no studies which implement handling third parties on an advanced level. This is a critical point because regulations for data protection by design and by default in combination with the responsibility of organizations for actions taken by data processors in the GDPR will enter into force in May 2018. Furthermore, by analyzing the articles, further shortcomings become apparent. Thus, we derive a research agenda to examine ways for organizations to be compliant with the requirements raised by GDPR.

Table 7. Research agenda for the implementation of PbD regarding data processors

Research Agenda	
I.	Consolidate research perspective to establish common foundations for Privacy by Design
II.	Derive and validate core requirements for Privacy by Design to comply with GDPR
III.	Expand design science research efforts beyond derivation of requirements
IV.	Develop concepts to ensure transparency in and between organizations
V.	Develop benchmarking for the evaluation of data processors
VI.	Develop decision support tools to enable developers to carefully decide on integrating data processors in the form of third parties and resulting consequences regarding to be compliant with the GDPR

As the analysis shows, the issue of PbD is relevant to a broad range of disciplines and research traditions. These efforts are right now unconnected and do not develop a consolidated research perspective. Thus, an initial focus of research on the issue of data processing in ecosystems should seek to consolidate the different research streams to establish a common foundation (I). Moreover, as the analysis shows, only few papers focus on third parties but rather tackle this facet incidentally. A focused approach should seek to reflect on requirements derived to propose a comprehensive set of requirements to ensure compliance with GDPR (II). At the beginning, we pointed out the relevance of the regulation due to existing organizational structures where data processors are common. The review clearly shows that so far, no solutions have been offered on how companies should handle PbD dealing with data processors. Thirteen studies do not address the handling regarding third parties at all. The lack of feasible, accepted designs and implementations for dealing with third parties is a major research gap that this review reveals. The studies published are fragmented and are still at the beginning regarding the handling of third parties. Practical solutions and evaluations are not yet available at all. Consequently, future research should seek to expand design-oriented research beyond deriving requirements to design actual solutions that can be validated and evaluated (III). Such efforts could, for example, lead to concepts that ensure transparency (IV) within and between organizations. Due to modular structures, these data processing services can be integrated rather simply. At this point, organizations which must comply with the GDPR should be aware of how users’ data is treated by implemented services. Building on this aspect, a privacy-related benchmarking (V) of third parties could lead to more sound decisions on the application of third parties. Based on the afore-mentioned potential research directions, an integrated perspective could lead to decision support for organizations (VI) from a strategic as well as operational level on the integration of third parties. Such a tool could guide design decisions by explicating consequences and GDPR compliance. The development of such a tool thus needs to be based on the prior research steps, to ensure appropriateness and usefulness.

9.5 Conclusion and Future Research

PbD can have different entry points for embedding privacy, in terms of GDPR embedding "data protection by design and by default", in systems, technologies, and organizations. Various studies have been published which have taken the technical implementation of PbD into account. However, privacy in the entire organization must be considered. In doing so, privacy must be a basic value that is anchored in an organization's mission statement, similar to the value of sustainability. This corresponds to the call that was made in the specification of the PbD concept as "[p]rivacy must be incorporated into networked data systems and technologies, by default. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives." (Cavoukian, 2009, p. 1). Only such an anchoring by integrating privacy-aware partner organizations, can ensure products and services which take privacy in the form of data regulation into account proactively, by default in a full lifecycle.

In Principle 6 (Cavoukian, 2009), it is emphasized that it is to assure that the third parties involved in the organizations' practices must also act in accordance with the PbD principles. Only by acting and considering such a comprehensive approach can guarantee the effectiveness of PbD. This is now also relevant for the companies themselves, as they can be made responsible for it in the future regarding the GDPR. As this literature review shows, such a strong anchor is missing. Only few papers explicitly address third parties and their integration in organization practices in order to process data according to the GDPR. First aspects have already been examined (Table 5, Table 6). To deal with this shortcoming, we propose a comprehensive research agenda that enables and guides researchers as well as practitioners to a decision process that explicitly addresses consequences and the impact on compliance regarding GDPR. Because this regulation becomes effective in May 2018, convincing solutions for the issues raised are urgently needed.

9.6 Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality in the project Information Governance Technologies under the reference LFF-FV 34.

9.7 References

Aïvodji, U. M., Gambs, S., Huguet, M.-J., and Killijian, M.-O. 2016. "Meeting Points in Ridesharing: A Privacy-Preserving Approach," Transportation Research Part C: Emerging Technologies (72), pp. 239–253.

Bier, C., and Krempel, E. 2012. "Common Privacy Patterns in Video Surveillance and Smart Energy," 2012 7th International Conference on Computing and Convergence Technology (ICCCT), pp. 610–615.

Böhmann, T., Leimeister, J. M. and Möslein, K. (2014) 'Service Systems Engineering', Business & Information Systems Engineering, 6(2), 73–79.

Caiza, J. C., Martín, Y.-S., Del Alamo, J. M., and Guam, D. S. 2017. "Organizing Design Patterns for Privacy: A Taxonomy of Types of Relationships," in: Proceedings of the 22nd European Conference on Pattern Languages of Programs. Irsee, Germany: ACM, pp. 1–11.

Callegati, F., Campi, A., Melis, A., Prandini, M., and Zevenbergen, B. 2015. "Privacy-Preserving Design of Data Processing Systems in the Public Transport Context," PACIS (7:4).

Cavoukian, A. 2009. "Privacy by Design," Information and privacy commissioner of Ontario, Canada).

Cavoukian, A. 2012. "Operationalizing Privacy by Design." Association for Computing Machinery, pp. 7–7.

Cavoukian, A., Chibba, M., and Stoianov, A. 2012. "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment," Review of Policy Research (29:1), pp. 37–61.

Cavoukian, A., and Kursawe, K. 2012. "Implementing Privacy by Design: The Smart Meter Case," 2012 International Conference on Smart Grid (SGE), pp. 1–8.

Chandler, J. D. and Lusch, R. F. (2015) 'Service systems a broadened framework and research agenda on value propositions, engagement, and service experience', Journal of Service Research, 18(1), 6–22.

Chandramouli, K., Arguedas, V. F., and Izquierdo, E. 2013. "Knowledge Modeling for Privacy-by-Design in Smart Surveillance Solution," 10th IEEE Int. Conf. on Adv. Video and Signal Based Surv., pp. 171–176.

Colesky, M., Hoepman, J. H., and Hillen, C. 2016. "A Critical Analysis of Privacy Design Strategies," 2016 IEEE Security and Privacy Workshops (SPW), pp. 33–40.

Conger, S., Pratt, J. H., and Loch, K. D. 2013. "Personal Information Privacy and Emerging Technologies," Information Systems Journal (23:5), pp. 401–417.

Cooper, H. M. 1988. "Organizing Knowledge Syntheses," Knowledge in society (1:1), p. 104.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Le Métayer, D., Tirtea, R., and Schiffner, S. 2015. "Privacy and Data Protection by Design–from Policy to Engineering, European Union Agency for Network and Information Security (Enisa), 2015."

Degeling, M., Lentzsch, C., Nolte, A., Herrmann, T., and Loser, K. U. 2016. "Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design," IEEE 2nd CIC, pp. 502–505.

Diamantopoulou, V., Argyropoulos, N., Kalloniatis, C., and Gritzalis, S. 2017. "Supporting the Design of Privacy-Aware Business Processes Via Privacy Process Patterns," 2017 11th RCIS, pp. 187–198.

Diver, L., and Schafer, B. 2017. "Opening the Black Box: Petri Nets and Privacy by Design," International Review of Law, Computers & Technology (31:1), pp. 68–90.

Friedman, B. 1997. Human Values and the Design of Computer Technology. Cambridge University Press.

Hartzog, W., and Stutzman, F. 2013. "Obscurity by Design," Washington Law Review (88:2), pp. 385–418.

Jaime, F., Maña, A., Ma, Z., Wagner, C., Hovie, D., and Bossuet, M. 2015. "Building a Privacy Accountable Surveillance System," 3rd Int. Conf. on Model-Driven Engineering and Software Dev., pp. 646–654.

Jutla, D. N., and Bodorik, P. 2015. "Pause: A Privacy Architecture for Heterogeneous Big Data Environments," 2015 IEEE International Conference on Big Data (Big Data), pp. 1919–1928.

Jutla, D. N., Bodorik, P., and Ali, S. 2013. "Engineering Privacy for Big Data Apps with the Unified Modeling Language," 2013 IEEE International Congress on Big Data, pp. 38–45.

Karwatzki, S., Trenz, M., Tuunainen, V. K., and Veit, D. 2017. "Adverse Consequences of Access to Individuals' Information," European Journal of Information Systems), pp. 1–28.

Koops, B.-J., and Leenes, R. 2014. "Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law," Int. Rev. of Law, Comp. & Tech. (28:2), p. 159.

Koops, B. J., Hoepman, J. H., and Leenes, R. 2013. "Open-Source Intelligence and Privacy by Design," Computer Law & Security Review (29:6), pp. 676–688.

Kopp, H., Mödinger, D., Hauck, F., Kargl, F., and Bösch, C. 2017. "Design of a Privacy-Preserving Decentralized File Storage with Financial Incentives," IEEE Eur. Symp. on Sec. and Privacy, pp. 14–22.

Kroener, I. and Wright, D. 2014. "A Strategy for Operationalizing Privacy by Design," Inf. Soc. (30:5), pp. 355–365.

Kroon, U. 2013. "Ma3tch: Privacy and Knowledge: 'Dynamic Networked Collective Intelligence'," 2013 IEEE International Conference on Big Data, pp. 23–31.

Kung, A., Freytag, J. C., and Kargl, F. 2011. "Privacy-by-Design in Its Applications," 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 1–6.

Kung, A., Jouvray, C., and Coudert, F. 2015. "Salt Frameworks to Tackle Surveillance and Privacy Concerns," 2015 3rd Int. Conf. on Model-Driven Engineering and Software Development, pp. 665–673.

Leitner, M., Bonitz, A., Herzog, B., Hotzendorfer, W., Kenngott, C., Kuhta, T., Terbu, O., Vogl, S., and Zehetbauer, S. 2016. "A Versatile, Secure and Privacy-Aware Tool for Online Participation," EDOCW, pp. 1–4.

Liegl, M., Boden, A., Buscher, M., Oliphant, R., and Kerasidou, X. 2016. "Designing for Ethical Innovation: A Case Study on Elsi Co-Design in Emergency," Int. Journal of Human-Computer St. (95), pp. 80–95.

Lusch, R. F. and Vargo, S. L. (2014) Service-dominant logic: Premises, perspectives, possibilities, Cambridge University Press.

March, S. T., and Smith, G. F. 1995. "Design and Natural-Science Research on Information Technology," Decision Support Systems (15:4), pp. 251–266.

Martín, Y. S., del Alamo, J. M., and Yelmo, J. C. 2014. "Engineering Privacy Requirements Valuable Lessons from Another Realm," 2014 IEEE 1st ESPRE, pp. 19–24.

Métayer, D. L. 2013. "Privacy by Design: A Formal Framework for the Analysis of Architectural Choices," in: Proc. of the third ACM conf. on data and application security and privacy: ACM, pp. 95–104.

Milutinovic, M., and De Decker, B. 2016. "Ethical Aspects in Ehealth - Design of a Privacy-Friendly System," Journal of Information Communication & Ethics in Society (14:1), pp. 49–69.

Mohammad, A., Stader, J., and Westhoff, D. 2015. "A Privacy-Friendly Smart Metering Architecture with Few-Instance Storage," I4CS, pp. 1–7.

Morizio, P. 2016. "Understanding Privacy-Control Arrangements Based on a Theory of Interactive Computation in B2c Service Models," 2016 HICSS, pp. 5348–5357.

Morton, A., and Sasse, M. A. 2012. "Privacy Is a Process, Not a Pet: A Theory for Effective Privacy Practice," in: Proceedings of the 2012 New Security Paradigms Workshop. Bertinoro, Italy: ACM, pp. 87–104.

Nordgren, A. 2015. "Privacy by Design in Personal Health Monitoring," Health Care (23:2), pp. 148–164.

Notario, N., Crespo, A., Martín, Y. S., Alamo, J. M. D., Métayer, D. L., Antignac, T., Kung, A., Kroener, I., and Wright, D. 2015. "Pripare: Integrating Privacy Best Practices into a Privacy Engineering Methodology," IEEE Security and Privacy Workshops, pp. 151–158.

O'Connor, Y., Rowan, W., Lynch, L., and Heavin, C. 2017. "Privacy by Design: Informed Consent and Internet of Things for Smart Health," Procedia Computer Science (113), pp. 653–658.

Ostrom, A. L., Parasuraman, A., Bowen, D. E., Patricio, L., Voss, C. A., and Lemon, K. 2015. "Service Research Priorities in a Rapidly Changing Context," Journal of Service Research (18:2), pp. 127–159.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," Journal of Management Inf. Sys. (24:3), pp. 45–77.

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., and Nuseibeh, B. 2016. "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms," in: Proceedings of the 6th International Conference on the Internet of Things. Stuttgart, Germany: ACM, pp. 83–92.

Peters, C., Maglio, P., Badinelli, R., Harmon, R. R., Maull, R., Spohrer, J. C., Tuunanen, T., Vargo, S. L., Welser, J. J., Demirkan, H., Griffith, T. L., and Moghaddam, Y. 2016. "Emerging Digital

Frontiers for Service Innovation," Communications of the Association for Information Systems (39), pp. 136–149.

Popescu, M., and Baruh, L. 2013. "Captive but Mobile: Privacy Concerns and Remedies for the Mobile Environment," Information Society (29:5), pp. 272–286.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., and Gill, P. 2018. "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem,").

Regulation, G. D. P. 2016. "Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46," Of. J. of the EU (OJ) (59), pp. 1–88.

Reznichenko, A., and Francis, P. 2014. "Private-by-Design Advertising Meets the Real World," in: Proceedings of the 2014 ACM SIGSAC. Scottsdale, Arizona, USA: ACM, pp. 116–128.

Romanou, A. 2017. "The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise," Computer Law & Security Review.

Rowan, M., and Dehlinger, J. 2014. "Encouraging Privacy by Design Concepts with Privacy Policy Auto-Generation in Eclipse (Page)," Workshop Eclipse Technology eXchange: ACM, pp. 9–14.

Rubinstein, I. S., and Good, N. 2013. "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents," Berkeley Technology Law Journal (28:2), pp. 1333–1413.

Schoonmaker, J. 2016. "Proactive Privacy for a Driverless Age," Inf. & Com. Tech. Law (25:2), pp. 96–128.

Senst, T., Eiselein, V., Badii, A., Einig, M., Keller, I., and Sikora, T. 2013. "A Decentralized Privacy-Sensitive Video Surveillance Framework," 2013. 18th Inter. Conference on Digital Signal Processing, pp. 1–6.

Siljee, J. 2015. "Privacy Transparency Patterns," in: Proceedings of the 20th European Conference on Pattern Languages of Programs. Kaufbeuren, Germany: ACM, pp. 1–11.

Spohrer, J., Maglio, P., Bailey, J. and Gruhl, D. (2007) 'Steps toward a science of service systems', Computer, 40(3), 71–77.

Sun, Z., Zan, B., Ban, X., and Gruteser, M. 2013. "Privacy Protection Method for Fine-Grained Urban Traffic Modeling Using Mobile Sensors," Transportation Research (56), pp. 50–69.

Vallez, N., Espinosa-Aranda, J., Rico-Saavedra, J., Parra-Patino, J., Deniz, O., Pagani, A., Krauss, S., Reiser, R., Stricker, D., Moloney, D., Dehghani, A., Dunne, A., Pena, D., Waeny, M., Santos, P., Sorci, M., Llewellynn, T., Fedorczak, C., Larmoire, T., Roche, E., Herbst, M., Seirafi, A., and Seirafi, K. 2017. "Eyes of Things," IEEE IC2E, pp. 292–297.

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., and Gill, P. 2016. "Tracking the Trackers," arXiv preprint arXiv:1609.07190).

Van Der Sype, Y. S., and Maalej, W. 2014. "On Lawful Disclosure of Personal User Data: What Should App Developers Do?" 2014 IEEE 7th Int. Workshop on Requirements Engineering and Law, pp. 25–34.

van Lieshout, M., Kool, L., van Schoonhoven, B., and de Jonge, M. 2011. "Privacy by Design: An Alternative to Existing Practice in Safeguarding Privacy," Info (13:6), pp. 55–68.

Vargo, S. L. and Lusch, R. F. (2011) 'It's all B2B... and beyond: Toward a systems perspective of the market', Industrial Marketing Management, 40(2), 181–187.

Vicini, S., Alberti, F., Notario, N., Crespo, A., Pastoriza, J. R. T., and Sanna, A. 2016. "Co-Creating Security-and-Privacy-by-Design Systems," 2016 11th ARES, pp. 768–775.

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. 2009. "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process," ECIS, pp. 2206–2217.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly (26:2), pp. Xiii–Xxiii.

Ye, T., Moynagh, B., Albatal, R., and Gurrin, C. 2014. "Negative Faceblurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass," in: Proceedings of the 23rd ACM International Conference on Information and Knowledge Management, pp. 2036–2038.

10 Article No. 2 (Kurtz et al. 2018a)

Kurtz, C., Semmann, M., and Schulz, W. Towards a Framework for Information Privacy in Complex Service Ecosystems. Proceedings of the 39th International Conference on Information Systems (ICIS), San Fransisco, 2018.

Abstract

Information Privacy gained visibility and rising awareness in society as well as media coverage due to the case of Cambridge Analytica and Facebook. This case demonstrates the extent of complex service ecosystems with a multitude of actors involved in actions that impact information privacy. As such ecosystems are nowadays ubiquitous the implementation of the General Data Protection Regulation (GDPR) seeks to establish responsibility regarding actions taken by data processors. With this paper, propose an analytical framework that builds on an analysis of privacy-invasive critical cases in complex service ecosystems. We applied a cross impact matrix to systematically identify critical issues. Additionally, by visualizing data flows between actors, privacy-critical issues in service ecosystems become apparent. Building on these insights privacy-related problem propositions are derived that lead to future design-oriented research directions. Thus, we propose a framework that helps scholars and practitioners to identify blind spots and privacy-critical issues in service ecosystems.

10.1 Introduction

A 2015 editorial in the *Information Systems Journal* stated that "recent technological changes are generating additional privacy challenges beyond the existing landscape" (Belanger and Xu, 2015, p. 575). The newly publicized case of Cambridge Analytica's misuse of Facebook user data is just one prominent example of such challenges. About 87 million Facebook users were affected by the privacy-invasive access of user data by an application that was published on Facebook (Frier, 2018). This application was able to access a wide variety of data from Facebook users and users' friends, subsequently delivering the data to a third actor, Cambridge Analytica. As the case shows, users nowadays face the challenge of maintaining their privacy in the context of highly interconnected information processing. Currently, users often once make a single decision to use a service in general. However, technological advances have led to complex service ecosystems that combine services from a multitude of service providers. Organizations implement other, backend services in their services for various purposes. These include application performance management, social network integration, or monetization of services through advertisements. A single user decision to use a service can result in giving access to multiple parties who may process this data (Conger et al., 2013; Razaghpanah et al., 2018). Information about a user is aggregated through many avenues of data access, which is both highly complex and confusing for users. Where users previously faced one decision about one organization, they now face a multitude of actors that are not necessarily even visible to the user. These changes to complex services have led to problems regarding users' privacy over time.

In this article we propose a framework that is appropriate to analyze privacy-critical issues associated with these changes. As the case of Facebook demonstrates, no solution exists until now that fully cover all critical issues to protect user's privacy. The problems that arise within digital, interconnected services have not yet been sufficiently considered in the design of solutions. However, according to the framework of Privacy by Design, privacy must be approached from a design-thinking perspective (Cavoukian, 2009). Though, without a precise description of a problem, the necessary requirements for a suitable solution cannot be derived (Peffers et al., 2007). We develop a framework to analyze critical cases to identify privacy-related problems, as we believe that privacy protection requires better solutions than those that already exist. Our framework makes it possible to identify blind spots and enables an examination of privacy-critical issues between multiple actors located in an interconnected service ecosystem. In the next step, organizations and regulators may benefit from guidance on where to position privacy-based modifications in order to prevent critical cases like that of Facebook. This knowledge is also indispensable because the General Data Protection Regulation (GDPR) specifies that organizations bear responsibility with regard to actions taken by "processors", which also includes integrated backend services (GDPR, 2016, Chapter 4 Article 25). To perform data protection impact assessments knowledge is required that cannot be easily produced for complex service ecosystems (GDPR, 2016, Chapter 4 Article 35). The same is true for the information basis on which a data subject, a user, gives consent. In summary, we research privacy-critical issues of multi-actor information-processing that are related to service ecosystems.

This paper begins with a theoretical framework that includes the foundations of service ecosystems and information privacy in multi-actor relationships. We then derive a multi-actor perspective on service ecosystems. Afterwards, in the research design section, we deduce the framework to the assessment of multilateral, independent (design) decisions and consider their implications for privacy in critical cases. Subsequently, two critical cases are analyzed. Building on the results, we derive in the discussion the critical issues for privacy in that cases. These issues are used to deduce problem propositions that may act as the basis of solution designs. The paper finishes with a conclusion and outlook for future research endeavors that build on the results of this research-in-progress article.

10.2 Theoretical Framework

In general, the ways in which service is delivered have changed essentially in many respects and have become a key driver in the information systems discipline (Böhmann et al., 2014). Research on service has likewise shifted from focusing on single services towards systems of services (Spohrer et al., 2007; Vargo and Lusch, 2011; Böhmann et al., 2014; Chandler and Lusch, 2015). Building on this systemic perspective, service ecosystems are defined as "a relatively self-contained, self-adjusting system of resource-integrating actors connected by shared institutional arrangements and mutual value creation through service exchange" (Lusch and Vargo, 2014, p. 24) that includes rules and norms (Vargo and Lusch, 2016, p. 11). This definition implies a dynamic, combined configuration across multiple actors that creates value for the beneficiary. Recently published studies show the high dissemination of third parties in (mobile) services from a privacy-critical perspective (Backes et al., 2016; Lerner et al., 2016; Meng et al., 2016; Vallina-Rodriguez et al., 2016; Razaghpanah et al., 2018). Third parties have numerous points of access both on one device and across multiple devices (Buss, 2015; Brookman et al., 2017; Zimmeck et al., 2017), and they can thus condense the information they gather on a single user via unique identifiers such as IP addresses or user settings (Kurtz et al., 2016).

Early privacy studies mention practices of companies that are privacy-critical (Westin, 1972; Tolchinsky et al., 1981; Stone et al., 1983; Linowes, 1990; Culnan, 1993; Smith et al., 1996). Also, studies have examined the dimensions reflecting individuals' concerns about organizational practices that impact privacy (Smith et al., 1996). In the models subsequently developed with the intention of examining user privacy decision-making, such practices were considered in user privacy risks and privacy concerns (Malhotra et al., 2004; Dinev and Hart, 2006; Nikkhah and Sabherwal, 2017). In this context, the conflict experienced by web-based service providers with regard to how much data to share with third parties was examined, taking user privacy concerns into account (Gopal et al., 2018). However, decision-making on the part of an individual implies both choice and consent, and today, with increasingly complex trade-offs, these notions are no longer sufficient (Solove, 2012; Acquisti et al., 2015). The complexity result in individuals sharing and providing their personal data without realizing it (Belanger and Xu, 2015, p. 576). For instance, smartphone operating systems do not enable users to view the way third-party applications collect and share their data (Enck et al., 2014; Crossler and Bélanger, 2017). These modifications in information technology lead to confusing and unclear sharing of personal data (Acquisti et al., 2015, p. 509). Incomplete and asymmetric information are reasons for privacy uncertainty among users, which results in an inability to act in a self-interested manner (Acquisti et al., 2015; Crossler and Bélanger, 2017).

The GDPR has come into effect in May 2018 in the European Union where it remains to be seen to what extent the GDPR can address these problems. The GDPR is not based on a specific theory of privacy but sticks to the concept of using "personal data" as the starting point of regulation, trying to guarantee the persons control over the processing of those data. Additionally, the GDPR includes elements of systemic data protection (Tikkinen-Piri et al., 2018). This act aims to protect privacy in the digital world, thus relating to service ecosystems, in the form of data protection and data regulation (Danezis et al., 2015). Our approach can therefore also help to demonstrate to what extend the GDPR can address privacy issues in complex ecosystems. We intend to assess the critical cases we detect based on the GDPR in further projects (Kurtz et al., 2019). The evaluation of the cases on the basis of normative standards basically follows the same procedure as the analysis presented here but is an independent assessment that is not scope of this paper and thus not presented here. The results of that assessment will be shared with regulators and policy makers to create a real-world impact of our research and to find ways, how society can deal with the issues.

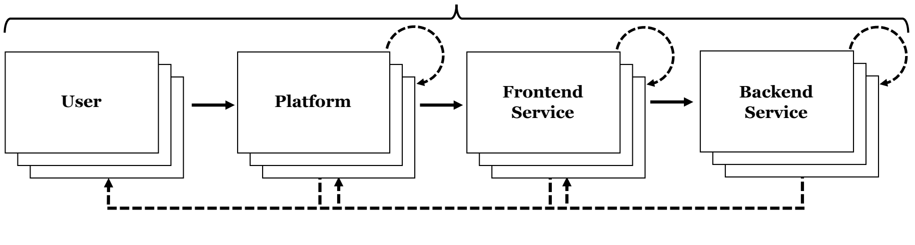


Figure 1. Adapted Model of Privacy in Ecosystems (based on (Conger et al., 2013))

In this article, we use the term "ecosystem" to indicate that actors interact not only with well-designed information systems (IS) but also with systems of systems. Parts of these systems emerge in the spontaneous interaction among actors. At some point, actors make (design) decisions that have consequences for other actors, for instance for the scope of subsequent (design) decisions. The objectives of those systems can be in terms of a broad sense that includes software and hardware architecture or the structuring of social procedures – as well as the interaction of all of these. These ecosystems have consequences for the privacy of actors that have not yet been examined in detail. A model previously published offers a system perspective on the interactions between an individual, an organization and an integrated third organization which can influence individual's privacy (Conger et al., 2013). Our focus is on the interactions among these actors. To illustrate this, we have refined and modified the existing model (Figure 1) to depict a part of the ecosystem that we will discuss in more detail below.

We name the actors as "user", "frontend service", and "backend service". Furthermore, we consider the actor "platform" to allow us to analyze the critical cases in more detail and reflect how services are provided in a digital world. These actors occur not just once but several times, for instance, a frontend service integrates various backend services as mentioned above. In line with this concept, our investigation does not factor in the characteristics influencing the disclosure of personal information by the first party (privacy calculus). Furthermore, we do not factor in the author's understanding of the fourth party (which is considered an illegal entity i.e., hackers). The actors and their actions take effect in service ecosystems.

10.3 Research Design

In the following, we develop an analytical framework that helps to specify the problems and phenomena in these complex service ecosystems that current privacy research until now cannot explain entirely. The service ecosystem is subject to problems that occur directly where the actors are located or at the interfaces between them. To reveal these problems, we make use of critical cases. We understand "critical" in a way that builds on the epistemological understanding of "critique", that is, discussing issues with the intention of preventing (unproductive) separation of single categories, fields, and practices of thought. To do that we work with those established categories and extend them from a service ecosystem perspective. By shifting the perspective towards multi-actor service systems, we are able to identify privacy related issues along interfaces and distributed data processing. Thus, we contribute to the ongoing discourse about information privacy. Our research will help to identify blind spots and specify problems that are results of paths dependencies, sector- and layer-specificities, and disciplinary boundaries. This research is thus the first step towards design science projects that can lead to practices and models that foster privacy aware service ecosystem design and thus can support regulators identifying inconsistencies of recent approaches.

A "critical case" is thus also a case for which no capable analytical framework existed of systematically locating privacy-critical issues in their entirety. This need has already been raised, as "[m]uch of the research on information privacy has focused on individuals […]" (Belanger and Xu, 2015, p. 576) as a consequence of which existing privacy models cannot be used to adequately examine the critical cases. There has already been a call for the examination of information privacy violations and of the organizational factors which lead them (Belanger and Xu, 2015, p. 576). Building on this call for research, we propose an analytical framework for privacy-critical issues located in complex service ecosystems.

Different critical issues for privacy can become visible in the examination of the entire complex service ecosystem. For this, as a method of analyzing the critical cases, we use a cross impact matrix to identify privacy-related problems. This enables us to identify actions and their corresponding impacts in the complex service ecosystem. Additionally, we can explore which impacts the multilateral, independent (design) decisions of each actor within the service ecosystem cause which effects. In the matrix, the actors are arranged across the top of the matrix and down one side. This allows a simple and clear presentation of both the actors and the cause–effect relationships among them. There can also be issues where the cause-effect relation only affects one actor. This arrangement of actors is necessary to create transparency and to identify critical privacy issues. This is needed to specify the problems, forming the basis of designing suitable requirements for artifacts for protecting individual's privacy. Design is the act of creating an explicitly appropriate solution to a defined problem, and in the process of designing, it is necessary to specify the problem such that the solution can take into account its complexity (Peffers et al., 2007). Without such problem specification, no solutions can be designed that take the problems into account to their full extent. This problem specification is the first process step of the Design Science Process Model (Peffers et al., 2007) of which the next steps will be focused by us. In our analytical framework the critical issues for privacy are identified by the application of the cross-impact matrix. By the analysis of critical cases in this cross-impact matrix we identify distinguishing as well as repeating patterns. Subsequently, this enables us to derive problem propositions. Building on this methodology, our research process, shown schematically in Figure 2, is divided into three steps: (1) apply critical cases to the cross-impact matrix, enabling us to identify critical issues for privacy, (2) use these issues to derive privacy-related objectives and requirements of a solution, and (3) and finally derive suitable design solutions for users, policy makers, and industry.

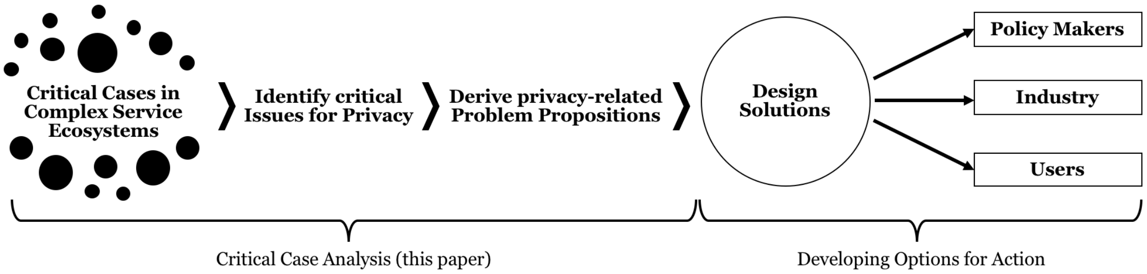

Critical Cases in Complex Service Ecosystems
Identify critical Issues for Privacy
Derive privacy-related Problem Propositions
Design Solutions
Policy Makers
Industry
Users
Critical Case Analysis (this paper)
Developing Options for Action

Figure 2. Analytical Framework for Establishing Information Privacy in Complex Service Ecosystems

In this article, which considers research that is still in progress, we conduct, to a limited extent, the first two steps of the research process. We examine two different critical cases that show the range of application of the analytical framework. The critical cases have their own peculiarities. During the whole research process, we analyze multiple critical cases in the context of a full research paper. This allows us to sharpen our analytical framework and to identify and specify problems and patterns that do not occur in the two critical cases analyzed here.

10.4 Critical Case Analysis

10.4.1 "Facebook and Cambridge Analytica"

The data scandal of Facebook and Cambridge Analytica with a widely coverage in the media has also led to a hearing of Facebook' CEO Mark Zuckerberg before the United States House of Representatives Committee on Energy and Commerce (Rosenberg et al., 2018; Solon, 2018; Zuckerberg, 2018). In this case, users of the platform Facebook used the on the platform provided frontend service "Your Digital Life". By authorize the requested data access rights to this frontend service, users disclosed their own data as well as enabled the access to data of their friends for Your Digital Life. 270,000 users directly used Your Digital Life, by contrast, the data of in total 87 million Facebook users was shared with the service (Frier, 2018). After that, Your Digital Life sold this data to a backend service, Cambridge Analytica, which used it to target users on Facebook (Rosenberg et al., 2018).

Table 1. "Facebook" - Problem Description (Grey Fields Symbolize Data Flows)

		Impact on			
		User	**Platform** Facebook	**Frontend Service** Your Digital Life	**Backend Service** Cambridge Analytica
Action of | Data from	**User**	4) Didn't carefully check Privacy Settings	A		
	Platform	1) Opt-out Privacy Settings for User's Friends		2) Enables Service Data Access on the Platform B	
	Frontend Service	3) Offers data-collecting Application	5) Breaks the Policy		6) User and Friends' Data are actively transmitted C
	Backend Service	7) Use the received Data for Targeted Advertising	8) Exploits Possibilities of Targeting on the Platform D		

In this case, several flaws led to this large data breach. In the time that the case was formed, users had to manually opt-out of sharing their data with the services used by friends' (1). Facebook enabled external services on the platform to access the data of both users and users' friends (2). The frontend service Your Digital Life thus collected data (3) of Facebook users who did not carefully check their privacy settings (4). Your Digital Life then did not comply with Facebook's data policy (5) and transmitted the data to the backend service Cambridge Analytica (6). Based on this data, Cambridge Analytica delivered individualized advertisements (7) that exploited the potential that is intended by the platform provider (8).

The data-flows (grey fields in Table 1) of this case show that the data is passed from the platform Facebook (A) to the frontend service Your Digital Life (B). Data are then actively transmitted to the backend service Cambridge Analytica (C), who used this data for target advertisements on Facebook (D). Such deceitful behavior could have been prevented if mechanisms had been implemented to limit data sharing as well as access to and forwarding of data on the platform.

10.4.2 "AccuWeather and RevealMobile"

In the second critical case, the iOS application AccuWeather transmitted user device data to a backend service called RevealMobile which approximated user's location using this data even when the permission that the application may access location services was revoked by the user. This latter organization focusses on mobile marketing by using such data to segment user groups for advertising (RevealMobile, 2017).

In this case, the application AccuWeather was after a review of Apple available for download in the iOS AppStore (1). The privacy statement declared that the application uses methods to approximate user's location and that this data is transmitted to backend services (AccuWeather, 2018). The backend services receiving this data were neither explicitly stated nor was a complete specification of these services included (2). Approximation of a user's location was possible because in iOS, access to a user's location is linked to technical access to GPS data (3). This is not visible for users who do not read the privacy statement intensively. Here, the technologies and the approximation actions of backend services were mentioned (4), but the backend services were not named explicitly. When using the application, the platform iOS sent the wi-fi name, BSSID (Basic Service Set Identification, corresponds to the MAC address of the connected wireless access point), and Bluetooth status, which were used to approximate the location of a user's device (5). During a testing period lasting 36 hours, while the application was not in the foreground of the screen, the mentioned data was sent 16 times to the company RevealMobile (Strafach, 2017). A study of RevealMobile states that the "[…] technology sits inside hundreds of apps […]" (6) and "[i]t turns the location data coming out of those apps into meaningful audience data […]" (7) (RevealMobile, 2016, p. 2).

Table 2. "AccuWeather" - Problem Description (Grey Fields Symbolize Data Flows)

		Impact on			
		User	**Platform** iOS	**Frontend Service** AccuWeather	**Backend Service** RevealMobile
Action of | Data from	**User**	4) Didn't carefully check the Privacy Statement	A		
	Platform			1) App published 3) Location Access only linked to GPS Data B	C
	Frontend Service	2) Privacy Statement does not include Backend Services			5) Transmission of Data via API to approximate Location D
	Backend Service	7) Turns Data into Audience Data for Advertising	6) Wide Distribution of RevealMobile on Platform		E

The data-flows (Table 2) differentiates this case from the prior case. The user's device data (A) is passed on from the platform iOS to the application AccuWeather (B). Then, the data are passed from the platform via the API in the application (C) to the backend service RevealMobile (D). Here, the data are enriched with data sources of other backend services to approximate the location of users (E) (Wu et al., 2015).

The main issue was that users' negotiation to the app to don't access the location is not consistent with the technical implementation. The operating system transmitted Wi-fi BSSID data which at a first view seem to be non-privacy related to the application with included backend services. In normal usage of iOS, users have no opportunity to consent or neglect this information flow. In the next step, this data is enriched with databases which include the locations of WiFi networks. Next, it is possible for actors in the service ecosystem to approximate the device's location. And this, despite the fact that the user denies the access to his location. Such transmission of data could have been prevented by the platform if mechanisms had been implemented to regulate access to data with which may become privacy-critical for users.

10.5 Discussion

The following offers an overview of the problem propositions, shown in Table 3, deduced from the privacy critical issues based on the analyzed cases. The propositions are linked to the different aspects of the cases. As the critical case analysis shows, service ecosystems apply several modes of action and impacts on privacy. Nevertheless, both analyzed cases share commonalities that regarding the possibility to embed actors within the service ecosystem and process data of users. Further research and an extension of the critical case analysis is thus needed to validate the identified issues. However, the problems identified relate to core mechanics of the service ecosystems and thus can be deemed worthwhile building on them. As several problems are identified, we discuss only two problem propositions in detail to provide insights on the following design science projects. In total, these are only exemplary and initial problem propositions that require further enrichment by other cases.

The problem proposition, "Overview of Backend Service", can be derived from both cases. It consists of the problem for users that no overview of backend services exists. It is not always possible to identify which backend services are available in a given frontend service (second case). It is even more difficult to maintain an overview of which frontend services used by a user are connected to which backend services.

The second problem proposition "Format of Transparency" highlights the problem of the complexity of privacy statements (Keith et al., 2018) which due to emerging backend services in services intensifies. In the statements the interactions with backend services are mentioned and described. However, also the backend privacy policies are implicitly accepted. Nevertheless, consent to privacy statements must be given informed which seems for such complex privacy statements very doubtful.

Table 3. Derived Privacy-Related Problem Propositions

		Impact on			
		Users	**Platforms**	**Frontend Services**	**Backend Services**
Action of	**Users**	Check of Privacy Statements and Settings (FB4, AW4)	Careful Use of Platforms (FB1, FB5, AW3, AW6)		
	Platforms	Default Settings for Privacy Protection (FB1, FB5)		Implementation of User Decisions (AW3) Control when Data leave Platform (FB2, FB3, FB6, AW1, AW5)	Control when Data leave Platform (FB6, FB8, AW5)
	Frontend Services	Format of Transparency (FB4, AW2, AW4)			Interaction with Backend Services (FB6, AW5, AW7)
	Backend Services	Overview of Backend Services (FB6, FB7, AW5, AW6, AW7)			

The two cases have data flows with different characteristics. The data flow models contain active data transmitting on the part of the frontend service ("Your Digital Life") or data transmission via an API (implemented in the application AccuWeather). The data flows may be classified differently. Relevant for this may be which prior action took that the privacy-critical data flow occur. Such aspects will be considered in our subsequent research. Building on the identified problems (Figure 2), we will apply the Design Science Research Process Model (Peffers et al., 2007) to develop socio-technical artifacts that aim for improving privacy in service ecosystems. Next, objectives of a solution are derived and instantiated by designing solutions accordingly. This is followed by demonstrating and evaluating the artifacts. For policy makers, we would work out the requirements for regulations to develop solutions to deal with the identified issues.

10.6 Conclusion and Outlook

According to the GDPR, the frontend service provider may be held responsible for implemented backend services in the future. As digital services comprise modules of different backend services, issues regarding users privacy as well as regarding frontend service providers responsibility arise (Kurtz et al., 2018). We have developed a framework to specify the problems of multi-actor information-processing that are related to service ecosystems. This is also essential for evaluating the GDPR and the responsibility of actors under the assumption that the supervision of those actors is sufficient to control the privacy risks to users. Moreover, within the GDPR are instruments that could be improved based on our framework, especially instruments such as the data protection impact assessments (GDPR, 2016, Chapter 4 Article 35).

In further developing this framework and the problem propositions briefly outlined herein, we expect that the number of problem specifications will grow. We would substantiate this through analysis of additional cases. To summarize, we would like to emphasize once again the necessity of such a framework. A complete view of complex ecosystems is needed to protect privacy – as the interview with the platform operations manager at Facebook shows. To the question of what kind of control Facebook had over the data given to external services, he stated "Absolutely none. Once the data left Facebook servers there was not any control, and there was no insight into what was going on" (Lewis, 2018). We offer a framework by which such privacy-critical problems can be specified. This is a necessary step to enable design of comprehensive solutions for privacy, so that users and organizations are not affected by repeated and unnecessary failures.

10.7 Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality in the project Information Governance Technologies under the reference LFF-FV 34. We thank Tilo Böhmann for his valuable feedback throughout the development of this paper.

10.8 References

AccuWeather. 2018. "Privacy Statement" Retrieved 03.06.2018. https://www.accuweather.com /en/privacy

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information" Science (347:6221), pp. 509-514.

Backes, M., Bugiel, S., and Derr, E. 2016. "Reliable Third-Party Library Detection in Android and Its Security Applications" Conference on Computer and Communications Security. pp. 356-367.

Belanger, F., and Xu, H. 2015. "The Role of Information Systems Research in Shaping the Future of Information Privacy" Information Systems Journal (25:6), pp. 573-578.

Böhmann, T., Leimeister, J. M., and Möslein, K. 2014. "Service Systems Engineering" Business & Information Systems Engineering (6:2), pp. 73-79.

Brookman, J., Rouge, P., Alva, A., and Yeung, C. 2017. "Cross-Device Tracking: Measurement and Disclosures" Proceedings on Privacy Enhancing Technologies (2017:2), pp. 133-148.

Buss, J. 2015. "Cross-Device Advertising: How to Navigate Mobile Marketing's Next Big Opportunity" Journal of Digital & Social Media Marketing (3:1), pp. 73-79.

Cavoukian, A. 2009. "Privacy by Design" Information and privacy commissioner of Ontario, Canada).

Chandler, J. D., and Lusch, R. F. 2015. "Service Systems a Broadened Framework and Research Agenda on Value Propositions, Engagement, and Service Experience" Journal of Service Research, pp. 6-22.

Conger, S., Pratt, J. H., and Loch, K. D. 2013. "Personal Information Privacy and Emerging Technologies" Information Systems Journal (23:5), pp. 401-417.

Crossler, R. E., and Bélanger, F. 2017. "The Mobile Privacy-Security Knowledge Gap Model: Understanding Behaviors" Proceedings of the 50th Hawaii International Conference on System Sciences.

Culnan, M. J. 1993. "" How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use". MIS quarterly, pp. 341-363.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirtea, R., and Schiffner, S. 2015. "Privacy and Data Protection by Design-from Policy to Engineering" arXiv preprint:1501.03726).

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions" Information Systems Research (17:1), pp. 61-80.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. 2014. "Taintdroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones" ACM Transactions on Computer Systems (TOCS) (32:2), p. 5.

Frier, S. 2018. "Facebook Says There May Be More Cambridge Analytica-Sized Leaks". Retrieved 03.06.2018. Bloomberg. https://www. bloomberg.com/news/articles/2018-04-26/facebook-says-there-may-be-more-cambridge-analytica-sized-leaks

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., and Zhdanov, D. 2018. "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas" Man. Inf. Sys. Quar. (42:1), pp. 143-164.

Keith, M. J., Frederickson, J. T., Reeves, K. S., and Babb, J. 2018. "Optimizing Privacy Policy Videos to Mitigate the Privacy Policy Paradox" in Proceedings of the 51st Hawaii International Conference on System Sciences. Hawaii.

Kurtz, A., Gascon, H., Becker, T., Rieck, K., and Freiling, F. 2016. "Fingerprinting Mobile Devices Using Personalized Configurations" Proceedings on Privacy Enhancing Technologies (2016:1), pp. 4-19.

Kurtz, C., Semmann, M., and Böhmann, T. 2018. "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors" in: Americas Conference on Information Systems. New Orleans.

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. 2019. "The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems" Proceedings of the 52nd Hawaii International Conference on System Sciences. Hawaii.

Lerner, A., Simpson, A. K., Kohno, T., and Roesner, F. 2016. "Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016" USENIX Security Symposium.

Lewis, P. 2018. "'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting Was Routine" The Guardian.

Lusch, R. F., and Vargo, S. L. 2014. Service-Dominant Logic: Premises, Perspectives, Possibilities. Cambridge University Press.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model" Information Systems Research (15:4), pp. 336-355.

Meng, W., Ding, R., Chung, S. P., Han, S., and Lee, W. 2016. "The Price of Free: Privacy Leakage in Personalized Mobile in-Apps Ads" NDSS.

Nikkhah, H. R., and Sabherwal, R. 2017. "A Privacy-Security Model of Mobile Cloud Computing Applications" in: Thirty Eighth International Conference on Information Systems.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research" Journal of Management Inf. Sys. (24:3), pp. 45-77.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., and Gill, P. 2018. "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem".

Regulation, General Data Protection Regulation. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46," Official Journal of the European Union (OJ) (59), pp. 1-88.

RevealMobile. 2016. "Using Mobile Location Data and Beacons to Measure Retail Shopping Behavior."

RevealMobile. 2017. "Revealmobile Website." Retrieved 15.08.2017. https://revealmobile.com

Rosenberg, M., Confessore, N., and Cadwalladr, C. 2018. "How Trump Consultants Exploited the Facebook Data of Millions," in: The New York Times.

Sapiezynski, P., Stopczynski, A., Gatej, R., and Lehmann, S. 2015. "Tracking Human Mobility Using Wifi Signals" Plos One (10:7).

Smith, H. J., Milburg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices" Mis Quarterly (20:2), pp. 167-196.

Solon, O. 2018. "Facebook Says Cambridge Analytica May Have Gained 37m More Users' Data" in: The Guardian.

Solove, D. J. 2012. "Introduction: Privacy Self-Management and the Consent Dilemma" Harv. L. Rev. (126).

Strafach, W. 2017. "Advisory: Accuweather iOS App Sends Location Information to Data Monetization Firm." Retrieved 21.08.2017. https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. 2018. "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies" Computer Law & Security Review (34:1), pp. 134-153.

United States House of Representatives Committee on Energy and Commerce. 2018. "Testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook."

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., and Gill, P. 2016. "Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem" arXiv:1609.07190.

Vargo, S. L., and Lusch, R. F. 2011. "It's All B2b… and Beyond: Toward a Systems Perspective of the Market" Industrial marketing management (40:2), pp. 181-187.

Vargo, S. L., and Lusch, R. F. 2016. "Institutions and Axioms: An Extension and Update of Service-Dominant Logic" Journal of the Academy of Marketing Science (44:1), pp. 5-23.

11 Article No. 3 (Kurtz et al. 2019)

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems. Proceedings of the 52nd Hawaii International Conference on System Sciences, Hawaii, 2019.

Abstract

The digital age is characterized by hyper-connected services. Whenever we engage with an app we likely engage with a broader set of actors, often facilitated by a platform. Essentially, we engage with a service ecosystem posing particular challenges for privacy regulation. With GDPR taking effect we seek to understand the implications of it for privacy in such ecosystems. Interconnected services can facilitate the diffusion of personal data and thus impede with individual privacy rights. We apply a novel techno-legal analysis to the flow of personal information in service ecosystems. Based on two cases, we show that novel requirements arise for platforms as key actors in service ecosystems. Using our techno-legal analysis we conclude that two major platform providers, Apple and Facebook, have more in common from a legal perspective than the current rhetoric suggests. Based on the analysis, we discuss where privacy-preserving solutions in service ecosystems need to be positioned.

11.1 Introduction

Recently, numerous cases have been reported in which Facebook had a big impact on the diffusion of personal data. These are linked by the fact that Facebook has illegitimately shared data of users in data partnerships to different companies, at least to 60 device manufacturers (Dance et al., 2018). Moreover, Facebook shared information with apps, although this was technically revised before and should prevent such privacy-critical transmission (2018). The most controversial case that became public can be referred to as the case of Cambridge Analytica's misuse of Facebook user data. About 87 million Facebook users were affected by the privacy-invasive access of data (Frier, 2018). Afterwards, this data was delivered to Cambridge Analytica which, based on personality analyses, placed targeted election advertisement on Facebook.

Tim Cook, CEO of Apple, criticized Facebook how user data is handled on that platform. He stated that the "[…] situation is so dire and has become so large that probably some well-crafted regulation is necessary" (Wong, 2018). Furthermore, he also stated in the context of the Cambridge Analytica case that he "[…] wouldn't be in this situation" (Wong, 2018).

In this article we examine two published privacy-critical cases with two different platforms. The first case, with 'This Is Your Digital Life' (hereinafter referred to as 'Digital Life') and Cambridge Analytica, where Facebook acts as platform, and the case with AccuWeather and RevealMobile, where iOS acts as platform by the provider Apple. The cases represent today's interconnected service ecosystems in which personal data is diffused. In our analysis, we examine the technical aspects and we build on the GDPR for a legal perspective. We specify the responsibilities, contributing to a realization of the GDPR in practice and the design of privacy-aware service ecosystems (Kurtz et al., 2018). Consequently, research may benefit from a further discussion about the scope of actor obligations in service ecosystems and where to position responsibility.

The article begins with a theoretical framework that includes the foundations of information privacy in service ecosystems. Afterwards, we describe the roles defined in the GDPR. Subsequently, we carry out a techno-legal analysis of the two cases. Based on this, we position the accountability and derive legal obligations according to the GDPR. From this, we outline possible solution positions in service ecosystems and draw a conclusion.

11.2 Theoretical Framework

11.2.1 Information Privacy in Service Ecosystems

In this article, we focus on the diffusion of personal data respectively personal information in hyperconnected services. In general, the ways in which services are delivered have changed essentially in many respects (Böhmann et al., 2014). Service delivery has likewise shifted from single services towards ecosystems of services (Vargo and Lusch, 2011; Böhmann et al., 2014) (Figure 1). We posit these service ecosystems comprise users, platforms, frontend services, and backend services.

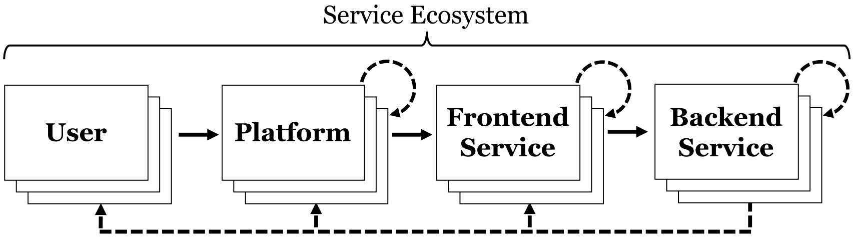


Figure 1. Adapted model of information privacy in service ecosystems (Conger et al., 2013)

Users are the individuals with his/her personal information interacting on the platform. Information privacy of users can be related to an individual's ability to personally control information about oneself (Stone et al., 1983; Milberg et al., 1995). In this context, privacy risks and privacy concerns exist in the decision-making of users whether to share data (Malhotra et al., 2004; Dinev and Hart, 2006). However, decision-making implies both choice and consent, while in reality users have incomplete and asymmetric information about actors accessing their personal data, which results in an inability to act in a self-interested manner (Acquisti et al., 2015).

Platforms facilitate multi-sided interactions of different actors (Böhmann et al., 2014; Parker et al., 2016), typically between users and frontend services (Hagiu and Wright, 2015). In this article, we define platforms as a set of digital resources that enable value-creating interactions between frontend services and users (Parker et al., 2016). Examples for platforms are Facebook, iOS and Android, which are not limited to the set of digital, technical resources and include also the governance of this set. In this context, Apple represents the platform provider of the platform iOS which includes digital resources like the operating systems and the AppStore. Platform providers define the governance rules that attempt to balance platform usage (Constantinides et al., 2018). Here, platforms act as intermediaries and can exert control over how data and service flows between platform participants (Van Alstyne et al., 2016; Constantinides et al., 2018). Examples for this are Apple's rules for developers (Apple, 2017).

Frontend services access and interact on these platforms and offer their services to users in form of e. g. applications. Backend services are implemented by frontend services for application performance management, additional features like 'Login with Facebook' but also to increase income streams through implementing advertisement companies.

The actors in the service ecosystems can appear not just once but several times; for instance, a frontend service integrates various backend services (Razaghpanah et al., 2018). The interactions of the actors result in the diffusion of personal data in hyper-connected services ecosystems (Razaghpanah et al., 2018). In this context, the term "service ecosystems" is used to indicate that the included actors interact not only with well-designed information systems. At some points, actors make decisions that have consequences for other actors on subsequent (design) decisions. In total, the multi-actor information-processing in service ecosystems have consequences for information privacy of users. That poses particular challenges (Kurtz et al., 2018), where it remains to be seen to what extent the GDPR in form of data regulation can cover these challenges.

11.2.2 GDPR

In May 2018 the GDPR (GDPR, 2016), drafted already in 2016 after long discussion in the so called trialogue (between European Commission, European Parliament and the Council), was implemented after a two-year transitional phase. Its aim is to protect EU citizens' privacy in the digital world in the form of data protection and data regulation (Danezis et al., 2015). One of its important changes in comparison to the Data Protection Directive it replaced is an expanded scope of applicability, binding even companies outside of the EU when they process EU citizens' data.

On the most fundamental level data protection offers a binary system of two opposed actors: a controller and a data subject. A person processing personal data and the person to whom this data is relating. However, just as the service ecosystems offer a more complex reality of actors, the GDPR does not limit itself to this traditional scenario and offers more possible roles. In the following paragraph we give a short introduction to those roles and the responsibilities they bring with them.

According to the GDPR (GDPR, 2016, Art. 4 No. 7)[7], a *Controller* is any (natural or legal) person that, alone or jointly, determines the purposes and means of the processing of personal data. It is a role that is always determined in relation to a specific act or set of acts of processing (GDPR, 2016, Art. 4 No. 2). These can include the collection, recording, organization, structuring, storage, adaptation, usage,

[7] All further articles without designation are those of the GDPR.

disclosure, cf. In order to limit risks from acts of processing, the GDPR enjoins controllers with certain obligations that are meant to safeguard data subjects' rights. Most prominently, Art. 6 declares that every act of processing is in need of a legal basis, making it the controller's duty to make sure that and declare which one of the legal grounds listed in the provision applies.

Furthermore, certain organizational and technical measures need to be taken in order to ensure that the controller is also in compliance with all the GDPR's specific data protection and data security provisions and is able to prove said compliance at any time, as Art. 24 declares. This concretizes Art. 5 (2) which, in even more general terms, lays down the principle of accountability as one of the cornerstones of lawful processing. What makes the determination of the scope of these obligations difficult is the rather abstract way in which they are defined.

The measures that a controller has to take are dependent on the scope, context and purpose of the processing and on the severity and the probability of occurrence of the risks for data subjects' rights and need to be "suitable" and "appropriate". In summary, there is no general way of defining measures that every controller can take without taking into account the context and specifics. The specific provisions whose compliance these measures are safeguarding are numerous. They include data subjects' rights like the processors' obligation to information, Art. 13, 14, or the right to be forgotten, Art. 17.

According to Art. 4 No. 8, a *Processor* is any natural or legal person, public authority, agency or other body that processes data on behalf of the controller. While exercising physical control over the processing act itself, a processor has no own agency and only acts upon the controller instructions (Martini, 2018). Referring back to the definition in Art. 4 No. 7, this means that the determination of purposes and means of processing have to remain with the controller. While Art. 28 (3) additionally states that controller and processor have to formally bestow this role on the latter through a contract that contains the details of their cooperation, the classification is independent from such formal designations and primarily follows factual elements (EuropeanCommission, 2010, p. 8). This provision follows the technical reality of the outsourcing of know-how and certain steps of action. Consequently, the GDPR privileges such cooperation in two ways: the transmission of data from a controller to a processor and the subsequent handling through the processor do not fall under Art. 6 and thus are still covered by the original legal ground declared by the controller; processors do not need to meet the same obligations that controllers do. Instead, the GDPR deems it sufficient to put onto the controller the duty of responsible selection, Art. 28 (1), and oblige processors to keep records of their processing and ensure basic safeguards of data security, Art. 30, 32.

According to Art. 26, two or more actors can be *Joint Controllers* for an act of processing where they jointly determine its purposes and means. Consequently, the GDPR's controller obligations affect all joint controllers, although not necessarily equally, as the ECJ notes: "operators […] may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case" (ECJ, 2018). On the other hand, data subjects can direct their claims on and execute their subject rights against whichever controller they like or can reach more easily, according to Art. 26 (3).

11.3 Case Studies

In the following, we analyze two cases to identify the reasons for the diffusion of personal data in service ecosystems. In this context, there has already been a call that "[…] researchers could explore current privacy violations and their consequences and factors that lead to organizational practices regarding information privacy" (Belanger and Xu, 2015, p. 576). We selected cases which have been published in news. This shows that a virulence is present and has been brought to public attention. We want to prove where critical aspects, blind spots or violations of expectations exist.

To this end, we examine the cases at actor level, from both a technical and legal point of view. Technically, we examine systems settings, interfaces and data flows. This is the basis for the legal analysis. We classify the actors according to the GDPR, which had not yet come into force at the time of the cases. However, the analysis aims at preventing such cases nowadays. The actor obligations following from it pose the most interesting question. Here, the tracks are being laid down for two further questions: which of the actors were responsible in what way and did they meet their responsibilities?

11.3.1 "Facebook, 'Digital Life' and Cambridge Analytica"

The case of Cambridge Analytica and Facebook has been widely covered in the media, also due to the hearing of Facebook CEO Mark Zuckerberg before the United States House of Representatives Committee on Energy and Commerce (Zuckerberg, 2018). In this case, users used the frontend service application 'Digital Life' on the platform Facebook. By granting the requested rights to this app, users disclosed to it their own data as well as the opportunity to access the data of their friends on Facebook. While only 270,000 users directly used the quiz app, the data of in total 87 million Facebook users was unveiled to the app (Frier, 2018). At the time that the case was formed, users had to manually opt-out of sharing their data with the apps used by friends (McCausland and Schecter, 2018). Where users did not do that, Facebook enabled apps to access their data. After that, 'Digital Life' did not comply with the platform policy to share such data. The developer of the app shared data to the backend service

Cambridge Analytica, which used it to target users on Facebook to deliver individualized advertising (Rosenberg et al., 2018).

Technically, Facebook stores user data on servers around the world. Other services acting on the platform can access user data by the Graph API of Facebook. During the time of the case, the API version 1.0 was implemented. Services in form of apps could request a huge range of user and user's friends' data (Hartmans, 2018) caused by the extended data access permissions of the API. The 1.0 version was launched in April 2010 and was available in the form up to April 2015 (Albright, 2018). After that, the Graph API v2.0 was introduced. With this API, requests of frontend services on user friends' data, which previously depicted the critical data flow in the case, returned no data to the services (Kaşlı, 2014). At this point, Facebook had restricted the outgoing data to frontend services.

From a legal point of view, data of affected users were initially on the servers of Facebook. By allowing apps access via Graph API, Facebook opened up the possibility for apps to request data. Thus, concerning the transmission of data from Facebook to an app like 'Digital Life', Facebook at least determined the means of processing by offering the necessary technical infrastructure including possible limitations. Considering that the existence of apps on the Facebook platform – and in extension the usage of user data by these apps – is part of Facebooks business model, it does not seem farfetched to classify them as a controller pertaining to this act of processing. Whether or not 'Digital Life' is a separate controller next to them or whether they are joint controllers can be left aside at this point. Consequently, Facebook would be fully responsible for adhering to the GDPR's provisions in regard to these transmissions.

'Digital Life' directly collected two kinds of data: profile data of users that installed and used the app, their friends' profile data that represent the critical data in this case as well as data when a user interacted with the app. Profile data was already stored on Facebook's servers while the second category of data were created through the usage of the app (and presumably saved by Facebook). In both cases the frontend service was completely responsible for determining the purpose of data requests. Since this was known to and approved by Facebook a classification as joint controllers should be made, at least for the first part of processing (sharing of data from Facebook to 'Digital Life').

Cambridge Analytica bought the collected data from 'Digital Life' to provide target advertisements for elections and other purposes on behalf of their own clients. Through this collection they obtained control over data and started acting as an (independent) controller in their own right.

11.3.2 "iOS, AccuWeather and RevealMobile"

In the second case, the platform iOS transmitted via the application AccuWeather user device data which were used to approximate users' location by the backend service called RevealMobile. This seems to be in contrast to the permissions revoked by the user in iOS to access her/his location. The privacy statement of the frontend service AccuWeather declared that the application and implemented backend services can use methods to approximate users' locations (AccuWeather, 2017). Backend services were not named in detail. However, RevealMobile states that the technology the company uses "[…] sits inside hundreds of apps […]" and "[i]t turns the location data coming out of those apps into meaningful audience data […]" (RevealMobile, 2016, p. 2). More precisely, RevealMobile focusses on mobile marketing by using such data to segment user groups for advertising (RevealMobile, 2017).

Technically, the backend service RevealMobile gained access to data of the iOS platform of a user when s/he installed the application of AccuWeather, which was after a review of Apple available in the AppStore. In this application the RevealMobile SDK is implemented. The user specifies when starting the application for the first time whether or not the application can access the location via the location services of iOS. These location services are explained in the iOS settings in the following way: "Location Services uses GPS, Bluetooth, and crowd-sources Wi-Fi hotspot and cell tower locations to determine your approximate location (…)". Users rejected to share this location services data. Despite this, the backend service on iOS took a detour to approximate users' location. In this case, the Wi-Fi router name, BSSID (Basic Service Set Identification which corresponds to the MAC address of the currently connected wireless access point) as well as the Bluetooth status was transmitted from the iOS platform to the application (Strafach, 2017). During a testing period of 36 hours, the data was sent 16 times to the company RevealMobile (Strafach, 2017). Using this data, the company was then able to determine the location of

the user by enriching it with public databases about stored locations of wireless access points (Vaughan-Nichols; Wu et al., 2015). On Apple's website (which corresponds to the iOS version of the case) (Apple, 2017) about location services in iOS, however, this is presented differently to the user. Thus, it is stated "Tap Don't Allow to prevent access" (Apple, 2017; Apple, 2018). A user can derive from this, that if s/he deactivates access to location services to applications, this is technically implemented in such a way that iOS does not return any location data or data for location approximation to applications. It is important to stress, however, that on a technical level, Apple's statement still holds: RevealMobile did not gain direct data through Apple's location services, instead bypassing this access channel.

The legal classification in this case is more complex than in the first case. Since affected data was directly transmitted from the phone's operating system to RevealMobile in the moment it was accrued, no active act of processing by iOS had happened before. Data was only stored on the user's phone, not on Apple servers. Nevertheless, the platform iOS provided the technical infrastructure and the legal agreement that determined how and in which scenarios apps can access certain types of data. In addition, the way the existence of apps is part of iOS's appeal to users and therefore heavily important for Apple, can be compared to the way Facebook offers apps access to users' data. A classification of the platform provider Apple as processor, if not controller, should therefore not be ruled out.

One important difference to the first case concerns the type of data and data transfer in the context of users' actions. While on Facebook the overwhelming part of affected data had been shared and therefore transmitted to Facebook – although not to 'Digital Life' when the users' friends are in question – consciously and voluntarily, this was not the case with iOS. On the contrary, users explicitly declined the transmission of what Apple labeled "location data" to AccuWeather, thereby implicitly voicing their rejection of the transmission of any data that might be used to determine the user's location. Of course, one might argue that the accruement of WiFi and Bluetooth data is a technical necessity and therefore covered by the users' general intention of using the phone with all its features. Still, this data would not be necessary for a functioning weather application – making the user ask for a specific city's or area's weather is less comfortable for him but might still be what he wants.

On the one hand, the platform's involvement is smaller here than in the first case since Apple does not initially determine the precise purpose of the subsequent processing. On the other hand, it is the deliberate design of the platform that allows apps to directly access particular data. The way Apple actively changes this design to accommodate disclosed cases of misuse can be seen in the way the access to iOS devices' MAC addresses was deprecated in iOS 7 (Apple, 2017), the access to MAC addresses of network devices (such as WiFi routers) barred in iOS 11 (Butts, 2017). Apple is thereby at least contributing to the determination of the means through which this data is processed. It is also, at least partly, determining the general purpose on an upstream level by opening up the possibility for approved apps to access this data in the first place and giving app developers specific terms of use to sign, thereby specifying which purposes are allowed and which are not. Apps that violate the Apple License Agreement or are in conflict with some of the App Review Guidelines get rejected and don't make it into the AppStore. This is also what distinguishes a controlled platform like iOS from an open one like Windows, where a user can freely install programs that weren't vetted and officially included in an AppStore equivalent. While this level of involvement still does not mirror the one typically associated with data controllers determining all purposes and means of processing, it does not mean that a classification as controller is impossible. As Art. 29 states: even when at the micro-level the actions of different actors "appear as disconnected, as each of them may have a different purpose", they can still on the macro-level be "pursuing a joint purpose or using jointly defined means" (EuropeanCommission, 2010, p. 20).

This interpretation of the GDPR's roles in iOS's case is also in line with the significance the European Court of Justice (ECJ) attributes to the classification of actors as controllers and processors for the effective protection of the affected users' rights and freedoms (ECJ, 2018). This means that one criterion for deciding between possible classifications is the way the respective roles allow for a better or worse protection of the users' rights. The judgement is based on the now obsolete EU Data Protection Directive but its results, at least concerning this aspect, can be applied to the GDPR as well. This also applies to the ECJ's notion that where several operators are jointly responsible, it is *not* required that each of those necessarily have access to the personal data concerned (ECJ, 2018). Referring back that data is accrued from the users' phone without their awareness and that iOS provides the technical infrastructure that constitutes the means for the processing and consequently has the possibility of somewhat influencing possibilities and limitations of access, it therefore to us seems commanded to classify them as a controller in relation to these acts of processing.

For the classification of the frontend service the course of data is not as trivial as in the other case. In this case AccuWeather never got its hands on the data. Instead, RevealMobile had direct access to the data of the platform and accrued them in a straight line from there without a data flow through AccuWeather servers. The way that RevealMobile was able to do that was due to their SDK being implemented in the code of the AccuWeather app, thus an active decision of the app's organization. This raises the question if a classification as either controller or processor is possible even when the actor in question didn't consciously know how much access to certain kinds of data it allowed another actor. Such classification could be constructed as a kind of accountability through negligence, triggered by implementing an SDK without exact knowledge of what the code is able to request. The attribution of responsibility connected to this role follows the affected actor's control over the processing act in question. Here, AccuWeather once made the conscious decision of implementing RevealMobile's SDK for clearly specified purposes. Without this decision RevealMobile wouldn't have had access to users' data. AccuWeather was therefore heavily involved in determining both purposes and means of the processing and should be classified as (joint) controller as well. The fact that they not have known about data that was accrued does not change anything about that but becomes relevant when checking for compliance of the obligations connected to the role.

RevealMobile actively accrued data from the users' phone for purposes they determined on their own. They used infrastructure provided by iOS and by AccuWeather, but for their own purpose and in situations that were contractually (if not technically) forbidden and therefore clearly acted as a controller. In this context, a classification of Apple as joint controller seems the most plausible.

11.4 Discussion

At this point we compare the two cases with regard to their factual circumstances (Table 1) and demonstrate differences and similarities by looking at the actors, their motivations and the ways they had the possibility to do things differently, including reciprocal consequences and effects. Hereafter, we examine to what extent the GDPR's controller obligations are able to reflect the differences.

Both platforms, Facebook and iOS, offer an infrastructure that brings together users and different kinds of services, while also offering their own services. Through technical measures both can handle their infrastructure to limit the ways external services can access personal data. In both cases personal data was disseminated and, in both cases, this could have been prevented technically but was not.

One major difference concerns the way that user knowledge and actions were reflected in the processing. In the first case, friends of those users that actively used the 'Digital Life' application did not explicitly deny Facebook this usage of their data. However, the option of sharing their data, with their friends' apps was hidden under multiple layers of settings and by default turned on, meaning a user had to actively "opt out" of this usage (McCausland and Schecter, 2018). This affected data was actively shared by users to Facebook. In the second case, users were specifically asked whether they want to share their location with the app. However, even when sharing was rejected, data was transmitted directly from iOS via the AccuWeather app to the backend service RevealMobile with which the location was approximated. This might seem like the bigger breach since the users' explicit rejection was violated. However, implying the users' consent by forcing them to opt out of the sharing and hiding the respective option under multiple layers of settings instead of asking them when a decision becomes relevant effectively keeps the majority of users from ever consciously making that decision. In the first case, Facebook had been the subject of public criticism. In the other case, the focus was usually on AccuWeather and RevealMobile. However, the analysis in this article reveals that Apple as a platform provider can be made responsible due to its crucial role regarding the diffusion of personal information. At least since the GDPR is in effect.

As described above, we propose a classification of the platforms as joint controllers in both examined cases in order to reflect their prominent role in the diffusion of users' data throughout the respective ecosystems. Following this classification certain obligations are inflicted by the GDPR. We will introduce these obligations below. In this context, another question arises: how should these obligations be distributed amongst the controllers and how can they be adhered by them? While the question of distribution can to some extent be decided by the controllers through contractual arrangements, the external distribution in relation to the affected data subject has to always mirror the impact on his/her rights. This means that, while a data subject can demand the fulfillment of obligations from each controller individually, it makes sense to encourage each controller to fulfill those obligations that are connected to its area and scope of involvement in the processing, since this ensures the highest probability of overall compliance and therefore safeguards the data subjects' rights in the most efficient way.

Table 1. Overview of the techno-legal analysis with the focus on the two platforms

	Classes	"Facebook, 'Digital Life' and Cambridge Analytica"	"iOS, AccuWeather and RevealMobile"
Techno	*Data Storage*	Facebook stored user data on servers	Data was stored on user's phone, not on Apple servers
	Interface	'Digital Life' accessed user data on the platform via the Graph API	RevealMobile used iOS functions to access WiFi data
	Third Party Data Access	Subsequent data transmission of 'Digital Life' to Cambridge Analytica	Transmission from iOS via integrated SDK of RevealMobile in the AccuWeather app
	Data Type	App users' profile data, app usage data, app user's friends' profile data	Name, BSSID of Wi-Fi connection, Bluetooth status
	Data Amount	270,000 app users' profile and usage data, 87 million app user's friends' profile data	In 36 hours, data was transmitted 16 times
Legal	*User Consent*	Default setting of sharing data with the apps used by friends'	User's rejection of sharing location data
	User's Role in Data Sharing	Overwhelming part of the affected data was shared by users to the platform	No settings options except to disable WiFi or Bluetooth functions
	Infrastructure	Facebook offered the technical infrastructure including possible limitations	iOS provided the technical infrastructure that determined how and when apps can access data
	Purpose of Processing	'Digital Life' was completely responsible for the purpose of data processing	AccuWeather determined the purpose, Apple agreed by publishing the app in the AppStore
	Means of Processing	Facebook determined it by the design of the platform that allows apps to access data	iOS determined it by providing the technical infrastructure and had the possibility of influencing the data access
	Appeal	Existence of apps on Facebook– the usage of user data by these apps – is part of Facebook's business model	Existence of apps is part of iOS's appeal to users
	Platform Classification	Joint Controller	Joint Controller

11.4.1 "Facebook, 'Digital Life' and Cambridge Analytica"

Here, the platform Facebook offers the infrastructure for the processing of the personal data of its users and therefore determines the means. It also sets the purpose for the initial collection of data by encouraging users to add personal information to their profiles and to interact with the platform and other users. Consequently, they are obliged to present a legal ground (GDPR, 2016, Art. 6) and to inform their users about the ways they plan to use this data (GDPR, 2016, Art. 13). Concerning the legal basis, Facebook lists different kinds of potential bases on its website for different intended usage cases (Facebook, 2018). Since users have the possibility to opt out of the sharing of their data to apps that their friends are using, the basis of consent (GDPR, 2016, Art. 6 No. 1) seems most likely. However, since this option was automatically activated when signing up for Facebook and had to manually be turned off, the legal effectiveness of such consent seems very doubtful. Amongst other criteria, consent must be given freely and by an informed data subject. In addition, Art. 7 No. 2 states that where a consent is given through a statement that includes other matters. Where a user automatically and without explicitly opting in consents to sharing his/her data through friends using apps when s/he signs up to Facebook, no such manner can be seen. Furthermore, the ideal of data protection by default in Art. 25 (2) is not respected. It is highly doubtful that Facebook had legal grounds for sharing this data with apps.

The second problem concerns the lack of information that users received when their data were shared with 'Digital Life' and then with Cambridge Analytica. Here, again, Art. 13 and 14 demand that data subjects get informed who gains access to their data and what is being done with it. On the one hand, obligating each of the controllers to directly inform affected users when they each gain access to data seems like a logical proposal. On the other hand, Facebook as a platform is still mediating the way this data is transmitted and has the closest connection to the affected users. They should, at least of the transmission to 'Digital Life', directly inform users. However, the information was delayed by years (Hern, 2018).

On the next level, the data transmission from 'Digital Life' to Cambridge Analytica happens outside of Facebook. It would thus be too harsh – and make no sense with regard to the effective safeguarding of user rights – to once again oblige Facebook to inform users. 'Your Digital Life' is both closest to the affected users and in the position to fulfill the obligation most easily.

In conclusion, Facebook would be responsible for providing suitable technical and organizational measures that allow the gathering of legally effective acts of user consent and the provision of information at each point where date is passed on to the next controller (GDPR, 2016, Art. 24).

11.4.2 "iOS, AccuWeather and RevealMobile"

In this case, missing or ineffective acts of consent were not the problem. Instead explicitly denied consent - expressed by denying access to all location data through the location services settings in iOS – was ignored. Therefore, the legal focus in this case must concern the question whose responsibility it had been to ensure that the current data flows through the app corresponded with the scope of what the users' consent allowed. This again falls under the obligation to "[i]mplement technical and organizational measures to ensure […] that processing is performed in accordance with [the GDPR]" (GDPR, 2016, Art. 24). This is such a general obligation that forcing only one of the three joint controllers to adhere to it would be wrong. Since the norm is heavily context-depended and therefore does not offer a "one size fits all" solution to compliance with the obligation, the question is which measures could have reasonably been demanded from iOS in this case and could be demanded in similar cases.

In conjunction with this question one might look at the iOS settings for location services iOS already offers its users. By anchoring these settings within the phone's operating system, iOS takes up a mediating role between user and app. The user expresses the part of his consent that concerns location data in the broadest sense through iOS which passes it on to the respective app. Therefore, it would be consequential to obligate iOS to fill out this role appropriately, by denying the flow of data to the app for all data that might be used to approximate or determine the location of the user, on a technical level, as far as such a technical limitation of data flow can be achieved by reasonable measures. In addition to the case, other technical possibilities to determine the location of users (Mosenia et al., 2017) must also be excluded. On the other hand, such an unmitigated denial of all potentially "damaging" data would certainly not be feasible. Some data is fundamentally neutral and only becomes sensitive by third parties (mis)using them in contrast to the agreed purpose, a purpose for which it might in turn be necessary to use. This conundrum is beautifully shown in the example of iOS's complete ban of using network devices' MAC addresses in iOS 11 (Butts, 2017).This ban, a result of apps' misuse of this data, made many network scanning apps inoperable as they now couldn't do what they were designed to do.

Still, insisting on measures on the part of iOS seems to us inevitable. Even AccuWeather's privacy statement refers the user with regard to possible solutions when it states that if users "[…] turn off 'Location Services' or a similar setting that controls GPS functionality, the device still may automatically send or receive this other information as long as you [the user] have these other communications types enabled. [The user] should read the instructions related to [his/her] device, operating system or browser to learn about how to control the information [his/her] device may transmit" (AccuWeather, 2018).

In conclusion, no specific recommendation of technical and organizational measures that could downright and without a doubt prevent any diffusion of data that could potentially be used to infer the location can be made. Neither can we, consequently, say whether Apple violated its controller obligations or not. While there are several reasons for negating this question, the fact that access possibilities to MAC addresses were restricted in iOS 7 and iOS 11 indicates that Apple reacted to the disclosure of this problem. And even while there is no definitive solution, the mere examination of Apple as a potential controller and the subsequent discussions about the scope of their obligations seems to us like a fruitful starting point for discussion. Furthermore, establishing rules regarding procedures and transparency might be an advantage, where the knowledge of when and through which motivation Apple reacts lies with Apple alone.

11.4.3 Position privacy-preserving solutions

Building on the findings above, we posit that several generalizations can be made. First, and arguably not that surprising, platforms tend to be the actors within the service ecosystems described in 2.1. that have the most leverage when it comes to introducing efficient solutions that improve the preservation of information privacy within these ecosystems. As the gatekeepers regulating who is a part of an ecosystem and what is allowed there, changes of rules affect all actors and can therefore steer away from privacy-endangering trends.

Second, platform providers can be so heavily involved in the process of selecting the players that get allowed that it seems possible to classify them as controllers according to the GDPR and therefore subject them to obligations that force them to find good and effective solutions for privacy risks while making those solutions and their formation process transparent. While this paper discusses specific cases, these findings could potentially be applied to other similarly controlled platforms as well.

Third, it is apparent that imposing such obligations on platform providers cannot be the universal answer. Technical solutions possible today are always limited, as Apple's changes in disclosing MAC addresses in iOS 11 and the ensuring critique showed. Putting enhanced obligations on platforms also increases their power over smaller actors, thereby solidifying structures that might be problematic on other levels and leading to unexpected secondary effects.

Still, we envisage that with shining the light on platform providers as potential controllers we can start a public discourse about how far their obligations can reach, how they can be met and how they can be efficiently complemented by the obligations imposed on frontend services. The development of codes of conduct and certification schemes according to Art. 40-43 could help with the standardization.

11.5 Conclusion and Outlook

Taking into account the results of this article, platforms bear a great responsibility for the diffusion of personal data in service ecosystems. With a view to media, the case of Facebook, 'Digital Life' and Cambridge Analytica has been widely covered. It becomes clear that responsibility is seen on the side of Facebook which is also made clear in this article. The thrilling item in this story, however, is the role of the sibling Apple within the scope of its platform iOS. In accordance with the techno-legal analysis, we came to the same classification as a joint controller.

In total, such platforms take up a big role in the agency of the diffusion of personal data in today's interconnected services. At first glance it is positive for information privacy to read news such that Apple restrict using network devices' MAC addresses in iOS 11 (Butts, 2017), that "Facebook suspends 200 apps as part of investigation into data misuse" (Levin, 2018). However, these news also show the responsibility and scope of actions of platforms. It is questionable that platform rules and compliance with them are checked only occasionally to be followed by actions – this should be done comprehensively and continuously. To return to the beginning of this article – from a legal perspective Tim Cook finds himself with Apple in a very similar situation as Facebook. We make the call that responsibilities according the GDPR and outlined obligations should be debated for all platform siblings, in the whole GDPR family.

11.6 Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality in the project Information Governance Technologies under the reference LFF-FV 34.

11.7 References

AccuWeather (2017). 'Privacy Statement'. https://web.archive.org/web/20170831185056/https:/www.accuweather.com/en/privacy (visited on August 20 2018).

AccuWeather (2018). 'Privacy Statement'. https://www.accuweather.com/en/privacy (visited on03.06. 2018).

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). 'Privacy and human behavior in the age of information', Science, 347(6221), 509-514.

Albright, J. (2018). 'The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle'. (visited on01.06.2018 2018).

Apple (2017a). 'Apple Developer Program License Agreement‘. https://download.developer.apple.com/ Documentation/License_Agreements__Apple_Developer_Program/Apple_Developer_Progra m_License_Agreement_20180604.pdf (visited onMay 20 2018).

Apple (2017b). 'iOS 7: Understanding Location Services‘. https://support.apple.com/en-en/HT201357 (visited onJune 04 2018).

Apple (2017c). 'What's New in iOS - iOS 7.0‘. https://developer.apple.com/library/archive/ releasenotes/General/WhatsNewIniOS/Articles/iOS7.html (visited onSeptember 01 2018).

Apple (2018). 'Turn Location Services and GPS on or off on your iPhone, iPad, or iPod touch‘. https://support.apple.com/en-au/ht207092 (visited onJune 04 2018).

Belanger, F. and Xu, H. (2015). 'The role of information systems research in shaping the future of information privacy', Information Systems Journal, 25(6), 573-578.

Böhmann, T., Leimeister, J. M. and Möslein, K. (2014a). 'Service Systems Engineering', Business & Information Systems Engineering, 6(2), 73-79.

Böhmann, T., Leimeister, J. M. and Möslein, K. (2014b). 'Service Systems Engineering: A field for future Information Systems Research', Business Information Systems Engineering, 6(2), 73-79.

Butts, J. (2017). 'Thanks to Misuse, Apps Can’t View MAC Addresses on iOS 11‘. https://www.macobserver.com/news/product-news/apps-cant-view-mac-addresses-on-ios-11/ (visited onSeptember 01 2018).

Conger, S., Pratt, J. H. and Loch, K. D. (2013). 'Personal information privacy and emerging technologies', Information Systems Journal, 23(5), 401-417.

Constantinides, P., Henfridsson, O. and Parker, G. G. (2018) 'Introduction—Platforms and Infrastructures in the Digital Age',

Dance, G. J. X., Confessore, N. and LaForgia, M. (2018). 'Facebook Gave Device Makers Deep Access to Data on Users and Friends‘. https://www.nytimes.com/interactive/2018/06/03/technology/ facebook-device-partners-users-friends-data.html (visited on08.06. 2018).

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. L., Tirtea, R. and Schiffner, S. (2015). 'Privacy and Data Protection by Design-from policy to engineering', arXiv preprint:1501.03726.

Dinev, T. and Hart, P. (2006). 'An extended privacy calculus model for E-commerce transactions', Information Systems Research, 17(1), 61-80.

ECJ (2018). 'C-210/16: ULD ', European Court of Justice 2018(June 08).

EuropeanCommission (2010) Article 29 Data Protection Working Party

Facebook (2018). 'Legal Bases‘. https://www.facebook.com/about/privacy/legal_bases (visited onJune 09 2018).

Frier, S. (2018). 'Facebook Says There May Be More Cambridge Analytica-Sized Leaks‘. Bloomberg. https://www.bloomberg.com/news/articles/2018-04-26/facebook-says-there-may-be-more-cambridge-analytica-sized-leaks (visited on2018).

GDPR (2016). 'General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46', 59, 1-88.

Guardian, T. (2018). 'Facebook shared user details with firms after cutting developers' access‘. https://www.theguardian.com/technology/2018/jun/09/facebook-shared-user-details-firms-developers-access-cut-off (visited on10.06. 2018).

Hagiu, A. and Wright, J. (2015). 'Multi-sided platforms', International Journal of Industrial Organization, 43, 162-174.

Hartmans, A. (2018). 'It's impossible to know exactly what data Cambridge Analytica scraped from Facebook‘. https://www.businessinsider.com.au/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3 (visited onJune 01 2018).

Hern, A. (2018). 'How to check whether Facebook shared your data with Cambridge Analytica‘. https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica (visited onMay 28 2018).

Kaşlı, C. (2014). 'Facebook Graph API v2.0‘. https://stackoverflow.com/questions/23417356/facebook-graph-api-v2-0-me-friends-returns-empty-or-only-friends-who-also-u (visited on30.05.2018 2018).

Kurtz, C., Semmann, M. and Böhmann, T. (2018a) 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors', in Americas Conference on Information Systems, New Orleans,

Kurtz, C., Semmann, M. and Schulz, W. (2018b) 'Towards a Framework for Information Privacy in Complex Service Ecosystems', in International Conference on Information Systems (ICIS), San Fransisco,

Levin, S. (2018). 'Facebook suspends 200 apps as part of investigation into data misuse‘. https://www.theguardian.com/technology/2018/may/14/facebook-apps-suspended-privacy-scandal-cambridge-analytica (visited on10.06. 2018).

Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004). 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model', Information Systems Research, 15(4), 336-355.

Martini, M. (2018) 'Art. 28', Beck'sche Kompaktkommentare BDSG - DSGVO,

McCausland, P. and Schecter, A. R. (2018). 'Cambridge Analytica harvested data from millions of unsuspecting Facebook users‘. https://www.nbcnews.com/news/us-news/cambridge-analytica-harvested-data-millions-unsuspecting-facebook-users-n857591 (visited onMay 20 2018).

Milberg, S. J., Burke, S. J., Smith, H. J. and Kallman, E. A. (1995). 'Values, Personal Information Privacy, and Regulatory Approaches', Communications of the ACM, 38(12), 65-74.

Mosenia, A., Dai, X., Mittal, P. and Jha, N. (2017). 'PinMe: Tracking a Smartphone User around the World', IEEE Transactions on Multi-Scale Computing Systems.

Parker, G. G., Van Alstyne, M. W. and Choudary, S. P. (2016) Platform Revolution: How Networked Markets Are Transforming the Economyand How to Make Them Work for You, WW Norton & Company.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C. and Gill, P. (2018). 'Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem'.

RevealMobile (2016) The location of black friday - Using mobile location data and beacons to measure retail shopping behavior.

RevealMobile (2017). 'RevealMobile Website‘. https://revealmobile.com (visited onAugust 15 2018).

Rosenberg, M., Confessore, N. and Cadwalladr, C. (2018) 'How Trump Consultants Exploited the Facebook Data of Millions', The New York Times, 17.03.2018,

Stone, E. F., Gardner, D. G., Gueutal, H. G. and Mcclure, S. (1983). 'A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations', Journal of applied psychology, 68(3), 459-468.

Strafach, W. (2017). 'Advisory: AccuWeather iOS app sends location information to data monetization firm'. https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870 (visited onAugust 21 2019).

Van Alstyne, M. W., Parker, G. G. and Choudary, S. P. (2016). 'Pipelines, platforms, and the new rules of strategy', Harvard Business Review, 94(4), 54-62.

Vargo, S. L. and Lusch, R. F. (2011). 'It's all B2B… and beyond: Toward a systems perspective of the market', Industrial Marketing Management, 40(2), 181-187.

Vaughan-Nichols, S. J. 'How Google--and everyone else--gets Wi-Fi location data'. http://www.zdnet.com/article/how-google-and-everyone-else-gets-wi-fi-location-data/ (visited onNovember 19 2017).

Wong, J. C. (2018). 'Apple's Tim Cook rebukes Zuckerberg over Facebook's business model'. https://www.theguardian.com/technology/2018/mar/28/facebook-apple-tim-cook-zuckerberg-business-model (visited onMay 10 2018).

Wu, Y., Sapiezynski, P., Stopczynski, A., Gatej, R. and Lehmann, S. (2015). 'Tracking Human Mobility Using WiFi Signals', PloS one, 10(7), e0130824.

Zuckerberg, M. (2018). 'Testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook', United States House of Representatives Committee on Energy and Commerce, (Hearing before the United States House of Representatives Committee on Energy and Commerce).

12 Article No. 4 (Kurtz et al. 2020)

Kurtz, C., Wittner, F., Vogel, P., Semmann, M., & Böhmann, T. (2020). Design Goals for Consent at Scale in Digital Service Ecosystems. In Proceedings of the 28th European Conference on Information Systems (ECIS2020) – A Virtual AIS Conference.

Abstract

Digital services have undergone a shift to multi-actor constellations characterised by the utilisation of personal data. By involving external actors, service capability and variety increase but so does the number of actors that gain access to personal data. Here, privacy policies are legal documents that serve two primary functions: specifying the purpose and details of data processing in a binding manner and informing users about it. Privacy policies therefore have special importance in which the processing is based on user consent. In a case study of the platform eBay, we identified 18 problems that point out difficulties in achieving consent in a meaningful way in today's large-scale and massively interconnected digital service ecosystems. Based on these problems, the design goals are determined which help to find meaningful consent in digital service ecosystems. These goals include notifications for changed purposes of data processing in ecosystems or the reasonability of time needed for consent in relation to the usage time of the service. Thus far, no legal limits govern the reasonability of efforts for consent to privacy policies. This requires a fundamental rethinking of the concept of consent or far-reaching automation of privacy-related legal acts.

12.1 Introduction

The paradigm of a dyadic relationship between an individual and a single organisation is no longer valid in digital service interaction (Riedl et al., 2009, Vargo and Akaka, 2012). Digital interconnectivity manifests itself in individuals exposed to a broad range of actors when using a single digital service (Razaghpanah et al., 2018, Binns et al., 2018, Libert, 2018). These various actors are involved for different reasons, such as improving the service by providing analytics insights, adding functionality, or providing streams of income via, for example, advertisements (Kurtz et al., 2018b). In this context, personal data are shared with involved third parties. A common form for lawful processing of these personal data is to obtain the permission of an individual to receive consent (GDPR, 2016). In this relation, privacy policies are binding legal documents. They bind the data controller (the person responsible for the processing) to the purpose laid out in them and serve as the basis for ensuring that a service user is informed about data processing when providing consent. However, the importance of privacy policies far exceeds the attention that users paid to them, as individuals suffer from consent fatigue (Schraefel et al., 2017). Individuals have too frequently to determine whether and to what extent to grant consent in everyday life.

A New York Times article felicitously illustrates the existing problems of 150 privacy policies (Litman-Navarro, 2019). Most of the analysed policies exceed a level of comprehensibility, even for people with a higher education. Policies are written in such a complex manner that they are more difficult to access than Immanuel Kant’s manuscripts (Litman-Navarro, 2019). A recent legal judgement indicates that Google's privacy policy does not conform to the General Data Protection Regulation (GDPR) due to its complexity and obscurity (Bahr, 2019). Already in 2016, 91% of questioned consumers believe that they have lost control of how their personal data is being used (Rainie and Duggan, 2016). Additionally, a study highlights the fear of data being transmitted to third parties as the most frequent issue preventing users from using an online service (Rohleder, 2015); these issues are in tension with the plethora of actors involved in contemporary digital services. A study of one million applications observed that a median of 10 third parties is included per application, and approximately 18% applications involve more than 20 third parties (Binns et al., 2018).

While digital services have undergone a shift towards multi-actor constellations, we question whether privacy policies can still pave the way for meaningful and informed consent. From a legal perspective, the limits governing the reasonability of the extent of privacy policies have hardly been tested. In addition, there is reason to believe that even when legal requirements are met, consent is still failing regarding the (regulatory) aims connected with it. We utilise a single case study of the platform eBay and derive design goals which cover the problems for consent which arise by digital service ecosystems. In our study, we address the gap originating from two directions. First, disseminating digital service ecosystems increasingly involve third parties. Existing studies address the occurrence of and statistics concerning third parties in privacy policies (Yu et al., 2016, Zimmeck et al., 2019, Libert, 2018). However, these studies do not address prescriptive design knowledge to overcome upcoming issues. Second, new solutions address existing problems of consent and policies (Tesfay et al., 2018, Wilson et al., 2016, Harkous et al., 2018). Nevertheless, these approaches do not address the effects of emerging digital service ecosystems. To this end, we present insights from an interdisciplinary study at the intersection of information systems research and law. Our findings indicate new dimensions of necessary effort in the act of determining whether and to what extent to grant consent for a digital service, located in a digital service ecosystem. Our results challenge the assumption that the form of privacy policies being used in digital service ecosystems is still manageable for an individual.

The following section begins by introducing the literature and background (Section 2). Afterwards, we describe the methodology used to determine design knowledge for consent in digital service ecosystems (Section 3). Based on the case study (Section 4), we determine prescriptive design goals (Section 5). We then discuss and legally assess our results (Section 6) before we draw a conclusion (Section 7).

12.2 Literature and Background

The form of services has shifted from single services to systems of services (Chandler and Lusch, 2015). In service systems, actors collaboratively create value in interactive configurations of mutual exchange (Vargo et al., 2008). Different technological and organisational networks are linked together for joint service provision. Within these networks, activities for integrating and exchanging resources are coordinated through institutional arrangements to achieve mutual value creation (Lusch and Vargo, 2014, Barrett et al., 2015). Service ecosystems encompass self-contained and self-adjusting service systems of resource-integrating actors (Lusch and Vargo, 2014). In digital service ecosystems, mediating platforms can establish the framework by connecting two or more interest groups (Van Alstyne et al., 2016, Bitner et al., 2008). Thereupon, platforms utilise network effects to capture, share and monetise various data sources within a service ecosystem (de Reuver et al., 2018, Hein et al., 2018).

From a user's point of view, personal data are consequently accessible by multiple actors in interaction with a digital service, as the focal element of a digital service ecosystem. We use the definition of 'personal data', declared in the GDPR as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (GDPR, 2016, Art. 4 (1)). The categories and nature of data being disseminated throughout a service ecosystem and its inhabitants can differ, as can the data's proximity to individual users. Depending on the purpose of a data recipient, data can be bundled, aggregated and even pseudonymised to differing degrees that may border on anonymisation. However, the GDPR's barrier for true anonymisation regarding data that was formerly personal is arguably high. Only when the data is so robust that no party can (e.g. through the combination of different data sets or inference of certain information) trace them back to individual users under any reasonable circumstance does the GDPR consider data to be no longer personally identifiable (European Commission, 2014). However, various de-anonymisation approaches exist and are continuously developed (Narayanan and Shmatikov, 2008, Ji et al., 2016, Paspatis et al., 2017, Di Luzio et al., 2016).

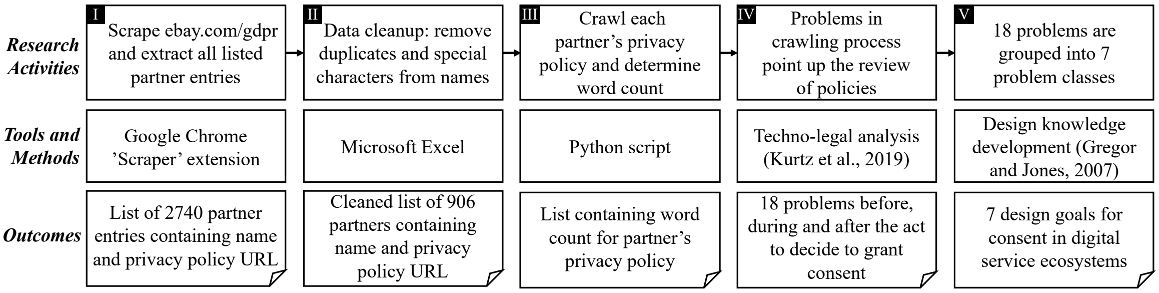
The goal of the GDPR, implemented in May 2018 after a two-year transitional phase, is to protect individuals regarding the processing of personal data pertaining to them (GDPR, 2016, Art. 1 (1)); thus, organisations are obliged to inform users when processing personal data pertaining to them (GDPR, 2016, Art. 13, 14). This typically occurs through organisations using privacy policies that are, most famously, linked to cookie or other prominent notices. Such policies inform a user about, for example, the types of data being processed, the purpose of the processing and possible recipients of further data transfers (GDPR, 2016, Art. 13 and 14). These obligations serve to making processing acts transparent and thereby enable users to exercise their informational privacy, as enshrined in the GDPR's data subject rights (GDPR, 2016, Art. 15-21). When the organisation in question wishes to base its acts of data processing on the consent of its users, its privacy policy serves another important purpose. Within the GDPR's framework for lawful data processing, consent is one – albeit arguably the most important and widely use – of six legal bases (GDPR, 2016, Art. 6 (1)). Processing can be lawful without a user's consent when inter alia, it is necessary for the performance of a contract or when its purpose serves the organisation's legitimate interests and the user's interests do not outweigh those interests. Consent as a legal basis is only accepted as such by the GDPR when it is expressed in the form of a 'freely given, specific, informed and unambiguous indication' (GDPR, 2016, Art. 4 (11)).

However, the assumption that the existing form of privacy policies achieves such imperatives is questionable. Findings identify that users as data subjects do not understand privacy policies and describe the practices therein (Reidenberg et al., 2015). This is driven, inter alia, by the difficulty of privacy policies (Ermakova et al., 2015). It follows that users cannot access the potential magnitude of harm, because users cannot build an expectation concerning when and how organisations are accessing and processing their personal data (Malandrino and Scarano, 2013). Moreover, some organisations exploit behavioural and psychological processes in privacy settings to promote data disclosure (Acquisti et al., 2015). This behaviour includes default settings with opt out rather than opt in to share data (Acquisti et al., 2015). In this relation, the phenomenon of individual's consent fatigue is increasing, which results in ineffective consent by accepting policies without informing oneself (Schraefel et al., 2017). Solution approaches introduce automatised methods of extracting user-relevant details from privacy policies by applying natural language processing and machine learning (Tesfay et al., 2018, Wilson et al., 2016). One example is the project pribot.org, which provides privacy policy summaries using deep learning (Harkous et al., 2018). Such approaches address the problem of the immense opportunity costs of users to read and understand privacy policies (McDonald and Cranor, 2008) and can be used for improved and easier content processing of privacy policies. Our design goals based on the case study (cf. Section 5) can be put into practice by combining such existing approaches to address the challenges posed by service ecosystems.

Digital service ecosystems with involved and emerging actors exacerbate the reservations and problems of privacy policies. An increasing number of third parties is involved in a single digital service (Razaghpanah et al., 2018, Binns et al., 2018, Libert, 2018, Kurtz et al., 2018a). In this context, the organisational view of how much service providers should share with third parties is investigated (Gopal et al., 2018). In addition, studies revealed the incongruous mismatch between the statements in organisations' privacy policies and the practices actually performed by involved third parties (Yu et al., 2016, Zimmeck et al., 2019). Based on a large-scale data set, an investigation identifies crucial findings regarding the massive third-party data collection, yet with fewer than 15% of attributed data flows disclosed in related privacy policies (Libert, 2018).

12.3 Research Methodology

The creation of design knowledge is fundamental for design science research (Legner and Löhe, 2012, Kuechler and Vaishnavi, 2008, Gregor and Jones, 2007). A design theory explains how an artefact should be constructed (Walls et al., 1992). However, no commonly accepted method exists for developing design knowledge and related theories (Baskerville and Pries-Heje, 2010, Fischer et al., 2010, Legner and Löhe, 2012). We utilise a case study to create design knowledge and have identified the platform eBay and its interconnected partner organisations as an exemplary manifestation of a digital service ecosystem. We conducted a case study appropriate for when the research focus is on contemporary events (Benbasat et al., 1987). A single case study approach is typically chosen to explore a significant phenomenon under rare or extreme circumstances which is representative of a situation (Yin, 2009). For our case study, eBay is particularly well suited, as it transparently provides an account of all involved third parties on a dedicated website. This is not the case for every platform or service provider involved in a digital service ecosystem. In some instances, the general term is utilised that third parties are involved but that actors and actions are not specified. Thus, the transparency of eBay's digital ecosystem allows for an in-depth investigation. The platform specifies a staggering number of third parties involved in data processing on www.ebay.com/gdpr (eBay, 2019a), which has access to eBay users' personal data.



	I	II	III	IV	V
Research Activities	Scrape ebay.com/gdpr and extract all listed partner entries	Data cleanup: remove duplicates and special characters from names	Crawl each partner's privacy policy and determine word count	Problems in crawling process point up the review of policies	18 problems are grouped into 7 problem classes
Tools and Methods	Google Chrome 'Scraper' extension	Microsoft Excel	Python script	Techno-legal analysis (Kurtz et al., 2019)	Design knowledge development (Gregor and Jones, 2007)
Outcomes	List of 2740 partner entries containing name and privacy policy URL	Cleaned list of 906 partners containing name and privacy policy URL	List containing word count for partner's privacy policy	18 problems before, during and after the act to decide to grant consent	7 design goals for consent in digital service ecosystems

Figure 1. Research approach

Our research approach is illustrated in Figure 1. For the data collection, conducted in August 2019, we utilised the Google Chrome extension 'Scraper' (chrome web store, 2019) as a first step and extracted a list containing the name of each eBay partner and the corresponding privacy policy URL in a .csv file. Some partners are listed in more than one purpose category of data processing. In the second step, we performed a data clean-up: we removed duplicates by reviewing the partner names and privacy policy URLs. Partners listed with several services and several corresponding policies were not removed as duplicates. After removing duplicates, a total of 906 unique partners resulted across all purpose categories. Once more, we extracted the list as a .csv file, which we fed into our Python crawler script. In step three, we parsed the .csv list in our Python script and utilised standard libraries to request the website containing the privacy policy for each contained URL. We used the Python library Beautiful Soup (Crummy, 2015) to parse the HTML content and remove unwanted elements such as styling information or scripts. To obtain an accurate word count, we fed the resulting raw text into the tokeniser package contained in the Python Natural Language Toolkit library (Natural Language Toolkit, 2019). We observed neglectable deviations between the precise, manually determined word count of a website and the word count determined by our script, as in some cases, words in a website's navigation bar or footer were included in the count. We subsequently stored the resulting word count for each URL in another .csv file for further analysis. Step four included the specification of different errors, and problems arose in the scraping and crawling process steps. These issues highlighted the need for a manual review of the user act of determining whether and to what extent to grant consent. By utilising a techno-legal analysis (Kurtz et al., 2019), we considered a user's perspective to identify the hurdles and problems. We divided these problems chronologically: before (P_{before}), during (P_{during}) and after (P_{after}) the act of consent. In step five, we grouped these problems into problem classes, which set the basis to determine the differences between an envisaged state and the current state of an artifact (Cronholm and Göbel, 2019). Based on this, we created design knowledge and derived a set of design goals (DGs) (Gregor and Jones, 2007); design goals represent the design theory's purpose and scope (Gregor and Jones, 2007). Generalised design goals enable the application regardless of a specific setup (Horlach et al., 2019). Our universally applicable design goals can serve as the basis for consent in digital service ecosystems.

12.4 Case Study

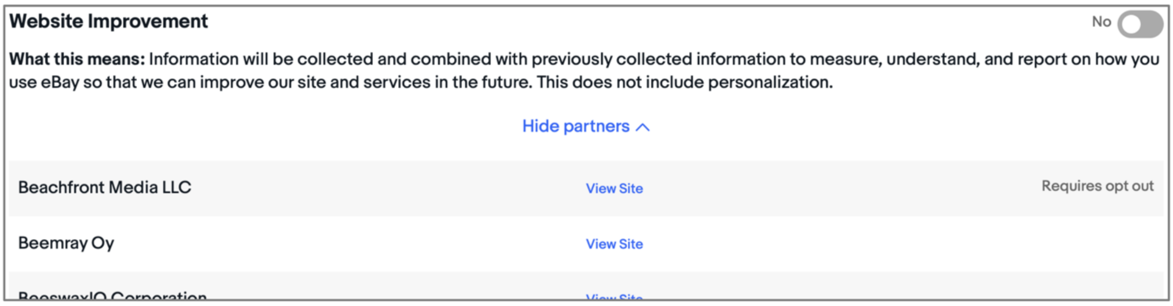
12.4.1 eBay and Included Partners

The platform eBay specifies the involvement of many partners for different purposes (eBay, 2019a). In the following, we detail eBay's specification. In addition, we illustrate the purpose categories and the number of included parties by eBay and related policies. The first time a user visits the eBay website or eBay application, the notice for the cookie and other technologies is displayed. In this notice, the aforementioned website is linked to the text 'Learn more, including how to manage your privacy settings'. Moreover, eBay's privacy policy specifies that this referenced website describes how eBay and related partners are processing users' personal data (eBay, 2019b). Users in the European Economic Area (EEA) have the choice to provide consent for related data processing.

Table 1. Count of partner entries per purpose category (August 2019)

Purpose category	Count of partner entries
'Content selection, delivery, and reporting'	315
'Website Improvement'	421
'Google Advertising'	645
'Storing and accessing information on your devices'	502
'Ad selection, delivery, and reporting'	460
'Personalizing advertising based on your behavior'	397
	2,740

In total, 2,740 partner entries are listed in the six purpose categories (Table 1) (research approach – step I). The name of each partner organisation and the URL to the related privacy policy are referenced in these categories. Users have the choice of deciding on partner's data processing and for each purpose category as a whole (Figure 2). On the website itself, the headline references 'Advertising and related preferences' for 'control the information eBay uses to show you ads'. This appears to conflict with two defined purpose categories. In particular, 'Content selection, delivery, and reporting' and 'Website Improvement' do not appear to fit the advertisement headline specified by eBay. The purpose categories described by eBay itself provide an indication that the majority of data in question is personally identifiable in nature. Apart from this, the fact that eBay itself lists these categories on a site about processing users' personal data clearly indicates that the data in question is personal data.



Website Improvement

No

What this means: Information will be collected and combined with previously collected information to measure, understand, and report on how you use eBay so that we can improve our site and services in the future. This does not include personalization.

Hide partners ^

Beachfront Media LLC	View Site	Requires opt out
Beemray Oy	View Site	
BeeswaxIO Corporation	View Site	

Figure 2. Extract of purpose category 'Website Improvement' (eBay, 2019a)

A data clean-up of the 2,740 listed partner entries resulted in 906 unique partners (Table 2) (research approach – step II). A single partner can be listed in multiple purpose categories, thus leading to the 2,740 entries. However, several listings of one partner do not link to several privacy policies – only to one policy. Typically, no data clean-up, such as the removal of duplicates, is performed by a user. Nevertheless, we performed a data clean-up to obtain further results.

Table 2. eBay partners' privacy policies in numbers

Partners	Count	Word count
Unique	906	-
Privacy policies not accessible	79	-
Privacy policies accessible	827	2,221,079
Privacy policies accessible, in English	735	1,984,823
Privacy policies accessible, in other languages (16 languages)	92	236,256

Only 827 privacy policies of 906 partners could be accessed (research approach – step III), as 79 policies were not accessible due to two reasons. First, 'ERROR: HTTP Error 404: Not Found' was displayed – the URLs to the partner policies specified by eBay did not exist. Second, security issues existed when opening the policies; in detail, the browser indicated an insecure, unencrypted connection or certificate errors when accessing websites. Of the 827 accessible privacy policies, 735 are written in English. The other policies are written in 16 other languages, namely Bulgarian, Chinese, Czech, Danish, Dutch, German, Finnish, French, Italian, Japanese, Polish, Portuguese, Russian, Slovak, Spanish and South Korean. On the related websites of these partners, no option existed to change the language.

12.4.2 Legal Classification

Pursuant to eBay's privacy policy, eBay bases its processing acts for the purpose of 'Personalization, measurement and improvement of [its] and third party advertisements in [its] online offerings, the online offerings of other eBay Inc. corporate family members or third parties' (eBay, 2019b, No. 5.5) on user consent as a legal basis for processing pursuant to the GDPR (GDPR, 2016, Art. 6 (1) (a)). Thus, eBay's aforementioned page (eBay, 2019a), offering further information on the various types of so-called 'eBay-Partners' that gain access to users' personal data under this purpose, is provided as a complementary document to the original privacy policy. This offers users more finely detailed information and allows them to change their consent preferences, either on a coarse level regarding different kinds of purposes or on a granulated level regarding every single partner. As the difficulties for determining and granting consent stem from the multitude of recipients to whom eBay transfers data, the focus shall be placed on the complimentary site that assesses the validity of consent granted by users.

When the personal data of eBay users is being transferred from eBay to a partner, two processing acts in need of a legal basis and other lawfulness requirements are actually occurring: the transfer itself, for which eBay evidently bases on user consent, and the saving and further processing of those data for which each individual recipient is a data controller with its own obligations, such as legal basis and user information. Thus, even if eBay were to act in a fully GDPR-compliant way regarding their transfer, unlawful processing acts might still occur within the digital service ecosystem, depending on each individual partner. Because of this, we shall evaluate the limits of user consent regarding both processing acts: Is the way eBay informs its users through its privacy policy sufficient to justify the initial processing and subsequent processing acts by partners? Only if this is the case, lawful types of processing acts are possible. This statement holds true for other, similar types of service ecosystems so long as they rely on consent as a legal basis and the service provider manages the way through which consent is being granted for the recipients in a service ecosystem.

The provided information by eBay must enable users to make an informed and free decision based on the specific purposes described to them. In addition, the mechanism through which consent is granted must be designed in such a way that the users can voice their wishes in an unambiguous manner (GDPR, 2016, Art. 4 No. 11). Differentiating here is important because the legal requirements for valid consent can differ based on the type of processing acts and data in question. For example, while it would suffice to inform about the 'recipients or categories of recipients of the personal data' (GDPR, 2016, Art. 13 (1) (e)) for consent encompassing only the processing and transfer of data by eBay itself, this would not suffice for consent that, as is the case here, aims to legitimise the subsequent processing acts by the recipients of the data, as well. Valid consent for these further processing acts would need to be granted based on the full range of information (GDPR, 2016, Art. 13). To consent to all such processing acts, users would need to know more information, such as the possible consequences. This would necessarily require access to the respective privacy policies of all the possible recipients at the times that consent is granted. However, consenting to so many (future) processing acts simultaneously also stretches the limits of the other aspects of valid consent, which is analysed in greater detail below.

12.4.3 Problems for Users in Deciding to Grant Consent

Hereafter, we specify the problems users have in determining whether and to what extent to grant consent in a digital service ecosystem (research approach – step IV). We have divided the categories into three chronological categories for a user: before, during and after the act. Eight problems exist *before the act* (Table 3). The first issue a user encounters is eBay's requirement for some partners 'to opt-out if [the user] do not wish [his/her] information to be shared […]. To opt-out, [the user has to] visit NAI, DAA or EDAA'. These acronyms belong to network advertising initiatives which bundle services – in this case, eBay partners. Partners included in these alliances receive personal data without consent by default (P_{before} 1). Second, neglecting the privacy settings banner linking to eBay's partner website in combination with any interaction, such as searching for an item or clicking on a bid, are followed by the automatised activation of every purpose category (P_{before} 2). Third, it is difficult to obtain an overview of which unique partners are involved by eBay (P_{before} 3). We scraped the partner entries and related privacy policy URLs and then removed the duplicates, resulting in 906 results of an initial 2,740. Such process steps cannot be expected from a user. However, if a user would complete these steps, the duration of reading the privacy policies could increase by up to a factor of three, as a user would not access all unique partners but all partner entries. Fourth and fifth, not all partner websites are accessible. In addition to websites not existing (P_{before} 4), security issues occur when attempting to open partner policies (P_{before} 5).

Table 3. Problems before the act of determining whether and to what extent to grant consent

No	Problem description
P_{before} 1	Personal data are shared to partners by default
P_{before} 2	Automised activation of every purpose category when a user neglects the privacy settings banner
P_{before} 3	Difficult to obtain an overview of unique partners (research approach – step II)
P_{before} 4	Partner privacy policies are not accessible (ERROR: HTTP Error 404: Not Found)
P_{before} 5	Security issues (partner sites comprise a non-secure connection)
P_{before} 6	Requirement to accept data collection and processing on partner websites
P_{before} 7	Navigation on partner website to partner's privacy policies is not possible
P_{before} 8	Different policies offered by a single partner

Sixth, before a user accesses partners' privacy policies, they must accept the different cookie and related personal data processing notices of partner websites (P_{before} 6). This issue leads to temporal expenditures. In addition, a partner can collect and process personal data based on the user visit and the user (necessary) acceptance of the cookie notice. These personal data can be processed by the partner independent of the processing formed by interactions with eBay. The consent is provided to the partner and related website itself, rather than eBay. This leads to the issue that, to gain more (necessary) information to understand the details of the consent that a user provides to eBay regarding data transfers to a partner, the user must consent to the processing of even more data on the partner's website simply to arrive at its privacy policy. Seventh, other partner sites, such as landing pages, are linked by eBay. Navigating to the privacy policy of the partners was not always possible (P_{before} 7). For cases in which the website has been displayed in a language not accessible to the user, the policy cannot be accessed. Moreover, some partners did not declare a privacy policy at all on their website. Eight, partners declared on the website a selection of policies to access (such as website and service privacy policies). The partner offered no clear indication of which policy is relevant to the user (P_{before} 8). For further analysis, we assume that the service privacy policy is relevant.

Five problems exist *during the act* of determining whether and to what extent to grant consent (Table 4). These problems occur when opening eBay's linked partner sites. First, rather than privacy policies, several other documents are linked (P_{during} 1). Cookie descriptions, data request sheets and opt-out descriptions represent a diverse collection of documents. Second, partners' privacy policies are not accessible for linguistic reasons. The policies are stated in 17 languages, and if written in a language other than English, they do not offer translated versions (P_{during} 2). Not every eBay user has the ability to understand policies not written in his or her native language. In addition, if capabilities in English exist, this competence might not cover complex sentences using legal terminology. Varying difficulty levels of readability are represented in the policies with, for example, in-depth technical descriptions or legal jargon (P_{during} 3). Fourth, diverse policy specification can be observed (P_{during} 4). The policies vary in word count, from 165 words up to 13,497 words. Fifth, the time required to read all partners' policies is extremely long (P_{during} 5) (cf. Section 4.4).

Table 4. Problems during the act of determining whether and to what extent to grant consent

No	Problem description
P_{during} 1	Variety of linked documents (cookie descriptions, privacy policies and data request sheets)
P_{during} 2	Privacy policies are written in 17 languages (735 in English and 92 in 16 other languages)
P_{during} 3	Varying difficulty levels (legal and technical jargon)
P_{during} 4	Varying levels of detail (165 words up to 13,497 words)
P_{during} 5	Massive amount of time required to read partner policies (cf. Section 4.4)

A user encounters five problems *after the act* of determining whether and to what extent to grant consent (Table 5). First, partners reference the involvement of third parties in their privacy policies (P_{after} 1). Thus, for the act, a user would also need to read the privacy policies of third parties involved by eBay's partners. Second, in its purpose category summary, eBay describes the purposes and related technologies used by partners; however, these descriptions do not match with the specifications made in the partners' policies (P_{after} 2). Declarations made by partners exceed those made on eBay's site. Third, no mechanism exists which notifies users of changes in the digital service ecosystem (P_{after} 3). This lack of notification mechanism pertains to changes of eBay's involved partners and in partners' privacy policies. Fourth, no indication is provided as to whether a partner is relevant for the user's transaction (P_{after} 4). Since these are international partners, such as Chinese or South Korean partners, the relevance for a user transaction from Europe is at least questionable. Unfortunately, an examination of the website for further information and a request to eBay did not yield any results. Fifth, partners are listed in multiple purpose categories. A user has the option to decide according to the purpose of the partner's data processing. However, only one privacy policy is linked to the partner independent from the purpose category (P_{after} 5). The question arises regarding the extent to what a user provides consent – the purpose listed on eBay's website or to all specifications made in the privacy policy by the partner.

Table 5. Problems after the act of determining whether and to what extent to grant consent

No	Problem description
P_{after} 1	Integration of third parties by eBay partners
P_{after} 2	Different statements regarding used technologies or purposes
P_{after} 3	No mechanism notifies about changes regarding partner changes or partners' policy changes
P_{after} 4	Relevance of partner for user transactions
P_{after} 5	Choices for a partner's data processing to multiple purpose categories but to only one partner policy

12.4.4 Average Reading Time for Users of Partners' Privacy Policies

In the following, we calculate the average reading time of the partners' privacy policies to serve as an example for the duration of providing consent in a digital service ecosystem (McDonald and Cranor, 2008). The privacy policies are written in 17 different languages; however, we utilise only the 735 privacy policies written in English. The 92 privacy policies not written in English (10.2% of partners) and 79 privacy policies not accessible (8.7% of partners) are not considered in the calculation. This restriction is driven by the assumption of Europeans being unable to understand languages such as Chinese or Japanese. The calculation represents an indicator but not the time for all partners. We use a scale of 250 words per minute as the basis for average reading time (McDonald and Cranor, 2008). The time depends on various factors, such as education level, difficulty level or language of a text. Moreover, different opinions exist, ranging between 200 and 300 words per minute (McDonald and Cranor, 2008, Carver, 1990). As a second variable, 1,984,823 words contained in 735 privacy policies is considered.

As result, a duration of 7,940 minutes is required to read the privacy policies in English for eBay's digital service ecosystem (Table 6). This time is equivalent to 132.3 hours, 16.5 working days (assuming 8 hours per day) and 5.5 days (assuming 24 hours a day). In addition, 171 partner policies are not considered in this result. Given the massive time amount of 5.5 days, this conflicts with eBay's listing duration options for articles of one, three or five days. In addition, our calculation relates to only the actual reading time, which might not necessarily correspond with the time required for the average user to fully understand the content and implications of the policies. The reading times for partners' policies range between 1 and 54 minutes, and the privacy policy with the longest reading time belongs to eBay itself. The platform is surprisingly mentioned in the purpose category of 'Google Advertising'.

Table 6. Reading time for eBay partner privacy policies in English (rounded up)

Policies in English	Word count	Reading rate per minute	Minutes	Hours	Working days	Days
735	1,984,823	250	7,940	132.3	16.5	5.5

12.5 Design Goals for Consent in Digital Service Ecosystems

Given that digital service has shifted from a single-actor encounter to a plethora of actors, this raises various problems identified in the case study. In the following, we use the identified problems to derive design goals (research approach – step V) as basis for enabling the act of consent to data processing in digital service ecosystems. In detail, we summarise the problems into multiple problem classes, which served as the basis for specifying the design goals (Table 7). Our design goals are generalised and independent from a specific ecosystem setup; therefore, the design goals for enabling consent can be applied in various digital ecosystems, and involved actors and actions can manifest in various ways (e.g. consent for mobile application service ecosystems or website ecosystems).

The first problem describes the circumstances that partners involved in network alliances encounter via default personal data – without consent (P_{before} 1). In addition, when a user neglects the settings banner, personal data may be shared and processed with not only those partners involved in the alliances but with all partners involved in the digital service ecosystem (P_{before} 2). This occurs without the act of providing consent. When accessing eBay partners' privacy policies, numerous personal data are already transmitted and processed on the partners' websites – request to confirm personal data processing to access the privacy policies (P_{before} 6). However, the concept of a policy is the specification of personal data usage and purposes prior to processing. Therefore, the problem class summarises the aspect that personal data is processed before the act of providing consent. Based on this issue, the first design goal is specified as **no personal data processing before providing consent (DG1)**.

In the case study, 79 partner privacy policies could not be accessed (P_{before}4). In this context, also security issues arise in attempting to open privacy policies (P_{before} 5). The navigation to policies was sometimes impossible, due to policies not existing or for linguistic reasons (P_{before} 7). Another problem of accessibility is the determination of the relevant policies across the several offered by one partner (P_{before} 8). Moreover, not all privacy policies are written in English; thus, the 16 other languages serve as a potential problem for the user being unable to access the policy content (P_{during} 2). Due to the increasing involvement of actors across national borders, this aspect will be present in other digital service ecosystems. In addition, the partners also involve multiple third parties (P_{after} 1); however, these parties are not mentioned in eBay's policy and appear in eBay partners' policies, creating the problem of initial access. These problems can be summarised in the problem class of inaccessibility regarding information pertaining to data processing and purposes. This problem class can be addressed by the design goal which addresses the **accessibility of information concerning data processing and purposes** (**DG2**).

Various document types such as privacy policy, support policy, cookie policy or security policy are offered by eBay's partners (P_{during} 1). The policies differ in terms of difficulty level, such as being highly legal or containing technical terminology (P_{during} 3). In addition, the information in linked documents is presented in varying detail levels (P_{during} 4). These issues result in the problems class in which the information and its representation vary massively. No uniform act of consent is possible whereby the user is confronted with new circumstances across policies. The third design goal seeks the **uniformity of information concerning data processing and purposes** (**DG3**).

Partner statements in privacy policies exceed the information of personal data, used technologies and purposes described in eBay's privacy policy and purpose summary (P_{after} 2). Neither the statements of eBay lack in completeness nor are the partners' policies too extensive in describing the data processing and purposes. In addition, the various categories allow a user to decide about the data processing of one partner. Since a partner appears in multiple categories, different choices can be made (P_{after} 5); however, dissociated of the choice, the same partner policy is placed for all purposes. It is not comprehensible how partners operate in the case of deselecting one purpose yet still gain access to personal data via another category. It remains hidden to the user as to whether the purpose leads to distinct processes and data processing at eBay partners. Thereupon, the fourth design goal addresses the non-corresponding statements and seeks **consistency in information concerning data processing and purposes (DG4)**.

The partners involved by eBay include users' personal data in their services and parties processing (P_{after} 1). In this context, no mechanism exists which notifies about changes in a dynamic digital ecosystem

(P_{after} 3). The involvement of multiple actors and related dynamics are summarised in the problem class of dynamic service ecosystems. The partners therein, the applied personal data and purposes for processing these data change over time. Thus, the fifth design goal addresses the need for **notifications about changed information of data processing, purposes or involved actors (DG5)**, as consent must be renewed. When consent is provided in a digital service ecosystem regarding processing acts performed by multiple actors, the correctness and accuracy of the information regarding such processing acts must be assured. If this is not possible, modifications in digital service ecosystems are difficult, as the user has provided consent to only the initial state of the ecosystem at the time of his or her granting consent.

The case includes the noteworthy aspect that no information is given if all 906 partners are involved in each user transaction (P_{after} 4). The platform eBay potentially requires all mentioned partners to monetise, improve or monitor their platform. Another interpretation is that eBay refers to only partners that sellers use without utilising them on their own. One could argue that eBay's management of partners is professional and detailed compared with other service providers, as it offers an overview to a large set of actors grouped in categories. However, 79 privacy policies of partners cannot be accessed at all. Users must assume that all listed partners can gain access to their personal data. As every partner specifies its used data and related purposes for data processing – and in this case, 906 partners are involved – consent is provided for an in-total extensive data processing. In addition, personal data may be shared to actors (P_{before} 1) which are not necessarily relevant for a user at all. We grouped these problems in the problem class of extensive consent; therefore, we develop the sixth design goal, which addresses **transaction-specific consent to data processing (DG6)**.

Of the 2,740 specified partner entries, 906 unique partners are involved in six purpose categories, which creates the problem of acquiring an overview of unique partners (P_{before} 3). In addition, eBay's partners involve other third parties and these parties in turn, which results in a large-scale digital service ecosystem (P_{after} 1). Privacy policies consequently tend to be recursive in digital service ecosystems. The user is exposed to a massive amount of reading time (P_{during} 5), which was calculated for only a fraction of the total digital ecosystem. A median shopping duration of five minutes (Salesforce Commerce Cloud, 2019) has no relation to at least 7,940 minutes of reading time for 'only' partners' privacy policies. The time amount of 5.5 days conflicts with eBay's listing duration options of one, three or five days. A bidding would not be possible if partners' policies were read. The sixth design goal seeks **reasonability of the time required to provide consent in relation to usage time of the service (DG7)**.

Table 7. Design goals for consent in digital service ecosystems

No	Problem	Problem Class	Design Goal
P_{before} 1	Personal data are shared with partners by default	Personal data is collected and processed before the user provides consent	DG1: No personal data processing before providing consent
P_{before} 2	Automised activation of every purpose category when a user neglects the privacy settings banner		
P_{before} 6	Requirement to accept data collection and processing on partner websites		
P_{before} 4	Partner privacy policy is not accessible	Inaccessibility of information concerning data processing and purposes	DG2: Accessibility of information concerning data processing and purposes
P_{before} 5	Security issues		
P_{before} 7	Navigation on partner website to partner's privacy policies is not possible		
P_{before} 8	Different policies offered by a single partner		
P_{during} 2	Privacy policies are written in 17 languages		
P_{after} 1	Integration of third parties by eBay partners		
P_{during} 1	Variety of linked documents	Variety of information concerning data processing and purposes in form, terminology and representation	DG3: Uniformity of information concerning data processing and purposes
P_{during} 3	Varying difficulty levels		
P_{during} 4	Varying levels of detail		
P_{after} 2	Different statements regarding used technologies or purposes	Non-corresponding statements concerning personal data processing and purposes in statements of service providers and involved partners	DG4: Consistency in information concerning data processing and purposes
P_{after} 5	Choices for a partner's data processing to multiple purpose categories, but to only one partner policy		
P_{after} 1	Integration of third parties by eBay partners	Dynamic ecosystems include changing and emergent actor involvements, related personal data processing and purposes	DG5: Notifications about changed information of data processing, purposes or involved actors
P_{after} 3	No mechanism notifies about changes regarding partner changes or partners' policy changes		
P_{before} 1	Personal data are shared with partners by default	Consent to an extensive number of actors processing personal data	DG6: Transaction-specific consent to data processing
P_{after} 4	Relevance of partner for user transactions		
P_{before} 3	Difficult to obtain an overview of unique partners	Massive amount of time required for the process of providing consent to use a single digital service	DG7: Reasonability of the time required to provide consent in relation to the usage time of the service
P_{during} 5	Massive amount of time required to read partner policies		
P_{after} 1	Integration of third parties by eBay partners		

12.6 Discussion

Our design goals can be applied to enable consent in other contemporary and rising digital service ecosystems. Plausible reasons exist for involving partners in digital service ecosystems(i.e. users expect at least solid performance of digital services, and thus, application performance management is a typical area in which third parties apply). Additionally, personalisation is a common driver for the inclusion of third parties. Nevertheless, the case of eBay demonstrates how large a digital service ecosystem can become and that the existing act of acquiring the user's consent becomes questionable. Even more, digital service ecosystems bear the challenge that privacy policies must consider third parties which include other parties, as well. Recursive digital service ecosystems cannot be covered by the existing form of policies. With numerous partners involved, obtaining access to diverse personal data, increasing points for potential data breaches and negative practices occur. Subsequently, the implications of service usage and associated data provision become incalculable for users. In practice, another method is for digital service providers to mention an involvement of different actor groups for specific purposes. This approach does not specify the involved actors, as categories of recipients may be sufficient (GDPR, 2016, Art. 13 (1) (e)). However, this approach cannot address the problem that oftentimes, these actors process personal data for purposes that are not covered by the digital service provider's policy and the purposes specified therein. This might explain why eBay and other websites link third-party policies.

In the following, we compare the determined design goals and the requirements for effective consent, according to the GDPR (GDPR, 2016, Art. 4 (11)). The aspect of freely given and unambiguous consent is covered by the first design goal pre-privacy protection (DG1). The design goals accessibility (DG2), uniformity (DG3), consistency (DG4) and notifications about changed information (DG5) can be mapped to the characteristic of informed consent. In addition, the design goal transaction-specific consent (DG6) addresses the characteristic of specific consent. However, the design goal reasonability (DG7) does not exactly match one of the requirements of consent as specified by the GDPR. While realising the identified design goals can mean fulfilling the GDPR's requirements for consent, neither the design goals nor the GDPR requirements has a fixed scale with a concrete endpoint. Realising the design goals in a more efficient and better manner could also raise the bar for what is expected by the GDPR. We wish to identify a new aspect of consideration that might be missing from the legal interpretation of what makes consent valid; as our case study demonstrates, the (dis)proportion between the time spent using a service and the time needed to read (let alone understand) its privacy policies are key elements for consent in digital service ecosystems and the plurality of involved actors and therefore privacy policies. Subsequently, two approaches appear suitable for overcoming the issue of reasonability. On one hand, law can attempt to restrict and limit digital service ecosystems and the involvement of numerous service partners. This approach may be successful in limiting personal data sharing in ecosystems. However, specifying the limits of ecosystems and involvement would be challenging and would need to be balanced with the legitimate interests and fundamental rights of the service provider and third parties. On the other hand, the uniformity and machine-readable data processing information would allow for a new form of consent, considering mandatory conditions. Employing a method of automatisation appears plausible in achieving the design goals. The Platform for Privacy Preferences Project (P3P) is no longer supported yet possibly relevant (Cranor and Wenning, 2019). The idea behind this technical platform was the exchange of data processing information as a standard, and it was recommended by the WWW Consortium (W3C) (Cranor and Wenning, 2019). The reactivation of this project would allow for standardising personal data processing information and would have the potential to establish a standard.

With our article, we call for research on the challenging issue of enabling consent to personal data processing in digital service ecosystems. Empirical studies already present manifold problems of single privacy policies (Acquisti and Gross, 2006, Sunyaev et al., 2014, Ermakova et al., 2016). However, as the analysis within this paper reveals, reading, understanding and consenting to a single privacy policy in a meaningful manner is not common practice in digital service ecosystems. The GDPR declares that consent is valid when it is freely given and unambiguously voiced for a specific purpose or specific set of purposes and based on an informed decision. In the absence of precedent court rulings, no definite lines of interpretation for these requirements exist. Practices consequently arise which may understate specifications made in the GDPR. Still, the existing understanding by both legal scholars and the few court decisions that exist are sufficient for casting serious doubts about the validity of consent provided in scenarios such as the one assessed in this paper. Given that privacy policies are a legal instrument necessary for ensuring consent to data processing in the lied-out manner, it is highly important that these policies are usable from a user's perspective. A broader dialogue with legal scholars in consideration of the existing laws is necessary for redesigning consent. In addition, the perspective of IS scholars can be highly beneficial in filling the GDPR's abstract provisions with life and developing their scope.

This study introduces interdisciplinary avenues for further research. In particular, this study reveals that enabling consent can be acquired only through a dialogue between stakeholders from both professions: the legal and information systems disciplines. In doing so, further research can contribute to this area by addressing the limitations of this study. Furthermore, how dynamic privacy policies in service ecosystems are is mirrored in a recent change made by eBay: The names of purpose categories changed. In addition, the platform began to include additional detail regarding what information is shared with third parties. However, this information is not yet available for all partners. Thus, we decided to not include this additional material, as the design goals are not affected by this change. An analysis of these changes can be beneficial for further results. By utilising other digital service ecosystems, the design goals can be expanded and refined for specific solutions towards design principles. However, this was not the aim of this manuscript and would have gone beyond the scope of this study.

12.7 Conclusion

This manuscript's primary contribution is seven design goals that guide organisations and researchers in addressing consent in digital service ecosystems. We demonstrated a new dimension of effort for the act in this context. With the benchmark of 906 involved partners and 132.3 hours needed for reading the policies, our selected case achieves a magnitude for which nobody can claim a well-balanced ratio of time to become informed before providing consent. The existing form leads to incomprehensibility of personal data processing. Users consequently possess consent fatigue (Schraefel et al., 2017) and may not be equipped to act in their own self-interests. It would be wrong to cling to forms which even today do not fulfil their function in ensuring effective consent and cannot keep up with service ecosystems.

Promising approaches through creating summaries based on artificial intelligence are already in use (Harkous et al., 2018) and could be combined with our design goals to address characteristics of emerging digital service ecosystems. As demonstrated in the comparison with the GDPR, the determined design goals can support service providers positioned in ecosystems to implement the legal requirements. Additionally, the balancing act of implementation and in turn the generative improvement of all design goals has the potential to shape the GDPR requirements in a way that raises the bar and gradually closes the gap between what the GDPR deems adequate regarding, for example, when a user is sufficiently informed about processing circumstances and the user's de facto understanding. As the scope of (most) GDPR provisions is dynamic rather than static, it evolves alongside the 'state of the art' (GDPR, 2016, Art. 24 (1), 25 (1)). The increasing complexity of connected actors involved in service provision lead to insufficient operability of consent and therefore necessitate a redesign. We pave the way for research and practice for consent in consideration of emerging digital service ecosystems.

12.8 Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality in the project Information Governance Technologies under the reference LFF-FV 34.

12.9 References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). 'Privacy and human behavior in the age of information', *Science,* 347(6221), 509-514.

Acquisti, A. and Gross, R. (2006). 'Imagined communities: Awareness, information sharing, and privacy on the Facebook', *International workshop on privacy enhancing technologies*, 36-58.

Bahr, K. D. (2019). 'KG Berlin: Umfangreiche DSGVO-Verstöße bei Google-Datenschutzerklärung'. https://www.dr-bahr.com/news/umfangreiche-dsgvo-verstoesse-bei-google-datenschutzerklaerung.html (visited on01.08. 2019).

Barrett, M., Davidson, E., Prabhu, J. and Vargo, S. L. (2015). 'Service innovation in the digital age: key contributions and future directions', *MIS Quarterly,* 39(1), 135-154.

Baskerville, R. and Pries-Heje, J. (2010). 'Explanatory design theory', *Business & Information Systems Engineering,* 2(5), 271-282.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987). 'The Case Research Strategy in Studies of Information Systems', *MIS Quarterly,* 11(3), 369-386.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N. (2018). 'Third Party Tracking in the Mobile Ecosystem', *Proceedings of the 10th ACM Conference on Web Science.*

Bitner, M. J., Ostrom, A. L. and Morgan, F. N. (2008). 'Service blueprinting: A practical technique for service innovation', *California Management Review,* 50(3), 66.

Carver, R. P. (1990) Reading rate: A review of research and theory, Academic Press.

Chandler, J. D. and Lusch, R. F. (2015). 'Service Systems: A Broadened Framework and Research Agenda on Value Propositions, Engagement, and Service Experience', *Journal of Service Research.*

chrome web store (2019). 'Scraper'. https://chrome.google.com/webstore/detail/scraper/mbigbapnjcgaffohmbkdlecaccepngjd (visited on20.07. 2019).

Cranor, L. and Wenning, R. (2019). 'Platform for Privacy Preferences (P3P) Project'. https://www.w3.org/P3P/ (visited on 12.11. 2020).

Cronholm, S. and Göbel, H. (2019). 'Design Science Research Constructs: a Conceptual Model', in *Pacific Asia Conference on Information Systems 2019*,

Crummy (2015). 'Beautiful Soup Documentation'. https://www.crummy.com/software/BeautifulSoup/bs4/doc/ (visited on28.07. 2019).

de Reuver, M., Sørensen, C. and Basole, R. C. (2018). 'The digital platform: a research agenda', *Journal of Information Technology,* 33(2), 124-135.

Di Luzio, A., Mei, A. and Stefa, J. (2016). 'Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests', in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, IEEE, 1-9.

eBay (2019a). 'Advertising and related preferences'. www.ebay.com/gdpr (visited on09.08. 2019).

eBay (2019b). 'User Privacy Notice'. https://www.ebay.com/help/policies/member-behaviour-policies/user-privacy-notice-privacy-policy?id=4260 (visited on27.07. 2019).

Ermakova, T., Fabian, B. and Babina, E. (2015). 'Readability of Privacy Policies of Healthcare Websites', *Wirtschaftsinformatik*, 1085-1099.

Ermakova, T., Krasnova, H. and Fabian, B. (2016). 'Exploring the impact of readability of privacy policies on users' trust', *European Conference on Information Systems (ECIS).*

EuropeanCommission (2014). 'Article 29 Data Protection Working Party - Opinion 05/2014 on Anonymisation Techniques'.

Fischer, C., Winter, R. and Wortmann, F. (2010). 'Design theory', *Business & Information Systems Engineering,* 2(6), 387-390.

GDPR (2016). 'General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Directive 95/46)', 59, 1-88.

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E. and Zhdanov, D. (2018). 'How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas', *MIS Quarterly,* 42(1), 143-164.

Gregor, S. and Jones, D. (2007). 'The anatomy of a design theory', *Journal of the Association for Information Systems,* 8(5), 312.

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G. and Aberer, K. (2018). 'Polisis: Automated analysis and presentation of privacy policies using deep learning', *27th Security 18*, 531-548.

Hein, A., Scheiber, M., Böhm, M., Weking, J. and Krcmar, H. (2018). 'Towards a Design Framework for Service Platform Ecosystems', in *The European Conference on Information Systems.*

Horlach, B., Schirmer, I. and Drews, P. (2019). 'Agile Portfolio Management: Design Goals and Principles', *Proceedings of the European Conference on Information Systems, Stockholm-Uppsala, Sweden (ECIS 2019).*

Ji, S., Mittal, P. and Beyah, R. (2016). 'Graph data anonymization, de-anonymization attacks, and de-anonymizability quantification: A survey', *IEEE Communications Surveys & Tutorials,* 19(2).

Kuechler, B. and Vaishnavi, V. (2008). 'On theory development in design science research: anatomy of a research project', *European Journal of Information Systems,* 17(5), 489-504.

Kurtz, C., Semmann, M. and Böhmann, T. (2018a) 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors', in *Americas Conference on Information Systems*, New Orleans,

Kurtz, C., Semmann, M. and Schulz, W. (2018b) 'Towards a Framework for Information Privacy in Complex Service Ecosystems', *International Conference on Information Systems*, San Fransisco,

Kurtz, C., Wittner, F., Semmann, M., Schulz, W. and Böhmann, T. (2019) 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems', in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Hawaii,

Legner, C. and Löhe, J. (2012). 'Improving the realization of IT demands: A design theory for end-to-end demand management'.

Libert, T. (2018). 'An automated approach to auditing disclosure of third-party data collection in website privacy policies', in *Proceedings of the 2018 World Wide Web Conference*, International World Wide Web Conferences Steering Committee, 207-216.

Litman-Navarro, K. (2019). 'We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.‘. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (visited on30.07. 2019).

Lusch, R. F. and Vargo, S. L. (2014) *Service-dominant logic: Premises, perspectives, possibilities,* Cambridge University Press.

Malaga, R. A. (2014). 'Do web privacy policies still matter?', *Journal of Management Information Systems,* 17(1), 95.

Malandrino, D. and Scarano, V. (2013). 'Privacy leakage on the Web: Diffusion and countermeasures', *Computer Networks,* 57(14), 2833-2855.

McDonald, A. M. and Cranor, L. F. (2008). 'The cost of reading privacy policies', *I/S: A Journal of Law and Policy for the Information Society,* 4, 543.

Narayanan, A. and Shmatikov, V. (2008). 'Robust de-anonymization of large sparse datasets', in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, IEEE, 111-125.

Natural Language Toolkit (2019). 'NLTK 3.4.5‘. https://www.nltk.org/# (visited on28.07. 2019).

Paspatis, I., Paspatis, I., Tsohou, A., Tsohou, A., Kokolakis, S. and Kokolakis, S. (2017). 'Mobile application privacy risks: Viber users' de-anonymization using public data', in *Mediterranean Conference on Information Systems (MCIS)*, Association For Information Systems,

Rainie, L. and Duggan, M. (2016). 'Privacy and information sharing', *Pew Research Center,* 16.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C. and Gill, P. (2018). 'Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem', *Network and Distributed Systems Security (NDSS) Symposium 2018*.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Liu, F., McDonald, A., Norton, T. B. and Ramanath, R. J. B. T. L. (2015). 'Disagreeable privacy policies: Mismatches between meaning and users' understanding', *Berkeley Tech. LJ,* 30, 39.

Riedl, C., Boehmann, T., Leimeister, J. M. and Krcmar, H. (2009). 'A framework for analysing service ecosystem capabilities to innovate', *17th European Conference on Information Systems*.

Rohleder, B. (2015). 'Datenschutz in der digitalen Welt', *bitkom*.

Schraefel, M., Gomer, R., Alan, A., Gerding, E. and Maple, C. (2017). 'The internet of things: interaction challenges to meaningful consent at scale', *interactions,* 24(6), 26-33.

Sunyaev, A., Dehling, T., Taylor, P. L. and Mandl, K. D. (2014). 'Availability and quality of mobile health app privacy policies', *Journal of the American Medical Informatics Association,* 22(e1).

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S. and Serna, J. (2018). 'I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR', in *Companion Proceedings of the The Web Conference 2018*, International World Wide Web Conferences Steering Committee, 163-166.

Van Alstyne, M. W., Parker, G. G. and Choudary, S. P. (2016). 'Pipelines, platforms, and the new rules of strategy', *Harvard Business Review,* 94(4), 54-62.

Vargo, S. L. and Akaka, M. A. (2012). 'Value cocreation and service systems (re) formation: A service ecosystems view', *Service Science,* 4(3), 207-217.

Vargo, S. L., Maglio, P. P. and Akaka, M. A. (2008). 'On value and value co-creation: A service systems and service logic perspective', *European management journal,* 26(3), 145-152.

Walls, J. G., Widmeyer, G. R. and El Sawy, O. A. (1992). 'Building an information system design theory for vigilant EIS', *Information Systems Research,* 3(1), 36-59.

Wilson, S., Schaub, F., Dara, A. A., Liu, F., Cherivirala, S., Leon, P. G., Andersen, M. S., Zimmeck, S., Sathyendra, K. M. and Russell, N. C. (2016). 'The creation and analysis of a website privacy policy corpus', *Meeting of the Association for Computational Linguistics*, 1330-1340.

Yin, R. K. (2009) Case Study Research: Design and Methods SAGE.

Yu, L., Luo, X., Liu, X. and Zhang, T. (2016). 'Can we trust the privacy policies of android apps?', *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 538-549.

Zimmeck, S., Story, P., Smullen, D., Ravichander, A., Wang, Z., Reidenberg, J., Russell, N. C. and Sadeh, N. (2019). 'MAPS: Scaling privacy compliance analysis to a million apps', *Proceedings on Privacy Enhancing Technologies,* 2019(3), 66-86.

13 Article No. 5 (Vogel et al. 2020)

Vogel, P., Grotherr, C., Kurtz, C., & Böhmann, T. Conceptualizing Design Parameters of Online Neighborhood Social Networks. In Proceedings of the 15th International Conference on Wirtschaftsinformatik, Potsdam (Germany), 2020.

Abstract

Online neighborhood social networks (ONSNs) represent an emerging phenomenon among a growing number of niche social networks. These platforms afford users the ability to engage in activities such social interaction with neighbors, sharing of information on local issues or neighborhood volunteering and exhibit promising effects, including improved relationships between neighbors and an increase in neighborly communication. Despite the mounting popularity of platforms such as Nextdoor or nebenan, extant research on ONSNs remains scarce. In this paper, we aim to alleviate this research gap by developing a conceptually and empirically validated taxonomy of ONSNs with a particular focus on their differentiating design properties. We further leverage this taxonomy to derive four distinct archetypes of ONSNs based on a cluster analysis. With our research we provide a first and structured overview on the domain of ONSNs and support researchers and practitioners in analyzing, designing and selecting ONSNs.

13.1 Introduction

Social network sites (SNS) are ubiquitous in our everyday use of information technology. More than forty percent of the world's population and more than seventy percent of all internet users are active on social media [1]. Besides the continuous growth of behemoths such as Facebook [2], there is an increasing number of niche social networks which enjoy rising popularity. These SNS cater to specific audiences, ranging from academics (ResearchGate, Academia) to designers (Behance, Dribble) or athletes (Runtastic, Strava), among others, and offer thematic features, focus as well as a community of likeminded individuals. Specialized sub-communities can also be observed on traditional SNS, for example in the form of Facebook groups, evoked by segmentive and negative network effects [3]. Online neighborhood social networks (ONSNs) represent a type of social network which affords users the ability to engage in activities such social interaction with neighbors, sharing of information on local issues and neighborhood volunteering [4]. Among niche social networks, they are unique not only in their topical focus on neighborhood-related issues but also because they consist of several sub-communities, each representing the inhabitants of a delimited geographic area. Previous research has demonstrated promising effects of ONSNs such as improved relationships between neighbors or an increase in neighborly communication and activities [5]. With 236,000 registered neighborhoods [6], San Francisco-based Nextdoor is the largest among these platforms. In Europe, Berlin-based nebenan has recently surpassed the one million user mark [7]. Despite this increasing popularity, extant research on ONSNs remains scarce. While some studies investigate ONSNs and related issues [4, 8, 9], academic literature lacks a comprehensive framework for their classification. We aim to contribute to closing this research gap by providing a systematic overview of the domain of ONSNs. As we observe a lack of design knowledge on ONSNs, we focus on principal differences in their design, i.e. their differentiating design properties. We formulate the following research question:

RQ: What are the conceptually and empirically validated design parameters of neighborhood social networks?

To answer this research question, we develop a taxonomy of ONSNs based on the methodology for taxonomy development presented by Nickerson et al [10]. Taxonomies are particularly useful to shed light on emerging phenomena [11] such as ONSNs. In line with previous taxonomy research in information systems (IS) [12, 13], we further leverage our developed taxonomy to derive a set of archetypes which represent repeating patterns of platforms among ONSNs. In the course of our research, we develop a first and comprehensive taxonomy of ONSNs, identify four distinct clusters of platforms and derive implications regarding the design of ONSNs. The contribution of our research is twofold. We support researchers and practitioners in the fields of social media, community and neighborhood research as well as smart cities and communities in analyzing, designing and selecting ONSNs. Our research sheds light on the quickly evolving topic of niche social networks and OSNS which have received little attention in previous research on social media. In the following Section 2, we present related work on ONSNs as well as taxonomy research in IS. Section 3 details our methodology, including taxonomy development and cluster analysis. In Section 4, we present our taxonomy and describe its dimensions and characteristics. We define archetypes of ONSNs in Section 5. Finally, we discuss theoretical and practical implications of our research in Section 6 and conclude with a summary and limitations of our work in Section 7.

13.2 Related Work

13.2.1 Online Neighborhood Social Networks

Connecting neighborhoods via the internet has a long tradition in the form of community informatics, 'the application of information and communications technology (ICT) to empower community processes' [14, p. 11]. Projects such as the Blacksburg Electronic Village provided neighbors with functionality for chat, email lists, discussion boards and local business listings as early as 1993 [15]. These artifacts were able to overcome spatial, temporal and social barriers to communication and enabled civic engagement among neighbors. Today's SNS harbor significant potential for increasing neighborliness through localized usage [16]. On SNSs such as Facebook, cumulative and segmentive network effects have resulted in the organic formation of city and neighborhood-level communities in the form of groups [3]. These groups can serve as grounds for discussion of local issues while restricted access groups enable neighbors to establish communities of trust among themselves [17].

ONSNs aim to provide a dedicated space for these neighborhood-centric communities. As to avoid confusion between ONSNs and the existing term of neighborhood social networks used in the social sciences, we choose *online neighborhood social networks* as a suitable term to describe the focal phenomenon. ONSNs can be classified as a private and local type of SNS [18]. They are private in that they restrict access to a specific group of individuals – neighbors – and are not open to the general public. They are local as they relate to a spatially delimited area or place, the neighborhood. The term *neighborhood* can be defined from various perspectives based on criteria such as administrative boundaries, an area's history or characteristics and perceptions of its inhabitants [19, 20]. We define an ONSN as a social network site whose intended audience comprises the inhabitants of one or more neighborhoods and whose thematic focus lies on neighborhood-related issues. Most ONSNs seem to share a common set of features and traits. They are free-to-use but often require users to verify their address to confirm their neighbor status. Each neighborhood represents a separate sub-community, limiting user-generated content to an audience of neighbors. Users possess a profile page and can access a directory of neighbors, exchange information on local issues, request and provide recommendations regarding local service providers as well as offer goods and services on a marketplace. However, literature on ONSNs remains scarce. Vogel et al. [4] propose an age-friendly digital neighborhood platform which aims at increasing social connectedness of the elderly. Masden et al. [8] analyze the ONSN Nextdoor and attest potential for fostering community connectedness. Further studies on ONSNs propose an app-based platform for fostering co-production in the neighborhood and a cross-generational neighborhood network [9, 21].

13.2.2 Taxonomy Research in Information Systems

Taxonomies, defined as 'conceptually or empirically derived groupings of dimensions and characteristics' [11, p. 13], enable researchers and practitioners to structure and analyze complex domains and the ordering of disorderly concepts [10]. While the IS discipline lacked thematic methodological guidance for taxonomy development for a long time, Nickerson et al. [10] presented a method for taxonomy development for IS research. They base their methodology on existing approaches from information systems, computer science and business research. Widespread use of this method can be observed, including cases in the context of social media research. Notable examples include taxonomies of organizational social media use [22],and social reading platforms [12]. Nickerson et al. [10] define a taxonomy as a set of dimensions each consisting of a set of mutually exclusive and collectively exhaustive characteristics that sufficiently describes objects in a specific domain of interest. Characteristics are considered mutually exclusive and collectively exhaustive if each object has one and only one characteristic in each dimension. Development kicks off by determining a meta-characteristic as a foundation for all other characteristics in the taxonomy. Next, ending conditions for the taxonomy development are to be determined. Nickerson et al. [10] provide a set of subjective and objective ending conditions. Characteristics and dimensions are determined iteratively using a conceptual-to-empirical or empirical-conceptual approach. The conceptual-to-empirical approach entails the deduction of characteristics based on a researcher's notions regarding a particular domain, supported for example by extant literature. In the empirical-to-conceptual approach, a set of objects is selected and common characteristics among these objects are identified based on the meta-characteristic. The combination of conceptual and empirical phases suits our case of ONSNs where extant literature remains scarce. These characteristics can in turn be grouped, leading to the formation of new or revision of existing taxonomy dimensions. The taxonomy development concludes once all ending conditions are met.

13.3 Methodology

13.3.1 Research Design

Our overall research design consists of (1) a literature review on ONSNs, (2) the identification of real-world ONSNs, (3) the development of a taxonomy of ONSNs and finally (4) the definition of archetypes of ONSNs via cluster analysis (see Figure 1). In the following sections, we provide a description of our conducted research steps.

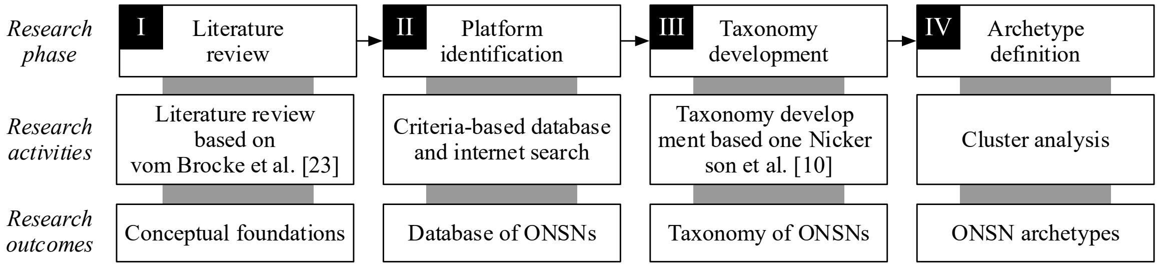


Figure 1. Overall research design

13.3.2 Literature Review

We conduct a structured literature review on ONSNs in order to gain an understanding of the subject and as input for the taxonomy development process. We follow guidance by vom Brocke et al. [23] and search citation indexing services (Google Scholar, Scopus, Web of Science) and bibliographic databases (ACM Digital Library, AISeL, Business Source Complete, IEEE Xplore, ProQuest ABI Inform and Springer Link), limiting our search to peer-reviewed results where possible. After a cursory search, we choose combinations of *neighborhood*, *community*, *social media*, *social network* and *platform* as the most productive terms. Articles included in our review analyze or implement artifacts fitting our definition of ONSNs presented in Section 2.1. Including backward and forward search and excluding duplicates, we identify 8 relevant articles (see also Section 3.4). The final iteration of our review was conducted in July 2019.

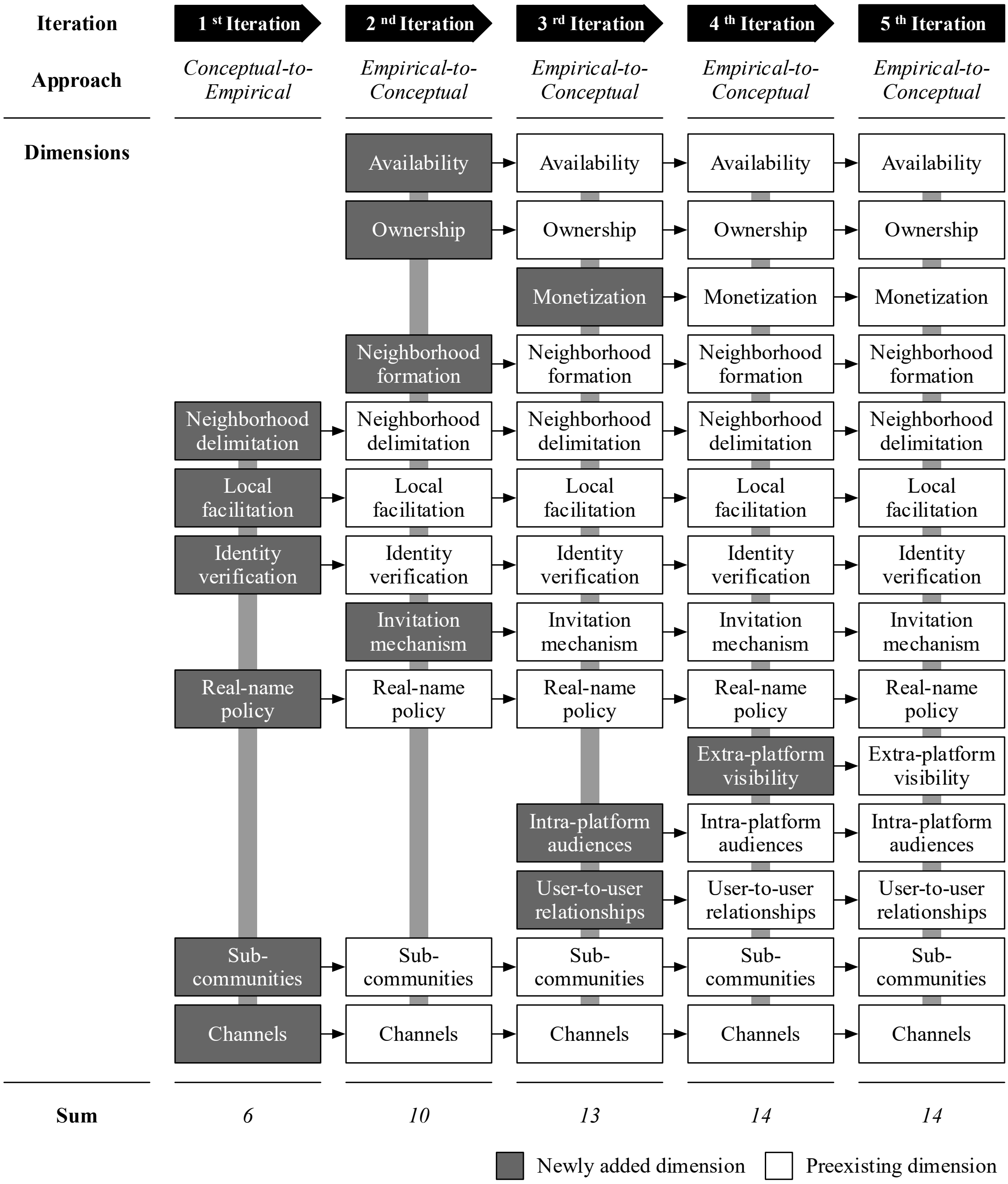
13.3.3 Platform Identification

In order to identify relevant objects for classification in our taxonomy, we perform a criteria-based search using online databases and the Google search engine. We search the crunchbase (crunchbase.com) and CB Insights (cbinsights.com) company databases as well as the iOS App Store and Google Play Store. We utilize combinations of the search terms *neighborhood*, *community*, *local*, *social media*, *social network*. For each identified platform we also perform a web search for corresponding competitors. We shortlist platforms which (1) fit our definition of ONSNs as presented in Section 2.1 and (2) are in operation at the time of analysis. We thereby exclude platforms which have a neighborhood focus but do not fit our definition of ONSNs (e.g. security-only platforms such as Neighbors by Ring) and local social networks without a specific neighborhood focus (e.g. local shopping apps such as Wiva). Where possible, we create user accounts and make direct observations. We supplement this data by analyzing the platforms' knowledge databases, FAQs as well as publicly available materials such as presentations and media reports. Based on these criteria, we identify a total of fifteen ONSNs which are listed as part of our description of ONSN archetypes in Section 5.

13.3.4 Taxonomy Development

Following the methodology presented by Nickerson et al. [10] as well as recommendations made by Oberländer et al. [11], we aim to provide a comprehensive account of our rigorous taxonomy development process. Figure 2 displays an overview of the evolution of our taxonomy of ONSNs across its five iterations. Initially, we define *design properties of online neighborhood social networks* as the meta-characteristic for our taxonomy as it is aimed at researchers and practitioners who intend to analyze, design or use ONSNs. We adopt both the objective and subjective ending conditions proposed by Nickerson et al. [10]. We commence the taxonomy development process by using the conceptual-to-empirical approach and leverage the results of our previously conducted literature review to determine an initial set of dimensions.

We extract the dimensions *neighborhood delimitation* [4], *local facilitation* [4, 5, 9, 15, 24, 25], *identity verification* [4, 9], *real-name policy* [4, 8, 9, 21], *sub-communities* [5, 8, 9, 15, 21, 24] and *channels* [4, 9]. Subsequently, we analyze our sample of ONSNs using the empirical-to-conceptual approach. In the second iteration, we analyze the largest ONSNs based on number of users, Nextdoor and nebenan. By contrasting these ONSNs with each other and the artifacts described in literature, we can identify several differentiating characteristics and group them into the dimensions *availability*, *ownership*, *neighborhood formation* and *invitation mechanism*. In both the third and fourth iteration, we include the entirety of our identified platforms in the analysis. We are able to define *monetization*, *intra-platform audiences, user-to-user relationships* and *extra-platform visibility* as novel dimensions as they provide differentiating characteristics for our taxonomy. In the fifth and last iteration, all ending conditions were met and we therefore concluded the taxonomy development process.



Iteration	1st Iteration	2nd Iteration	3rd Iteration	4th Iteration	5th Iteration
Approach	*Conceptual-to-Empirical*	*Empirical-to-Conceptual*	*Empirical-to-Conceptual*	*Empirical-to-Conceptual*	*Empirical-to-Conceptual*
Dimensions		■ Availability	□ Availability	□ Availability	□ Availability
		■ Ownership	□ Ownership	□ Ownership	□ Ownership
			■ Monetization	□ Monetization	□ Monetization
		■ Neighborhood formation	□ Neighborhood formation	□ Neighborhood formation	□ Neighborhood formation
	■ Neighborhood delimitation	□ Neighborhood delimitation	□ Neighborhood delimitation	□ Neighborhood delimitation	□ Neighborhood delimitation
	■ Local facilitation	□ Local facilitation	□ Local facilitation	□ Local facilitation	□ Local facilitation
	■ Identity verification	□ Identity verification	□ Identity verification	□ Identity verification	□ Identity verification
		■ Invitation mechanism	□ Invitation mechanism	□ Invitation mechanism	□ Invitation mechanism
	■ Real-name policy	□ Real-name policy	□ Real-name policy	□ Real-name policy	□ Real-name policy
				■ Extra-platform visibility	□ Extra-platform visibility
			■ Intra-platform audiences	□ Intra-platform audiences	□ Intra-platform audiences
			■ User-to-user relationships	□ User-to-user relationships	□ User-to-user relationships
	■ Sub-communities	□ Sub-communities	□ Sub-communities	□ Sub-communities	□ Sub-communities
	■ Channels	□ Channels	□ Channels	□ Channels	□ Channels
Sum	*6*	*10*	*13*	*14*	*14*

■ Newly added dimension □ Preexisting dimension

Figure 2. Evolution of taxonomy dimensions (adapted from [13])

13.3.5 Archetype Development

Archetypes represent typical or ideal configurations of object characteristics [26], in our case the design properties of ONSNs. In the last step of our research process, we empirically determine archetypes of ONSNs by performing a cluster analysis using our developed taxonomy. Via cluster analysis, a set of objects is grouped in a way so that objects in the same cluster are more similar to each other than to objects in other clusters [27]. We first calculate the Euclidian distance between our ONSNs to determine their similarly. Subsequently, we apply hierarchical clustering using Ward's method in order to ascertain an appropriate cluster count by observing the resulting cluster dendrogram. Additionally, we inspect the silhouette scores for various potential cluster counts in a preliminary k-means [28] clustering. Based on this pre-analysis, we choose four clusters as the most promising cluster count and perform our final k-means clustering using the k-means++ algorithm [29], resulting in the clusters presented in Section 5. We performed all data analysis actions using the Orange Data Science Toolkit.

13.4 Taxonomy of Online Neighborhood Social Networks

Our taxonomy consists of forty-one mutually exclusive and collectively exhaustive characteristics grouped into fourteen dimensions (see Table 1). We further induce the four overlying meta-categories *Operating model*, *Neighborhood*, *Trust & identity* and *User & content* from the final set of dimensions. In the following, we provide a description of each of our defined taxonomy dimensions.

D₁ Availability – ONSNs in our sample pursue varying approaches regarding their availability. While some platforms are available only in selected neighborhoods, other platforms have a national or multinational presence. A small number of platforms possesses no restrictions regarding availability and is available globally.

D₂ Ownership – Our analyzed ONSNs are either owned and operated by a private, for-profit company or by a public organization or institution.

D₃ Monetization – Monetizing SNSs represents a complex challenge with ONSNs being no exception [30]. While most analyzed platforms are either nonprofit or funded by venture capital, endeavors towards monetization can be observed. These include advertising in the form of sponsored posts, paid listings (e.g. real estate listings), subscriptions for local businesses and neighbors or combinations of these options.

D₄ Neighborhood formation – New neighborhoods are initialized on the initiative of either neighbors or platform providers. Most platforms initialize a new neighborhood only on the request of a neighbor located outside of the boundaries of all preexisting neighborhoods. Other ONSNs proactively initialize neighborhoods themselves and subsequently engage neighbors in order to generate interest in the platform.

D₅ Neighborhood delimitation – We observe a variety of neighborhood delimitation strategies. A number of platforms relies on neighbor's contextual knowledge on neighborhood boundaries and entrusts them with the task of delimiting new neighborhoods. Other platforms arbitrarily define neighborhood boundaries without neighbor input based on considerations such as population density or simply follow municipal boundaries. The remaining platforms in our dataset provide each neighbor with an individual, radius-based neighborhood.

D_6 Local Facilitation – Local facilitation can take the form of marketing activities, neighbor-onboarding or community management. Some ONSNs institute a key user concept of 'Founding Members' or 'Leads' in each neighborhood to perform the aforementioned tasks. Others are tightly integrated with professional neighborhood management services which provide local facilitation.

D_7 Identity verification – ONSNs may require users to verify their identity (name and address) as a precondition for sign-up. Self-service options include verification by submitting a copy of a photo ID or a copy of an official invoice, sharing one's device location, entering a code provided via a mailed letter or postcard and other options. Some platforms offer in-person verification by providing government ID in a local neighborhood management office.

D_8 Invitation mechanism – Some ONSNs offer verified users the ability to invite neighbors onto the platform, sometimes circumventing the need for identity verification for the new user. While most platforms offer a simple online invitation mechanism via sharing a customized link (e.g. via email or instant messenger), more sophisticated mechanisms include printable flyers which can be distributed by users in their building or neighborhood as well as an automated dispatch of postcards to specific neighbors.

Table 1. Taxonomy of online neighborhood social networks

	Dimensions	Characteristics				
Operating model	D_1 Availability	Global	Multi-country	Single-country	Selected cities	Selected neighborhoods
	D_2 Ownership	Private company	Public organization			
	D_3 Monetization	Advertising	Advertising + subscriptions	Advertising + paid listings	No monetiza-tion/nonprofit	
Neighborhood	D_4 Neighborhood formation	Platform-initiated	Neighbor-initiated			
	D_5 Neighborhood delimitation	Municipal boundaries	Arbitrarily neighbor-defined	Arbitrarily platform-defined	Radius-based	
	D_6 Local facilitation	Key user concept	Neighborhood management service	None		

<table>
<tr><td rowspan="3"><em>Trust &amp; identity</em></td><td>D_7 Identity verification</td><td>Self-service</td><td>Self-service + in-person</td><td>None</td></tr>
<tr><td>D_8 Invitation mechanism</td><td>Online</td><td>Online + offline</td><td>None</td></tr>
<tr><td>D_9 Real-name policy</td><td>Enforced</td><td>Encouraged</td><td>None</td></tr>
<tr><td rowspan="5"><em>User &amp; content</em></td><td>D_{10} Extra-platform visibility</td><td>Fully platform-exclusive</td><td colspan="2">Optionally semi-public</td></tr>
<tr><td>D_{11} Intra-platform audiences</td><td>Own + bordering neighborhoods</td><td colspan="2">Own neighborhood only</td></tr>
<tr><td>D_{12} User-to-user relationships</td><td>Available</td><td colspan="2">Not available</td></tr>
<tr><td>D_{13} Sub-communities</td><td>Groups</td><td>Groups + building-level communities</td><td>None</td></tr>
<tr><td>D_{14} Channels</td><td>Website</td><td>Mobile app</td><td>Website + mobile app</td></tr>
</table>

D_9 Real-name policy – There are a number of tradeoffs between anonymity and identifiability on SNS. While anonymous usage may provide a sense of privacy and encourage users to freely and honestly express their views, being identifiable on SNS may lead to stronger social connections, allows for reputation building and serves as a trust-enhancing factor between peers [31]. ONSNs which require identity verification (see D_7) automatically implement a real-name policy. Platforms which are more lenient regarding identity verification typically lack the means to enforce a real-name policy although some encourage usage of one's real-name in their community guidelines and reserve the right to remove accounts with false names. A third group of platforms explicitly has no real-name policy and remains neutral towards name usage.

D_{10} Extra-platform visibility –Some analyzed platforms allow neighbors to optionally expose their user-generated content to the general public, for example via link-sharing or by rendering the content traceable on search engines. This allows users to share for example event invitation with contacts which are not registered on the ONSN. In case of this extra-platform sharing, privacy-sensitive information such as the identities of users who liked a submission are not visible outside of the ONSN.

D_{11} Intra-platform audiences – A number of analyzed platforms pursue a concept of 'bordering neighborhoods'. Neighbors can optionally scale the audience of their submissions to include neighbors in bordering neighborhoods on the same platform, for example when trying to reach a larger audience when promoting an event with cross-neighborhood relevance.

D_{12} User-to-user relationships – Although user-to-user relationships and the resulting traversable social network are principal in the definition of SNSs [18], the functionality for establishing direct, one-to-one relationships by for example adding neighbors as contacts, friends or by following neighbors is not available in all ONSNs.

D$_{13}$ Sub-communities – Most ONSNs enable neighbors to create sub-communities in the form of groups which provide a public or private space related to specific topics of interest. A number of ONSNs automatically creates a sub-communities for all registered neighbors living inside of the same building.

D$_{14}$ Channel –The majority of platforms in our sample provides both a website and mobile app as means of access, however we observe some instances in which platforms are website or app-only.

13.5 Archetypes of Online Neighborhood Social Networks

Based on our cluster analysis described in Section 3.5, we identify four archetypes amongst our fifteen analyzed objects. The crosstab analysis presented in Table 2 illustrates the incidence of characteristics inside each cluster.

Archetype A: Strong neighbor-integration, growth-oriented: ONSNs in this cluster employ advanced monetization strategies, including subscriptions for neighbors and businesses, paid advertising and paid listings for classifieds or real estate. They further exhibit a growth-orientation and leverage their registered neighbors in plentiful ways to this end: they enable neighbors to initialize new neighborhoods, to define neighborhood boundaries and employ a key user concept for local facilitation. Thereby, much of the effort required for growing the platform's audience is crowdsourced to neighbors. Numerous offline and online invitation mechanisms contribute further to this growth-orientation. They strike a compelling balance between user trust, privacy and content reach: they do require identity verification and enforce usage of real-names but also implement a bordering neighborhood concept and allow content to be published semi-publicly if desired. By doing so, neighbors can choose to address a wide audience inside the ONSN itself and also do not run the risk of locking their content to the platform with non-neighbors being unable to access it. ONSNs in this cluster: nebenan (nebenan.de), Neighbourly (neighbourly.co.nz) and Nextdoor (nextdoor.com).

Table 2. Crosstab analysis results based on cluster analysis

	Dimension	Characteristic	**Archetypes** (# ONSNs)			
			A (3)	**B** (3)	**C** (5)	**D** (4)
Operating model	D_1 Availability	Global	0%	0%	0%	25%
		Multi-country	67%	0%	0%	25%
		Single-country	33%	0%	100%	0%
		Selected cities	0%	0%	0%	50%
		Selected neighborhoods	0%	100%	0%	0%
	D_2 Ownership	Private company	100%	0%	100%	100%
		Public organization	0%	100%	0%	0%
	D_3 Monetization	Advertising	0%	0%	20%	50%
		Advertising + subscriptions	67%	0%	0%	0%
		Advertising + paid listings	33%	0%	60%	0%
		No monetization/Nonprofit	0%	100%	20%	50%
Neighborhood	D_4 Neighborhood formation	Platform-initiated	0%	100%	0%	50%
		Neighbor-initiated	100%	0%	100%	50%
	D_5 Neighborhood delimitation	Municipal boundaries	33%	0%	0%	100%
		Arbitrarily neighbor-defined	100%	0%	0%	0%
		Arbitrarily platform-defined	0%	100%	20%	0%
		Radius-based	0%	0%	80%	0%
	D_6 Local facilitation	Key user concept	100%	0%	0%	0%
		Neighborhood management service	0%	100%	0%	0%
		None	0%	0%	100%	100%
Trust & identity	D_7 Identity verification	Self-service	100%	33%	80%	0%
		Self-service + in-person	0%	67%	0%	0%
		None	0%	0%	20%	100%
	D_8 Invitation mechanism	Online	0%	0%	60%	50%
		Online + offline	100%	0%	0%	25%
		None	0%	100%	40%	25%
	D_9 Real-name policy	Enforced	67%	100%	60%	0%
		Encouraged	33%	0%	20%	25%
		None	0%	0%	20%	75%
User & content	D_{10} Extra-platform visibility	Fully platform-exclusive	0%	100%	80%	75%
		Optionally semi-public	100%	0%	20%	25%
	D_{11} Intra-platform audiences	Own + bordering neighborhoods	100%	0%	20%	0%
		Own neighborhood only	0%	100%	80%	100%
	D_{12} User-to-user relationships	Available	0%	0%	40%	25%
		Not available	100%	100%	60%	75%
	D_{13} Sub-communities	Groups	67%	0%	60%	75%
		Groups + building-level communities	33%	0%	20%	25%
		None	0%	100%	20%	0%
	D_{14} Channels	Website	0%	33%	60%	50%
		Mobile app	0%	33%	40%	25%
		Website + mobile app	100%	33%	0%	25%

Archetype B: Publicly-owned, professional facilitation: ONSNs in this cluster are operated by public organizations or institutions such as city governments and universities. Consequently, no monetization strategy is pursued. Their availability is restricted to a handful of specifically selected and delimited neighborhoods. In case of these platforms, local facilitation is provided by professional neighborhood management services and the ONSN represents one element of a broader endeavor related to age-friendliness or smart cities and communities. Trust and privacy features are strictly implemented on these platforms, requiring self-service or in-person identity verification and usage of real-names. User-generated content is locked tightly into the ONSN, with no bordering neighborhood concept or optionally semi-public content being implemented. Included ONSNs: Meine Nachbarn (meinenachbarn.hamburg), Remishueb (remishueb.stadt.sg.ch), wirRauner (wir-rauner.de).

Archetype C: Radius-based, country-specific: ONSNs in this cluster are active in only one specific country, oftentimes possessing country-specific naming and branding. They predominantly use a radius-based approach to delimit neighborhoods, resulting in individual neighborhood boundaries which do not correspond with any traditional neighborhood delimitation concepts such as municipal boundaries. They mostly require some form of identity verification and enforce or encourage usage of real-names. While they do initialize neighborhoods on request of neighbors, they do not implement any local facilitation concept, be it using key users or professional services. User-generated content is restricted to one's own neighborhood and cannot be made visible outside of the ONSN. Platforms in this cluster include FragNebenan (fragnebenan.com), fürenand.ch (fuerenand.ch), JustMyNeighbors (justmyneighbors.com), Nachbarschaft.net (nachbarschaft.net) and ScoopLoop (scooploop.com).

Archetype D: Open, municipal boundaries: ONSNs in this cluster are characterized by their high degree of openness and low neighbor-involvement. They implement low barriers for signup as they abstain from requiring identity verification and enforcing or encouraging real-name usage. While this choice makes it easy for new neighbors to create accounts, it may also fail to create a culture of trust among members of the online community. Furthermore, these ONSNs do not require neighbors to define the boundaries of neighborhoods themselves and instead opt for adopting municipal boundaries to delimit neighborhoods. ONSNs in this cluster include GoNeighbour.Org (goneighbour.org), kiekmo (kiekmo.hamburg), lokalportal (lokalportal.de) and Meet the Neighbors (meettheneighbors.org).

13.6 Discussion

Based on our taxonomy and identified clusters, we derive implications regarding the nature and design of ONSNs along the three central themes of *openness* of ONSNs as well as *neighbor empowerment* and *neighborhood delimitation* on ONSNs. We further discuss the differences between SNS and ONSNs and highlight the role of ONSNs as socio-technical artifacts.

In the context of ONSNs, *openness* characterizes the ease of access to a platform as well as how tightly user-generated content is restricted to one's own neighborhood and the platform itself. ONSNs need to find the right balance between encouraging users to join their platform and restricting access to real neighbors in order to build trust. This trust represents a major advantage for ONSNs over traditional SNS. As a consequence, functionality which is present on both traditional SNSs and ONSNs may receive additional value, for example in case of increased trust between sellers and buyers on a local online marketplace, increased trust in recommendations made by neighbors regarding local businesses or in an increased readiness to request and provide neighborly assistance.

Neighbor-empowerment plays a critical role in ONSN design and is used extensively by some of our analyzed platforms to crowdsource tasks such as marketing, user acquisition or community management to neighbors. While this strategy may enable high growth, it in turn requires platform providers to implement robust platform governance including rules, policies and procedures which ensure the retention of control over factors such as the scope of expansion and quality of content [32].

In this context, letting neighbors define the boundaries of neighborhoods may also improve the chance of capturing already existing offline-communities of neighbors which would otherwise be at risk of being split up in case of platform-defined boundaries. As is already apparent from the discussion of possible definitions of the term neighborhood presented in Section 2.1, *neighborhood delimitation* is not a trivial task. For ONSNs, delimiting or scoping neighborhoods represents a core competency. If neighbors find boundaries on an ONSN which do not correspond with their understanding of their real-life neighborhood for example by being too extensive or too confined, they may not be inclined to use the platform. This challenge is intensified by the need of ONSNs to find an automated or semi-automated way of delimiting new neighborhoods if they hope to achieve scale. Here, our taxonomy shows that platform providers have found a variety of solutions to deal with this issue ranging from neutral, radius-based systems, directly adapting municipal boundaries or letting users delimit their own neighborhood.

We are further able to identify two properties of ONSNs which differentiate them from traditional SNS. First, when comparing our analyzed ONSNs with each other and with traditional SNSs, we find that most high-level functionality (e.g. existence of a timeline, direct messaging, user profiles or events, etc.) does not vary significantly between platforms. Therefore, features on this level were not included in our taxonomy. In consequence, however, this means that the main feature differentiating ONSNs from SNSs is the creation of a community of trust in a limited local area, realized through a combination of identity verification, neighborhood delimitation and real-name policy. If this is indeed the core competency of ONSNs, a central goal when designing ONSNs should be the further exploitation of this trust and identity management, for example in the form of third-party integrations which allow neighbors to transfer their established community of trust to other contexts and services.

Second, as a further differentiator between ONSNs and SNSs, we find that most ONSNs do not implement direct user-to-user relationships such as "friends" or "contacts" which are a defining characteristic of traditional SNS [18]. As opposed to SNS, relationships between users on an ONSN are not primarily based on their social network but on the proximity of inhabiting a common neighborhood. A closed community of neighbors may simply have no need for user-to-user relationships. However, most ONSNs do enable users to create sub-communities such as groups, allowing a further segmentation of neighbors inside the closed neighborhood.

Among our defined archetypes, Archetype B demonstrates an interest of public organizations and institutions to implement their own platforms despite the availability of solutions offered by private companies. Most likely, this is a result of a distinct need to control platform design and development, concerns regarding data privacy and the wish for tighter integration of an ONSN with existing efforts regarding neighborhood development for example via professional neighborhood management services.

Our research highlights the role of ONSNs as socio-technical artifacts whose success is determined to a large extent by the way they are embedded in their environment [33]. Considering this ensemble view of technology, ONSN providers must adequately embed their platforms into the constantly evolving social and environmental context of the neighborhood. Therefore, while the design of an ONSN may be technically sound, it is equally important to consider factors such as local facilitation, integration of organizations and institutions as well as the delimitation of neighborhoods which affect contextual integration [34], which is supported by a multilevel perspective [35]. Our taxonomy serves as a starting point for these considerations.

With our research on ONSNs, we provide a first and comprehensive overview of an increasingly relevant domain within social media which has received little attention in previous research. Our research contributes to understanding the nature of these ONSNs and enables their differentiation based on a set of conceptually grounded and empirically validated design properties. Thereby, our taxonomy can facilitate the design of new as well as the analysis and selection of existing ONSNs for researchers and practitioners. ONSN providers can utilize our defined archetypes to classify and compare their own platform with competing or alternative operating concepts. With our taxonomy and derived archetypes, we provide a common understanding and shared language for the future scholarly discussion of ONSNs.

13.7 Conclusion

Motivated by the potential of ONSNs for improving neighborhood life, their increasing popularity and a lack of research in the field, we develop a conceptually and empirically validated taxonomy of ONSNs. We leverage this taxonomy to derive four archetypes of ONSNs via cluster analysis. Based on these results, we induce implications regarding the nature and design of ONSNs. Our research is faced with several limitations. Our sample of ONSNs used for taxonomy building is biased towards English and German-language platforms, as those were the languages our search was conducted in. Furthermore, despite our cluster analysis following established procedure by employing Ward's method and the k-means algorithm [12, 13], a different clustering approach may have produced slightly varying results. Future research can utilize our taxonomy as well as archetypes and aim to extend our taxonomy with additional characteristics and dimensions based on novel conceptual and empirical insights.

13.8 Acknowledgements

This research was funded in part by the European Regional Development Fund and the City of Hamburg as part of the research project AGQua (https://www.agqua.de).

13.9 References

[1] Smart Insights: Global social media research summary 2019. (2019)

[2] https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Second-Quarter-2019-Results/

[3] Ilena, M., Ard, H., Wim, B.: On the Development of Online Cities and Neighborhoods: an Exploration of Cumulative and Segmentive Network Effects in Social Media.European Conference on Information Systems, Barcelona, Spain (2011)

[4] Vogel, P., Jurcevic, N., Meyer-Blankart, C.: Healthy, Active and Connected: Towards Designing an Age-Friendly Digital Neighborhood Platform.European Conference on Information Systems, Stockholm-Uppsala, Sweden (2019)

[5] Hampton, K.N.: Neighborhoods in the Network Society the e-Neighbors study. Information, Communication & Society 10, 714-748 (2007)

[6] https://blog.nextdoor.com/2019/05/14/nextdoor-raises-123m-to-accelerate-the-global-power-of-local/

[7] https://magazin.nebenan.de/artikel/nebenande-feiert-1-million-nutzer-so-tickt-das-grosste-netzwerk-fur-nachbarn

[8] Masden, C.A., Grevet, C., Grinter, R.E., Gilbert, E., Edwards, W.K.: Tensions in Scaling-Up Community Social Media: A Multi-Neighborhood Study of Nextdoor.ACM Conference on Human Factors in Computing Systems, pp. 3239-3248, Toronto, Canada (2014)

[9] Renyi, M., Gündogdu, R., Kunze, C., Gaugisch, P., Teuteberg, F.: The Networked Neighborhood.IEEE International Conference on Engineering, Technology and Innovation, Konstanz, Germany (2018)

[10] Nickerson, R.C., Varshney, U., Muntermann, J.: A method for taxonomy development and its application in information systems. EJIS 22, 336-359 (2013)

[11] Oberländer, A.M., Lösser, B., Rau, D.: Taxonomy Research in Information Systems: A Systematic Assessment.European Conference on Inofrmation Systems, Stockholm-Uppsala, Sweden (2019)

[12] Kutzner, K., Petzold, K., Knackstedt, R.: Characterising Social Reading Platforms - A Taxonomy-Based Approach to Structure the Field.International Conference on Wirtschaftsinformatik, Siegen, Germany (2019)

[13] Remane, G., Nickerson, R.C., Hanelt, A., Tesch, J.F., Kolbe, L.M.: A Taxonomy of Carsharing Business Models.International Conference on Information Systems, Dublin, Ireland (2016)

[14] Gurstein, M.: What is Community Informatics (and Why Does It Matter)? (2007)

[15] Carroll, J.M., Rosson, M.B.: Developing the Blacksburg electronic village. Communications of the ACM 39, 69-74 (1996)

[16] Kim, Y.-C., Shin, E.-K.: Localized Use of Information and Communication Technologies in Seoul's Urban Neighborhoods. American Behavioral Scientist 60, 81-100 (2016)

[17] Voskresenskiy, V., Musabirov, I., Alexandrov, D.: Studying Patterns of Communication in Virtual Urban Groups with Different Modes of Privacy. SSRN Electronic Journal (2017)

[18] boyd, d.m., Ellison, N.B.: Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication 13, 210-230 (2007)

[19] Diez Roux, A.V.: Investigating neighborhood and area effects on health. American journal of public health 91, 1783-1789 (2001)

[20] Sampson, R.J., Raudenbush, S.W., Earls, F.: Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy. Science 277, 918 (1997)

[21] Antonini, A., Boella, G., Calafiore, A., Salaroglio, C., Sanasi, L., Schifanella, C.: First Life, the Neighborhood Social Network: a Collaborative Environment for Citizens.ACM Conference on Computer Supported Cooperative Work and Social Computing Companion (CSCW), pp. 1-4. ACM, San Francisco, California, USA (2016)

[22] Emamjome, F.F., Gable, G.G., Bandara, W., Rabaa'i, A.: Understanding the value of social media in organisations: a taxonomic approach.Pacific Asia Conference on Information Systems, pp. 59, Chengdu, China (2014)

[23] vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. CAIS 37, (2015)

[24] Hampton, K., Wellman, B.: Neighboring in Netville: How the Internet Supports Community and Social Capital in a Wired Suburb. City & Community 2, 277-311 (2003)

[25] Rogers, E.M., Collins-Jarvis, L., Schmitz, J.: The PEN project in Santa Monica: Interactive communication, equality, and political action. Journal of the American Society for Information Science 45, 401-410 (1994)

[26] Blaschke, M., Haki, K., Aier, S., Winter, R.: Taxonomy of Digital Platforms: A Platform Architecture Perspective.International Conference on Wirtschaftsinformatik, Siegen, Germany (2019)

[27] Kaufman, L., Rousseeuw, P.J.: Finding Groups in Data: An Introduction to Cluster Analysis. Wiley-Interscience (2009)

[28] Hartigan, J.A., Wong, M.A.: Algorithm AS 136: A K-Means Clustering Algorithm. Journal of the Royal Statistical Society 28, 100-108 (1979)

[29] Arthur, D., Vassilvitskii, S.: k-means++: the advantages of careful seeding.ACM-SIAM Discrete Algorithms, pp. 1027-1035. Society for Industrial and Applied Mathematics, New Orleans, Louisiana (2007)

[30] Clemons, E.K.: The complex problem of monetizing virtual electronic social networks. Decision Support Systems 48, 46-56 (2009)

[31] Kang, R., Brown, S., Kiesler, S.: Why do people seek anonymity on the internet?: informing policy and design.SIGCHI Conference on Human Factors in Computing Systems, pp. 2657-2666. ACM, Paris, France (2013)

[32] Barrett, M., Oborn, E., Orlikowski, W.: Creating Value in Online Communities: The Sociomaterial Configuring of Strategy, Platform, and Stakeholder Engagement. Information Systems Research 27, 704-723 (2016)

[33] Orlikowski, W.J., Iacono, C.S.: Desperately Seeking the "IT" in IT Research—A Call to Theorizing the IT Artifact. Information Systems Research 12, 121-134 (2001)

[34] Grotherr, C., Vogel, P., Semmann, M.: Multilevel Design for Smart Communities: The Case of Building a Local Online Neighborhood Social Community.Hawaii International Conference on System Sciences, Grand Wailea, HI, USA (2020)

[35] Grotherr, C., Semmann, M., Böhmann, T.: Using Microfoundations of Value Co-Creation to Guide Service Systems Design – A Multilevel Design Framework.International Conference on Information Systems (ICIS), San Francisco, California, USA (2018)

14 Article No. 6 (Jacobs et al. 2021)

Jacobs, M., Kurtz, C., Simon, J., and Böhmann, T. Value sensitive design and power in socio-technical ecosystems. Internet Policy Review, 2021.

Abstract

Recent European policy papers call for the consideration of human values in the design of information technology. Value Sensitive Design (VSD) provides a framework for systematically accounting for values in the design of technical artefacts. This paper examines how the distribution of power within socio-technical ecosystems poses a challenge for the application of VSD. It identifies four crucial factors determining the effect of the distribution of power on VSD: the *level of decentralisation* of the ecosystem; if VSD is applied at the *core* or *periphery*; when power can be exercised *(temporality)*; and the *phase of VSD* (conceptual, empirical, and technical) that power can be exercised in. Based on these factors, it outlines how the challenge of accounting for power can be addressed.

14.1 Introduction

Recent European policy papers call for the consideration of human values[8] in the design of information technology (European Commission, 2020a, 2019; HLEG-AI, 2019; *Datenethikkommission*, 2019). Approaches such as Value Sensitive Design (VSD) promote the idea that human values can be accounted for in the development of technological artefacts and provide a framework for systematically analysing, weighing, and operationalising them (Friedman et al., 2008; Friedman & Hendry, 2019). However, while VSD is well received in the academic context and attracts attention from various disciplines such as computer science and information systems (Friedman et al., 2008; Friedman & Hendry, 2019; Winkler & Spiekermann, 2018; Mueller & Heger, 2018), computer ethics (Brey, 2010; Introna, 2005), healthcare (Walton & DeRenzi, 2009), urban design (Borning et al., 2008; Waddell et al., 2008) and others, there are challenges barring the path to widespread adoption.

Reflecting on such "grand challenges", Friedman and Hendry (2019) name "accounting for power" as one of them.[9] In this paper, the term "power" refers to "the ability of agents […] to realize a certain outcome" (Brey, 2008, p. 75)[10]—specifically design decisions—"even against resistance" (Weber, 2019, p. 134). Friedman and Hendry (2019) elaborate on the challenge: VSD "has not yet explicitly addressed how to handle differences in power among […]stakeholders [and how] best to account for power relations within a value sensitive design framing remains an open question."

This paper argues that this challenge is exacerbated in many cases by the integration of technical artefacts in increasingly vast and complex socio-technical ecosystems defined as "a dynamic community of competing and interdependent people, organizations, and computing systems operating in a complex, capricious environment" (McConahy et al., 2012, p. 1). In such socio-technical ecosystems, the power over the variety of independent design decisions which, in their totality, define the shape of an artefact is often distributed over various actors. Furthermore, due to their socio-technical nature, containing a "technical, social, political, and economic" (van House, 2004, p. 18) as well as "organizational […] and

[8] This paper uses Friedman and Hendry's (2019, p. 24) working definition of the term "human value," referring to "what is important to people in their lives, with a focus on ethics and morality". While the term has been criticised as being both under- and over-defined, it provides an appropriate balance for the practical application in the context of Value Sensitive Design. For an in-depth discussion of existing critique on the definition as well as the advantages and disadvantages of various alternative definitions see Friedman and Hendry (2019) and Brey (2010).

[9] The identification of the "grand challenges" for Value-Sensitive Design that Friedman and Hendry refer to took place at two workshops in 2015 and 2016 organised by Batya Friedman, David Hendry, Jeroen van den Hoven, Alina Huldtgren, Catholijn Jonker, Aimee van Wynsberghe, and Maike Haarbers in Aarhus, Denmark, and Leiden, The Netherlands, respectively. The workshops aimed at "Charting the next decade" for the approach (Friedman & Hendry, 2019).

[10] Accordingly, the conceptualisation of power used in this paper does not capture the ability to exercise control over other agents (Brey, 2008).

business" (Feiler et al., 2006, p. 27) domain, power can manifest in various forms in these ecosystems.[11] In order to account for all the domains in which power can manifest itself, the paper adopts a systemic view on power, which "regards power as the property of broader social, economic, cultural, and political networks, institutions, and structures" (Sattarov, 2019, p. 20) and focuses on how "systems confer differentials of dispositional power on agents, thus structuring possibilities for action" (Haugaard, 2010, p. 425; see also Sattarov, 2019).

The remainder of this paper explores the following questions: 1) how and to what extent does the "grand challenge" of accounting for power in VSD get exacerbated by the integration of technical artefacts in increasingly vast and complex socio-technical ecosystems; 2) how does the organisational structure of socio-technical ecosystems affect the challenge of accounting for power in VSD; 3) how can this challenge be addressed; and 4) are there positive effects for VSD if the approach is applied in settings in which the power to make design decisions is distributed over various actors.

Section 2 provides an overview of VSD. Section 3 further elaborates on the actors involved in developing technical artefacts in different types of socio-technical ecosystems and their respective leverage over how developers can account for specific values. It discusses two exemplary types of socio-technical ecosystems that differ in the degree of decentralisation and, thus, the way power is distributed within them: platform ecosystems such as Apple's iOS ecosystem (section 3.1) and blockchain-based systems such as Bitcoin and Ethereum (section 3.2). Section 4 outlines how adopting a power-sensitive ecosystem perspective can foster a more pronounced understanding of the challenge of accounting for power. Based on these observations, section 5 derives some reference points for addressing the challenge of accounting for power in socio-technical ecosystems. Lastly, section 6 concludes.

14.2 The Value Sensitive Design Approach

According to Friedman and Hendry (2019, p. 3), VSD "seeks to guide the shape of being with technology". Directed at "researchers, designers, engineers, policy makers, and anyone working at the intersection of technology and society […], it provides theory, method, and practice to account for human values in a principled systematic manner throughout the technical design process". To account for values in the design process of technical artefacts, VSD is structured in three phases of action: conceptual, empirical, and technical investigations. Pertinent literature maps out the respective phases

[11] See, e.g., van Dijck et al. (2018) for political and economic manifestations of power, Shilton and Greene (2019) for technical manifestations of power, and De Filippi et al. (2020) for social manifestations of power.

primarily by determining what practitioners should aim to achieve in them. The approach deliberately refrains from prescribing specific methods in the individual phases, allowing VSD practitioners to select and integrate methods tailored to the respective context of application on a case-by-case basis (Friedman et al., 2008; Friedman & Hendry, 2019).

Conceptual investigations "comprise analytic, theoretical, or philosophically informed explorations of the central issues and constructs under investigation" (Friedman & Hendry, 2019, p. 12). They address issues such as the identification of direct and indirect stakeholders, the nature of the respective stakeholder's implication, the conceptualisation of values, and dealing with value conflicts (Friedman et al., 2008). Regarding value conflicts, it is important to note that such conflicts can also exist between human and instrumental values (Friedman & Hendry, 2019) and between values that are directly affected and values whose preservation is being put at risk only in the future (see Czeskis et al., 2010). In a more recent publication, Friedman and Hendry (2019) also include developing a framework for evaluating a successful application of VSD into this phase.

Empirical investigations employ quantitative and qualitative social sciences methods to determine the stance of (groups of) stakeholders towards values and their respective weighing (Simon, 2016). Additionally, practitioners can deploy empirical methods in a later stage to "evaluate the success of a particular design" with regards to whether it supports the realisation of a particular value as intended (Friedman et al., 2008, p. 72). Empirical investigations of this second form aim to answer whether the objectives defined in the conceptual investigation have been achieved. In both early- and late-stage empirical investigations, developers apply advanced survey and interview methods to disclose discrepancies between the espoused practice of stakeholders with their actual practice (Friedman et al., 2008). Thus, empirical investigations provide "a more situated understanding of the socio-technical system" in question and facilitate "the observation of stakeholders' usage and appropriation patterns, but also whether the values envisioned in the design process are fulfilled, amended, or subverted" (Simon et al., 2020, p. 4).

Technical investigations also take two different forms in VSD. The first form comprises a retrospective analysis of existing technological artefacts and aims at disclosing "underlying mechanisms [that] support or hinder human values" (Friedman et al., 2008, p. 73). This form thus corresponds roughly to what Brey (2010) and Introna (2005) refer to as "Disclosive Computer Ethics". The second form of technical investigations "involve[s] the proactive design of systems to support values identified in the conceptual investigation" (Friedman et al., 2008, p. 73). Practitioners here address how the respective conceptualisation and weighing of values can be operationalised and accounted for in the design process, i.e., how they can be translated into code.

The three phases of Value Sensitive Design repeat iteratively. Neither a starting point nor an order is prescribed. The respective phases are intended "to inform and shape and reshape each other" through the iterations (Friedman & Hendry, 2019, p. 35).

Because VSD does not prescribe the use of specific methods in the respective phases, recent overview articles and literature reviews (Friedman et al., 2017; Friedman & Hendry, 2019; Winkler & Spiekermann, 2018) provide practitioners of VSD with heuristics on how to proceed by invoking exemplary case studies. They instance methods such as stakeholder analyses (Friedman et al., 2006), value scenarios (Nathan et al., 2007), ethnographically informed inquiries (Nathan, 2012), multi-lifespan timelines (Yoo et al., 2016), and others.Additionally, pertinent literature provides further heuristics such as lists "of human values with ethical import that are often implicated in system design" as a tangible basis for practical application (Simon et al., 2020, p. 4; see also Friedman et al., 2008).

14.3 Accounting for Power in Socio-Technical Ecosystems

In contrast to the development of independently working, stand-alone, monolithic technical artefacts, the development of artefacts integrated into socio-technical ecosystems have a much more constrained scope for design. To enable coordination among providers of components of a socio-technical ecosystem, the component's design must account for the existing technical and non-technical features of the ecosystem. Thus, the actors (co-)determining these features set restrictions to design decisions for novel components of an ecosystem (McConahy et al., 2012), including attempts to account for human values.

The following sections showcase two types of socio-technical ecosystems, characterised by different actor constellations, to reveal the specific manifestation of the challenges for applying VSD in the respective contexts. Section 3.1 focuses on platform-based ecosystems such as Apple's iOS, Google's Android, and the Facebook ecosystem, whereas section 3.2 focuses on blockchain-based ecosystems. The cases differ in how power is distributed in the respective types of ecosystems, how it manifests, how visible its distribution is, and the available modes of governance to address power-related issues. The dissimilarity of the cases allows to take a wide-angle perspective and to identify various facets of the challenge of accounting for power in VSD.

14.3.1 Platform-Based Ecosystems

The majority of digital interactions occur in ecosystems, often facilitated and connected over a digital platform (Lusch & Nambisan, 2015). The term "platform" is often a source of confusion due to a variety of definitions. In this paper, the term refers to a software-based system as the core with an extensible codebase that enables functionality for users through additional software subsystems in the form of peripheral applications—or modules—that interoperate with it (Baldwin & Woodard, 2009; Reuver et al., 2018; Tiwana et al., 2010). Peripheral services are provided by developers to enable the provision of functionality, service, or content (Constantinides et al., 2018), which can be accessed by the user via the platform (Ghazawneh & Henfridsson, 2013).

Previous research has already addressed some challenges for applying VSD (or accounting for human values more generally) in platform-based ecosystems (Shilton & Greene, 2016; Shilton & Greene, 2019; van Dijck et al., 2018; Warnier et al., 2015). For instance, focusing on deliberations of mobile application developers in developer forums on how to account for values, especially privacy, Shilton and Greene (2016) demonstrate the extent to which platform providers can assert their ideas without actively engaging in design processes. Shilton conceptualises the platform provider's means to do so as "value levers" (Shilton, 2012) and, together with Greene, provides comparative studies on the use of these levers in different platform ecosystems (Shilton & Greene, 2019). However, a more elaborate ecosystem perspective—as developed in information systems research—could provide a means to refine such an analysis.

According to information systems literature, the platform provider's central role in platform-based ecosystems is a facilitating one (van Alstyne et al., 2016). To scale a platform, the platform provider needs to attract external actors into the platform ecosystem that engage in interactions. In platform-based ecosystems, mainly actors of four different groups come together: users, platform providers, app providers, and third parties. Platforms enable external developers to contribute to the ecosystem by providing so-called *boundary resources* (Constantinides et al., 2018; Tiwana & Konsynski, 2010). Boundary resources are socio-technical manifestations of the platform provider's power to influence a platform ecosystem (Ghazawneh & Henfridsson, 2013), such as application programming interfaces (API), software development kits (SDK), legal guidelines, and application approval processes (Eaton et al., 2015; Karhu et al., 2018).

As control points for a platform provider, boundary resources facilitate an arm's length relationship between the platform provider and service providers (Ghazawneh & Henfridsson, 2013). They offer the providers of peripheral applications access to a platform's resources while allowing the platform provider to retain influence over the platform (Eaton et al., 2015). Using boundary resources, a platform provider orchestrates its platform ecosystems and enables service providers to participate in and contribute to the platform's development (Eaton et al., 2015). Designing and implementing boundary resources is a balancing act of retaining power while supporting service providers to create independent platform-based innovation (Eaton et al., 2015). Thus, platform providers hold the privileged position to exercise power by determining the design of boundary resources and thereby influence the actions of service providers and third parties involved with the platform (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013), with direct implications for how these actors can account for values.

This indicates that platform providers can serve a decisive role in encouraging (or discouraging) design decisions that support the realisation of human values. For instance, in the redesign of its boundary resources via iOS 13, Apple introduced fine-grained user configuration options regarding the usage of location data by apps (Apple, 2019). In previous iOS versions, users could choose among the three options 'Never', 'While Using the App', and 'Always' (Apple, 2019). iOS 13 introduced the additional option 'Ask Next Time'. Users and the developers of applications in Apple's ecosystem are directly affected by such decisions. The configuration options have a considerable impact on user information privacy since the user can make case-by-case decisions on whether or not to grant access to their location data to an app. App developers, on the other hand, have to consider these case-by-case decisions in the expected user behaviour. Platform providers mostly prescribe such changes in boundary resource design unilaterally. Users and developers of peripheral applications are often regarded as passive recipients of these changes. Although the developers of peripheral applications can generate some degree of pressure through public criticism (Hestres, 2013) or building coalitions to achieve their goals (Perez, 2020), the decision-making power lies with the platform provider, in this case, Apple.

In another instance, Apple changed the data interface design for apps to access the MAC (Media Access Control) addresses of the devices an iPhone is connected to. Various applications misused this interface to bypass restrictions on location data access. They approximated the location data by using these MAC addresses in combination with publicly available databases that offered the specific locations of the devices that hold the respective MAC addresses. With the update to iOS 11 in 2017, access to these network data was disabled (Butts, 2017). However, the interface design also blocked data access for app providers that offer network services. As a consequence, these apps were no longer functioning. Thus, Apple restricted the scope for design of app providers, ruling out an operationalisation of privacy that would maintain the existing functionality.

Lastly, digital service providers and related services may also be influenced by the necessity of maintaining and keeping up with platform updates by the platform provider, such as APIs or framework refinements (Ausloos & Veale, 2020). For instance, in OS 14, Apple established the framework *App Tracking Transparency,* playing out privacy features more prominently than in earlier versions of iOS. Due to these changes, app developers have to request user authorisation to access app-related data for tracking the user or the device (Apple, 2020). In the future, Apple intends to ban applications that track users without permission and thus violate the new requirements and respective guidelines (Leswing, 2021). In consequence, Apple's decision to establish third-party transparency has a significant influence on how developers of peripheral applications can conceptualise and operationalise data protection and information privacy.

14.3.2 Blockchain-Based Ecosystems

A blockchain is a distributed, encrypted, chronological database of transactions recorded by a distributed network of computers (Morabito, 2017; Wright & De Filippi, 2015). It contains "every transaction that has been carried out and shared among those participating in the network" (Morabito, 2017, p. 4). The entries are "encrypted and organized" in "smaller datasets referred to as 'blocks,'" each of which references "to the preceding block in the blockchain" (Wright & De Filippi, 2015, p. 7). A consensus mechanism warrants the integrity of each transaction over the network. Contrary to other approaches in computer security, in open, permissionless blockchains, the consensus mechanisms are not based on access control, i.e., on "carefully vetting participants and excluding bad actors" (Antonopoulos, 2014). Instead, they rely on economic incentive systems that aim at motivating actors—referred to as miners (Alsindi & Lotti, 2021)—to participate in the validation process and ensuring that it is "more profitable and attractive [for them] to contribute to the network than to attack it" (Brekke & Alsindi, 2021, p. 2). As a result of this approach, "the key characteristics of a blockchain [...] are that it is: distributed, decentralized, public or transparent, time-stamped, persistent, and verifiable." (DuPont & Maurer, 2015, p. 2). Moreover, the blockchain technology is not restricted to the record-keeping function it utilises in its origin in cryptocurrencies. More recently developed blockchain-based systems such as Ethereum incorporate Turing-complete virtual machines that allow executing not only simple transactions but also more complex operating steps. In turn, this enables running decentralised second-layer applications (DApps) as services on top of the system.

In line with discourses around earlier decentralised technical systems such as the internet (Bodó et al., 2021), developers, scholars, and the broader community discussed blockchain technology in value-related terms from the very beginning. In this discourse, a libertarian reading of the technology is dominant (De Filippi, 2017; Werbach, 2018; Wright & De Filippi, 2015). Furthermore, trustworthiness (Becker & Bodó, 2021; Hawlitschek et al., 2018; Jacobs, 2021; Werbach, 2018) and sustainability (Alsindi & Lotti, 2021; Giungato et al., 2017) are discussed prominently as values that should be accounted for in the technology's technical design.Notably, design decisions regarding comparably subtle changes in a system's protocol—such as a change in the number of transactions aggregated in one block—are debated by the community in terms of values embodied in the respective design decision (Werbach, 2018).

The technical properties of blockchain-based systems affect the applicability of VSD. In contrast to the platform-based ecosystems discussed in the previous section, there is no central entity controlling the system that can unilaterally determine the design of technical interfaces (Antonopoulos, 2017). Thus, consent between several (groups of) actors is necessary to implement protocol amendments successfully. These are, first and foremost, the developers themselves, but also a significant share of miners, cryptocurrency exchanges, and token holders.

The software protocols of open and permissionless blockchains are maintained as open source projects, i.e., the code is publicly available, everyone can propose or recommend code changes and amendments, and a "mix of volunteer and paid software developers write and update the software" (Walch, 2019, pp. 60–61). However, while there are no explicit boundaries to participating in the design process in many blockchain-based systems, there are still groups of core developers with additional rights that guide and oversee the design processes in most larger systems (Walch, 2019). Thus, as Werbach (2018, p. 104) notes, "developers have more power than they let on. […] And even in an open-source project, a single individual can exercise significant authority."

However, core developers only propose updates. Ultimately, the actors running the network need to "adopt and run [these] implementation[s]" (Antonopoulos, 2017, p. 259). Since the developers do not operate the system, they only create a new version of the system's protocol in a software repository, i.e., they create a "software fork". The respective nodes, miners, and wallet-holders individually decide whether or not they use client software with the updated version of the protocol, i.e., create a "network fork" (Antonopoulos, 2017).

As many protocol upgrades lead to consensus rules that are not "forward compatible" (Antonopoulos, 2017; see also Swan, 2015), i.e., they are incompatible with the pre-upgrade version's ones, miners continuing to proceed according to the old rules and miners proceeding according to the new rules from this point on participate in diverging ledgers. In such a *hard fork*, "two chains evolve independently" from one another (Antonopoulos, 2017, p. 257). If, in the long run, either all or no miners follow the core-developers advice to adhere to the new version of the protocol, one respective branch of the fork perishes. If a sufficiently large group of miners adheres to either version of the protocol, the network splits, with both ledgers persisting. These share the same history but are henceforth dissociated from one another (Antonopoulos, 2017; for a discussion of several cases see DuPont, 2019).

Furthermore, cryptocurrency exchanges, too, need to adopt the new rules for them to be successfully introduced (Antonopoulos, 2017). While exchanges do not directly engage in maintaining or running blockchain-based systems and exist merely at their fringes, they nevertheless impact the incentives that drive the more central actors. For instance, cryptocurrency exchanges need to decide which ledger they list, i.e., for which of the ledgers they offer exchanges to customers and thus provide easy access to the system as a whole. While a delisting on one exchange platform potentially only has negligible effects, a coordinated effort to delist a system by several major platforms can hinder access to the system and diminish the economic incentives to participate in it (Orcutt, 2019).

The actors involved in blockchain-based systems thus do not only potentially hold different values or have diverging preferences and incentives regarding the conceptualisation or operationalisation of values but wield sufficient power to unilaterally intervene in design decisions that concern the realisation of a specific value. Moreover, various recent examples showcase that this is not a mere theoretical possibility, but that diverging preferences regarding values in practice do entice these actors to make use of these means.

Regarding core developers, one of the most prominent instances took place in the aftermath of a hack—commonly referred to as "TheDAO hack"—in which an attacker was able to gain hold of assets worth around "$55 million at the time" (De Filippi & Wright, 2018, p. 141) and siphon them to a fund under its control. However, before the attacker was able to move the assets further or sell them on a cryptocurrency exchange (Botsman, 2017), the core developers of Ethereum pushed through a code update to ultimately void the illicit transactions and "recover the funds from the attackers" (De Filippi & Wright, 2018, p. 141). Because this update affected not just the general principles and functionality of the technology but also individual transactions, commentators commonly use the example of this update to illustrate the power of core developers in the system (De Filippi & Wright, 2018; Walch, 2019; Werbach, 2018). By voiding the transactions, the core developers made a value judgment in that they favoured the restoration of trust in the community over the ledger's integrity, understood as the immutable nature of ledger entries. This is because the reversal of the transactions "meant that Ethereum transactions were not truly immune from centralized interference" (Werbach, 2018, p. 68).[12]

Peculiarly, the case of "TheDAO" hack also serves as a curious case highlighting the role that significant miners take in the process of incorporating code amendments, as they independently decide whether or not to follow the core developers' advice to update their client software. In the case of the TheDAO hack, the community split (DuPont, 2018, 2019). While most miners followed the core developers' advice, a minority stuck to the old protocol and thereby created an incompatible version of the shared ledger called "Ethereum Classic" (Werbach, 2018). This example demonstrates that only by convincing large proportions of significant miners to adopt the updated implementation developers can turn a software

[12] Walch (2019) lists further examples of core developers wielding power in design processes.

fork into a network fork (Antonopoulos, 2017). Therefore, as a stakeholder group, miners cannot be overruled or circumvented in design decisions regarding protocol changes.[13]

Lastly, the coordinated approach of various cryptocurrency exchanges to delist the Bitcoin-Cash spin-off Bitcoin SV highlights the capability of cryptocurrency exchanges to engage in the negotiation process on how a blockchain-based system should account for human values. Here, two groups of stakeholders proposed different code upgrades for the Bitcoin Cash protocol. One group, surrounding "the developers of the most popular Bitcoin Cash software client, called Bitcoin ABC, proposed a series of upgrades, including smart contract capability." In contrast, another group, including a mining pool controlling "more than 15 percent of all Bitcoin Cash mining," proposed a divergent upgrade without such fundamental changes to the system's capabilities (Orcutt, 2018). The advocates of this alternative upgrade claimed that it adheres more closely to the original ideals of Bitcoin as outlined in early white papers.

Consequently, a *hard fork* occurred, establishing Bitcoin SV as a spin-off of Bitcoin Cash, followed by turmoil within the community and what Orcutt (2019) calls "social media-fueled coin delistings". Major cryptocurrency exchanges like Kraken or Binance released statements criticising the team behind the newly established Bitcoin SV. KRAKENFX (2019) announced that the behaviour of "the team behind Bitcoin SV" in the aftermath of the fork was incongruent with the values held by "Kraken and the wider crypto community". Binance (2019) questioned whether Bitcoin SV "continues to meet the high level of standard" they expect. Consequently, the two exchanges—among others—stopped exchanging Bitcoin SV on their platforms, which, in turn, lead to "a substantial drop in [Bitcoin SV's] value" (Orcutt, 2019), restricted access to the system for its users, and diminished economic incentives to participate in the system for Bitcoin SV miners.

14.4 Findings

Sections 3.1 and 3.2 offer several insights into the challenge of accounting for power in VSD. These allow identifying four crucial factors that co-determine the effects of the distribution of power in socio-technical ecosystems on the applicability of VSD.

[13] Highlighting the power of significant miners in design processes manifested in the discourse on the Bitcoin block-size, which resulted in the hard fork of Bitcoin and Bitcoin Cash in 2017 (DuPont, 2019).

14.4.1 Level of Decentralisation

Juxtaposing platform-based ecosystems and blockchain-based ecosystems suggests that considering the *level of decentralisation* of the ecosystem is of paramount importance for determining the kind of issues that might occur when accounting for power in the application of VSD. As Shilton and Greene (2019) demonstrate, actors like platform providers at the centre of more centralised ecosystems can assert their ideas of conceptions, weighings, and operationalisations of values to a large extent. Using boundary resources as value levers, they do not just enforce these conceptualisations, weighings, and operationalisations onto the core components of the ecosystem, which they directly control, but also onto the design of peripheral applications.

Conversely, in organisationally more decentralised ecosystems, there is, by definition, no central actor who can similarly assert itself. As shown in the case of open and permissionless blockchains, many actors have the power to impact decisions in the context of how human values are conceptualised, weighed, and operationalised in the design processes. The distribution of power in such ecosystems makes some form of deliberation and coordination inevitable to avoid gridlocks.

14.4.2 Core/Periphery

Different issues arise in design decisions concerning an ecosystem's core components and design decisions concerning peripheral applications. The design of the core components, for the most part, affects more stakeholder groups than the design of peripheral services. Accordingly, negotiation processes are often more complex and conflictual.

Conversely, on the side of peripheral applications, fewer actors are involved. Instead, VSD practitioners have to consider boundary resources that constrain their scope for design. They need to account for the ecosystem's technical and non-technical infrastructure and the actors in charge of it. Section 3.1 underlines the resulting power imbalance in platform-based ecosystems. Platform providers determine the design of boundary resources largely independently and, as a result, determine the scope for design of developers of peripheral services.

14.4.3 Temporality

As demonstrated in the two cases, how actors can exercise power varies considerably. One key difference is *temporality*. Some means of exercising power function *ex-ante*, i.e., actors suppress potential design decisions from being implemented in the first place. Examples of *ex-ante* exercises of power are the design of technical interfaces that predetermine how data can be accessed and managed, how users and peripheral services can interact, and more generally, which criteria peripheral services have to meet in order to be compatible with an ecosystem's technical infrastructure. By utilising technical interfaces, central actors can predetermine how human values like privacy can be conceptualised and operationalised in the entire ecosystem. Other modes of exercising power function *ex-post*, i.e., they interfere with a technical artefact's deployment or usage after an undesired design decision is implemented. Examples of means to exercise power *ex-post* are, for instance, app-store approval processes that central actors can use to exclude specific applications or services from a platform, or the decision of significant miners in blockchain-based ecosystems to omit using a new version of a blockchain protocol after developers deployed it in a software repository.

14.4.4 Phase of VSD

The two cases demonstrate that accounting for power is relevant for making decisions in the conceptual, empirical, and technical *phase of VSD*. They reveal that the way power is situated in the "broader social, economic, cultural, and political networks, institutions, and structures" (Sattarov, 2019, p. 20) of an ecosystem affects how human values are conceptualised (as demonstrated in the analysis of iOS and Android developer forums by Shilton and Greene (2019)), weighed (as demonstrated by Ethereum's core developers' value-judgement leading to recovering the funds after TheDAO hack), operationalised (as demonstrated by Apple's move to change the data interface design for apps to access the MAC addresses of devices), and how the overall process of accounting for values can be evaluated (as illustrated by "social media-fueled coin delistings"). Accounting for power thus concerns VSD practitioners in all phases of VSD.

14.5 Discussion

These observations allow deriving some points of reference for addressing the challenge of accounting for power. They suggest that the general applicability of VSD and its potential to address power-related issues varies tremendously depending on features of the ecosystem and the role that a given artefact is supposed to play in it. While the distribution of power within an ecosystem, in some cases, hinders the application of VSD, it appears to accommodate the approach in other cases. Though this is true for both more centralised and more decentralised systems, the decisive factors differ.

In more centralised ecosystems like platform-based ecosystems, boundary resources function as obligatory passage points (Law & Callon, 1992; see also Callon, 1984) for peripheral applications and constrain the application's design process. These constraints cut back on the agency of developers and can either obstruct or compel design decisions that promote or demote the realisation of specific values.[14] Shilton and Greene (2019) outline discussions from iOS and Android developer forums that illustrate this lack of agency of developers of peripheral applications in platform-based ecosystems. Here, developers are often required to interpret and realise a concept of privacy that is predefined and manifests, e.g., in the platform's boundary resource design. As Greene and Shilton (2017, p. 16) note, "platforms govern design by promoting particular ways of doing privacy, training devs on those practices, and (to varying degrees) rewarding or punishing them based on their performance". Thus, while developers of peripheral applications can always decide to collect less data, privacy here, for the most part, is whatever the platform providers define as privacy. A meaningful application of VSD is virtually non-viable for developers of peripheral applications in such settings.

While Hestres (2013) and van Dijck et al. (2018) outline how concerted efforts of various stakeholder groups can principally have success in appealing to platform providers and lead to changes in boundary resource design, this commonly is not part of the design process of individual technical artefacts and thus outside the scope of VSD. Nevertheless, grassroots efforts proved effective in many cases and should be considered a tool to create the necessary environment for an application of VSD by VSD practitioners in more centralised socio-technical ecosystems.[15]

However, if Apple's boundary resource design is assessed regarding its direct impact on the realisation of values, it's apparent that it gives users more autonomy by allowing them to configure the location data usage (Apple, 2019) and to protect their privacy by eradicating access to a device's MAC address (Butts, 2017). Thus, this case shows that powerful actors such as platform providers can also encourage "ethical practice within their ecosystems" (Shilton & Greene, 2019, p. 144) by making use of a carefully considered boundary resource design. Regarding privacy, Shilton and Greene (2016, n.p.) describe this phenomenon as "a 'trickledown privacy' effect in which platform providers exercise strong power over privacy definitions". As platform providers can shape the conceptualisation of values within the ecosystem more generally, similar effects can be realised with other values (Shilton & Greene, 2019).[16] Therefore, if VSD is used in boundary resource design, it enables the *value sensitive shaping of ecosystems.*

[14] This issue only comes into play where design decisions or other actions by platform providers are in conflict with (the operationalisation of) a value that VSD practitioners aim to account for. Applying VSD to account for other values is still possible for developers of peripheral applications.

[15] For a current example, observe the current dispute between Apple and the Coalition for App Fairness (Gartenberg, 2020).

[16] When using VSD in the design of individual technical artefacts, platform providers might have to deal with value conflicts during attempts to engage in the value-sensitive shaping of an ecosystem. These conflicts may arise between two or more human values or between a human value—such as privacy—and instrumental values—such as cost-efficiency or usability.

While the means by which the platform providers exert power in the discussed examples are primarily technical on the surface, they also affect developers of peripheral applications economically. For instance, as Ausloos and Veale (2020, p. 138) note, platform providers can utilise a restrictive API design to "break an entire set of business models" that rely on specific data streams through the respective APIs (see also Bucher, 2013; Leerssen et al., 2019). Thus, platform providers can use technical means such as API design to exert economic pressure on other actors within the respective ecosystem by affecting the economic viability and potential profitability of business models behind peripheral applications. Such strategic exploitation of the API design as a tool "to exclude certain business or functionality from integration" (Ausloos & Veale, 2020, p. 138) can establish economic constraints on the scope for design of VSD practitioners at the periphery of ecosystems.

In more decentralised ecosystems, the challenge of accounting for power manifests differently. Here, the negotiation processes among the involved actors on how to account for human values can lead to gridlock. This is because various actors with divergent incentives and interests may disagree as to how human values are conceptualised, weighed, or operationalised. Applying VSD in such cases could ensure that various stakeholder groups are represented in decision-making processes and balance the interests of different stakeholder groups without calling into question the ecosystem's decentralised nature. However, in more decentralised ecosystems, VSD practitioners need to ensure that actors who are not directly involved in design decisions, but affected by them, are also taken into account.

These differences in ecosystems suggest that if there is freedom of choice, the selection of the ecosystem that VSD practitioners embed an artefact in has a significant effect on how human values can be accounted for in the artefact's design. For instance, Atzori and Ulieru (2017) argue that research on platformisation, i.e., "the penetration of the infrastructures, economic processes, and governmental frameworks of platforms in different economic sectors and spheres of life" (Poell et al., 2019, pp. 5–6) is indicating that "the concept of distributive justice / distributive efficiency [is] strongly dependent on platform architectural design and they are unlikely to be achieved in centralized, two-sided markets" (Atzori & Ulieru, 2017, pp. 4–5). However, due to the quasi-monopolistic position of many platforms (Eaton et al., 2015), such a choice does not always exist for developers of peripheral applications if they want to attract a larger user group. Furthermore, that developers of peripheral applications need to consider not only a platform's current features, but also the platform provider's means (technical, economic, or other) to exert power in the future, further complicates the selection process.

Moreover, as the means of different actors to exercise power concern various phases of the design process and can come into play even after deployment, VSD practitioners have to consider the matter continuously: from early conceptualisations of values to the process of operationalising and implementing values to the deployment of artefacts and the evaluation of the design decisions related to values later on. More specifically, since both the development of core components of an ecosystem and peripheral applications often continue after deployment in the form of a constant redesign (Eaton et al., 2015), VSD similarly has to incorporate continuous monitoring of the respective ecosystem's modifications, updates, developments and related effects on the distribution of power within the ecosystem. While the foundational texts of VSD in principal already set out the approach as extending over all of these phases (Friedman et al., 2008; Friedman & Hendry, 2019), in practice, most practitioners do not perform several iterations of the three phases over the entire length of the design process (Winkler & Spiekermann, 2018). Therefore, it is essential to stress the importance of a continuous application of VSD once more.

Furthermore, the findings of this paper suggest that the spectrum of tasks involved in VSD expands if applied in the design of artefacts embedded in vast and complex socio-technical ecosystems. Some tasks, such as monitoring the distribution of power in the ecosystem over extended periods of time or dealing with platform monopolies, appear to be too extensive to be addressed by individual VSD practitioners or even small development teams. Therefore, the range of tasks needs to be distributed over more actors if they are to remain manageable. Regulatory authorities, in particular, must play a role in addressing some of these challenges. In particular, challenges arising due to 1) (quasi-) monopolistic players, 2) the complexity of continuously monitoring the manifold actor constellations and distribution of power within an ecosystem, and 3) boundary resource design that prevents developers of peripheral applications from accounting for values surpass the capabilities of VSD practitioners and the scope of VSD in a traditional sense.

Dealing with (quasi-) monopolistic actors, especially platform providers, is in the domain of antitrust and competition authorities (Crémer et al., 2019; Kommission Wettbewerbsrecht 4.0, 2019; Monopolkommission, 2015), which therefore play a crucial role in ensuring the applicability of VSD. Furthermore, the European Commission's recent proposal for the Digital Markets Act (European Commission, 2020c) contains several propositions for concrete regulatory measures aiming to curb the quasi-monopolistic standing of many platform providers. Relevant here are, for instance, the proposed requirements for gatekeepers to "allow business partners," such as the providers of peripheral applications in a platform-based ecosystem, "to offer the same products or services to end users through third party online intermediation services at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper"[17] (European Commission, 2020c, art. 5 (b)) or to "provide effective portability of data generated through the activity of a business user or end user […]" (European Commission, 2020c, art. 6 (h)). Thereby, regulation built on the European Commission's proposal for a Digital Markets Act could help to counteract "winner-takes-all dynamics" (Anderson & Mariniello, 2021) that favour the development of (quasi-)monopolies. In turn, such a development would provide more choices to select a suitable platform (or suitable platforms) for developers of peripheral applications and make it a more viable option to integrate this selection process in the application of VSD.

Additionally, establishing oversight institutions like the recently launched AI Observatory of the German Federal Ministry of Labour and Social Affairs (Bundesregierung, 2020) or a competence centre for algorithmic systems, as proposed by the German Data Ethics Commission (Datenethikkommission, 2019), could play a crucial role in the monitoring of platform-based ecosystems. The proposal for the Digital Markets Act outlines further supportive measures. Especially the requirement for gatekeepers "to refrain from preventing or restricting business users from raising issues with any relevant public authority relating to any practice of gatekeepers" (European Commission, 2020c, art. 5 (d)) is crucial here, as it would allow for a closer collaboration of regulatory authorities and developers of peripheral applications. If cooperating closely, oversight institutions and developers of peripheral applications could identify the most problematic practices of platform providers jointly in a bottom-up approach and lay the groundwork for possible future regulation and governance that addresses the most urgent issues for VSD practitioners.

Furthermore, in future regulatory frameworks, regulatory authorities should consider an ecosystem's boundary resource composition when determining. As outlined above, iOS is a closed platform. Apple controls and governs the unique distribution channel and, thus, establishes itself as an obligatory passage point. Developers of peripheral applications need to follow Apple's guidelines closely since there is no alternative distribution channel for applications on iOS devices. This is a conscious decision by Apple which brings the company a wide range of business benefits. Yet, from a regulatory perspective, this decision could also be linked to stricter obligations for Apple since it constrains the scope for design of developers of peripheral applications and predetermines to what degree they can account for human values in design decisions. If platform providers use their power to exert influence over design decisions and limit access to alternative distribution channels for developers of peripheral applications, it seems

[17] Note that the term "gatekeeper" is defined more narrowly by the European Commission than the term "platform provider" that is used in this paper (see European Commission, 2020c)

reasonable to link these activities to a stricter regime of obligations. Suppose platform providers engage in exercising control over how developers of peripheral applications account for human values in the technical design of their applications and shape the ecosystem more proactively. In that case, this *value sensitive shaping* of the ecosystem should be subject to increased scrutiny by regulators. Conversely, if platforms refrain from exercising control over how developers of peripheral applications account for human values in the technical design of their applications, the focus of regulators should shift more to the actors at the ecosystem's periphery.

14.6 Conclusion

Technical design in accordance with human values is increasingly considered a building block for shaping the digital future. VSD is a long-standing and well-established approach for achieving design in accordance with human values. This paper shows that the integration of technical artefacts in increasingly vast and complex socio-technical ecosystems with power distributed over various actors affects the applicability of VSD in multiple ways. Several factors determine how this challenge manifests in practice. This paper identifies 1) the *level of decentralisation* of the ecosystem in question, 2) whether VSD is applied regarding the design of components of an ecosystem's *core* or *periphery*, 3) the *temporality* of the exercise of power, and 4) the *phase of VSD* in which power is exercised in as four of these factors.

Adopting a power-sensitive ecosystem perspective provides some reference points for addressing the challenge of accounting for power. While in some constellations, the application of VSD appears to be less applicable since the scope for design of developers is restricted, other constellations appear to accommodate the approach. On the one hand, these are cases where a multitude of assertive actors engage in decision-making processes regarding specific design choices that result in conflicts or even gridlock. Here, VSD can provide a structured approach that supports resolving these conflicts and balances the interests of different stakeholder groups. VSD also appears to be of particular importance for the design of an ecosystem's core components, such as boundary resources. Here, individual design decisions can shape entire ecosystems in accordance with human values (see Shilton, 2012). For this reason, highly centralised ecosystems are also potentially more attractive to regulatory authorities because important nodes and actors in such ecosystems are more easily identifiable and addressable.

Dealing with (quasi-)monopolistic players, accounting for the complexity of continuously monitoring the complex actor constellations and distribution of power within an ecosystem, and addressing boundary resource design preventing developers of peripheral applications from accounting for values emerge as significant novel challenges when applying VSD in vast and complex socio-technical ecosystems. However, recent proposals for establishing new oversight institutions (*Bundesregierung*, 2020; *Datenethikkommission*, 2019) and new regulatory approaches such as the Digital Markets Act and the Digital Services Act (European Commission, 2020c, 2020b) indicate that regulatory authorities can support VSD practitioners in overcoming these challenges. Furthermore, in the future, close cooperation between oversight institutions and VSD practitioners can reveal problematic practices of powerful actors in socio-technical ecosystems and thereby lay the foundation for further regulatory action.

Lastly, a lesson that can be drawn for further research in the field of VSD is that developing a unified framework for dealing with power imbalances between stakeholders in socio-technical ecosystems does not seem to be an attainable goal because the way that power manifests in different ecosystems varies substantively. Thus, instead of aiming for a unified framework, practitioners need to make calls on adequate procedures on a case-by-case basis. Future research, therefore, should aim at advancing the understanding of the actor constellations in socio-technical ecosystems and the distribution of power within them. In particular, in-depth comparative analyses of various socio-technical ecosystems, the distribution of power among the actors involved in them, and the human values expressed in the design of their boundary resource design could provide valuable and more readily applicable insights for VSD practitioners.

14.7 References

Alsindi, W. Z., & Lotti, L. (2021). Mining. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1551

Alstyne, M., Parker, G., & Choudary, S. P. (2016). Pipelines, platforms, and the new rules of strategy. *Harvard Business Review*, *94*(4), 54–62.

Anderson, J., & Mariniello, M. (2021). Regulating big tech: The Digital Markets Act [Blog post]. *Bruegel*. https://www.bruegel.org/2021/02/regulating-big-tech-the-digital-markets-act/

Antonopoulos, A. (2014). Bitcoin security model: Trust by computation. *O'Reilly Radar*. http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html

Antonopoulos, A. (2017). Mastering Bitcoin: Programming the open Blockchain (2nd ed.). O'Reilly.

Apple. (2019). *Turn Location Services and GPS on or off on your iPhone*. Apple Support. https://support.apple.com/en-us/HT207092

Apple. (2020). App Tracking Transparency: Request user authorization to access app-related data for tracking the user or the device. Apple Developer Documentation. https://developer.apple.com/documentation/apptrackingtransparency

Atzori, M., & Ulieru, M. (2017). Architecting the eSociety on Blockchain: A Provocation to Human Nature. *SSRN Electronic Journal. Advance Online Publication*. https://doi.org/10.2139/ssrn.2999715

Ausloos, J., & Veale, M. (2020). *Researching with Data Rights*.

Baldwin, C., & Woodard, C. J. (2009). The Architecture of Platforms: A Unified View. In A. Gawer (Ed.), *Platforms, Markets and Innovation* (pp. 19–46). Edward Elgar.

Becker, M., & Bodó, B. (2021). Trust in blockchain-based systems. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1555

Binance. (2019, April 15). *Binance Will Delist BCHSV*. Binance Latest News. https://binance.zendesk.com/hc/en-us/articles/360026666152

Bodó, B., Brekke, J. K., & Hoepman, J. -H. (2021). Decentralisation: A multidisciplinary perspective. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1563

Borning, A., Waddell, P., & Förster, R. (2008). Urbansim: Using Simulation to Inform Public Deliberation and Decision-Making. In R. Sharda, S. Voß, H. Chen, L. Brandt, V. Gregg, R. Traunmüller, S. Dawes, E. Hovy, A. Macintosh, & C. A. Larson (Eds.), *Integrated Series In Information Systems. Digital Government* (Vol. 17, pp. 439–464). Springer US. https://doi.org/10.1007/978-0-387-71611-4_22

Botsman, R. (2017). Who can you trust? How technology brought us together and why it might drive us apart (1st ed.). Public Affairs.

Brekke, J. K., & Alsindi, W. Z. (2021). Cryptoeconomics. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1553

Brey, P. (2008). The Technological Construction of Social Power. *Social Epistemology*, *22*(1), 71–95. https://doi.org/10.1080/02691720701773551

Brey, P. (2010). Values in technology and disclosive computer ethics. In L. Floridi (Ed.), *The Cambridge handbook of information and computer ethics* (pp. 41–58). Cambridge Univerity Press. https://doi.org/10.1017/CBO9780511845239.004

Bucher, T. (2013). Objects of intense feeling: The case of the Twitter API. *Computational Culture*, *3*.

Bundesregierung. (2020). *Technologie soll dem Menschen dienen: KI-Observatorium nimmt Arbeit auf* [Press release]. Presse- und Informationsamt der Bundesregierung. https://www.bundesregierung.de/breg-de/aktuelles/ki-oberservatorium-1726794

Butts, J. (2017). Thanks to Misuse, Apps Can't View Mac Addresses on iOS 11. *Mac Observer*. https://www.macobserver.com/news/product-news/apps-cant-view-mac-addresses-on-ios-11/

Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, *32*(1_suppl), 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*, *29*(2), 381–400. https://doi.org/10.1287/isre.2018.0794

Crémer, J., Montjoye, Y.-A., & Schwitzer, H. (2019). *Competition Policy for the Digital Era* (Report KD-04-19-345-EN-N). Publications Office of the European Union. http://doi.org/10.2763/407537

Czeskis, A., Dermendjieva, I., Yapit, H., Borning, A., Friedman, B., Gill, B., & Kohno, T. (2010). Parenting from the pocket. In L. F. Cranor (Ed.), *Proceedings of the Sixth Symposium on Usable Privacy and Security—SOUPS '10* (p. 1). https://doi.org/10.1145/1837110.1837130

Datenethikkommission. (2019). *Gutachten der Datenethikkommission* [Report]. Bundesministerium des Innern, für Bau und Heimat. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf

De Filippi, P. (2017). In Blockchain we Trust: Vertrauenslose Technologie für eine vertrauenslose Gesellschaft. In Rudolf-Augstein-Stiftung (Ed.), *Reclaim Autonomy: Selbstermächtigung in der digitalen Weltordnung* (edition suhrkamp, Vol. 2714, pp. 53–81).

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*. https://doi.org/10.1016/j.techsoc.2020.101284

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

DuPont, Q. (2018). Experiments in Algorithmic Governance: A history and ethnography of 'The DAO,' a failed Decentralized Autonomous Organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains and global governance*. Routledge. https://doi.org/10.4324/9781315211909-8

DuPont, Q. (2019). *Cryptocurrencies and blockchains*. John Wiley & Sons.

DuPont, Q., & Maurer, B. (2015, June 23). Ledgers and Law in the Blockchain. *Kings Review*. https://www.kingsreview.co.uk/essays/ledgers-and-law-in-the-blockchain

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System. *MIS Quarterly*, *39*(1), 217–243. https://doi.org/10.25300/MISQ/2015/39.1.10

European Commission. (2019). *Building Trust in Human-Centric Artificial Intelligence*. https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence

European Commission. (2020). *On Artificial Intelligence—A European approach to excellence and trust* (White Paper COM(2020) 65 final). https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive, COM(2020) 825 final (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en

Feiler, P., Sullivan, K., Wallnau, K., Gabriel, R., Goodenough, J., Linger, R., Longstaff, T., Kazman, R., Klein, M., Northrop, L., & Schmidt, D. (2006). *Ultra-Large-Scale Systems: The Software Challenge of the Future*. Software Engineering Institute, Carnegie Mellon University.

Friedman, B., & Hendry, D. G. (2019). Value Sensitive Design: Shaping Technology with Moral Imagination. MIT Press.

Friedman, B., Hendry, D. G., & Borning, A. (2017). A Survey of Value Sensitive Design Methods. *Foundations and Trends® in Human–Computer Interaction*, *11*(2), 63–125. https://doi.org/10.1561/1100000015

Friedman, B., Kahn, P. H., & Borning, A. (2008). Value Sensitive Design and Information Systems. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 69–101). John Wiley & Sons, Inc. https://doi.org/10.1002/9780470281819.ch4

Friedman, B., Kahn, P., Hagman, J., Severson, R., & Gill, B. (2006). The Watcher and the Watched: Social Judgments About Privacy in a Public Place. *Human-Computer Interaction*, *21*(2), 235–272. https://doi.org/10.1207/s15327051hci2102_3

Gartenberg, C. (2020, September 24). Spotify, Epic, Tile, Match, and more are rallying developers against Apple's App Store policies: As the 'Coalition for App Fairness'. *The Verge*. https://www.theverge.com/2020/9/24/21453745/spotify-epic-tile-match-coalition-for-app-fairness-apple-app-store-policies-protest

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: The boundary resources model. *Information Systems Journal*, *23*(2), 173–192. https://doi.org/10.1111/j.1365-2575.2012.00406.x

Giungato, P., Rana, R., Tarabella, A., & Tricase, C. (2017). Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability*, *9*(12), 2214. https://doi.org/10.3390/su9122214

Greene, D., & Shilton, K. (2018). Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development. *New Media & Society*, *20*(4), 1640–1657. https://doi.org/10.1177/1461444817702397

Haugaard, M. (2010). Power: A 'family resemblance' concept. *European Journal of Cultural Studies*, *13*(4), 419–438. https://doi.org/10.1177/1367549410377152

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Hestres, L. (2013). App neutrality: Apple's app store and freedom of expression online. *International Journal of Communication*, *7*, 1265–1280. https://ijoc.org/index.php/ijoc/article/view/1904

High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI* [Report]. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Introna, L. D. (2005). Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems. *Ethics and Information Technology*, *7*(2), 75–86. https://doi.org/10.1007/s10676-005-4583-2

Jacobs, M. (2020). How Implicit Assumptions on the Nature of Trust Shape the Understanding of the Blockchain Technology. *Philosophy & Technology*. https://doi.org/10.1007/s13347-020-00410-x

Karhu, K., Gustafsson, R., & Lyytinen, K. (2018). Exploiting and defending open digital platforms with boundary resources: Android's five platform forks. *Information Systems Research : ISR : An Information Systems Journal of the Institute for Operations Research and the Management Sciences*, *29*(2), 479–497.

Kommission Wettbewerbsrecht. (2019). *A New Competition Framework for the Digital Economy: Report by the Commission 'Competition Law 4.0'* [Report]. https://www.bmwi.de/Redaktion/EN/Downloads/a/a-new-competition-framework.pdf?__blob=publicationFile&v=2

KRAKENFX. (2019). Kraken is Delisting BSV [Blog post]. *Kraken*. https://blog.kraken.com/post/2274/kraken-is-delisting-bsv/

Law, J., & Callon, M. (1992). The Life and Death of an Aircraft: A Network Analysis of Technical Change. In W. E. Bijker & J. Law (Eds.), *Inside technology. Shaping technology/building society: Studies in sociotechnical change* (pp. 21–52). MIT Press.

Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., & Vreese, C. H. (2019). Platform Ad Archives: Promises and Pitfalls. *Internet Policy Review*, *8*(4), 1–21. https://doi.org/10.14763/2019.4.1421

Leswing, K. (2021). *Apple exec warns it may remove apps that track users without permission*. https://www.cnbc.com/2020/12/08/apple-may-remove-apps-that-track-users-without-permission-in-2021.html

Lusch, R. F., & Nambisan, S. (2015). Service Innovation: A Service-Dominant Logic Perspective. *MIS Quarterly*, *39*(1), 155–175. https://doi.org/10.25300/MISQ/2015/39.1.07

McConahy, A., Eisenbraun, B., Howison, J., Herbsleb, J. D., & Sliz, P. (2012). *Techniques for monitoring runtime architectures of socio-technical ecosystems*. Workshop on Data-Intensive Collaboration in Science and Engineering (CSCW 2012).

Monopolkommission. (2015). Competition policy: The challenge of digital markets. Special Report by the Monopolies Commission pursuant to section 44(1)(4) of the Act Against Restraints on Competition (Special Report No. 68). Monopolies Commission. https://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf

Morabito, V. (2017). *Business Innovation Through Blockchain: The B3 Perspective*. Springer International Publishing. https://doi.org/10.1007/978-3-319-48478-5

Mueller, M., & Heger, O. (2018). Health at any Cost? Investigating Ethical Dimensions and Potential Conflicts of an Ambulatory Therapeutic Assistance System through Value Sensitive Design. 39th International Conference on Information Systems (ICIS). https://aisel.aisnet.org/icis2018/healthcare/Presentations/17/

Nathan, L. P. (2012). Sustainable information practice: An ethnographic investigation. *Journal of the American Society for Information Science and Technology*, *63*(11), 2254–2268. https://doi.org/10.1002/asi.22726

Nathan, L. P., Klasnja, P. V., & Friedman, B. (2007). Value scenarios: A technique for envisioning systemic effects of new technologies. *CHI '07 Extended Abstracts on Human Factors in Computing Systems*, 2585–2590. https://doi.org/10.1145/1240866.1241046

Orcutt, M. (2018). *Chain Letter #102: You can go your own way*. https://mailchi.mp/technologyreview/chain-letter-767541?e=93dc606e34&utm_campaign=chain_letter.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=71892724&_hsenc=p2ANqtz--2S3Tqvwcm1BQc_Eb-ArlTKDA-f9cAdBdc6Lxq67nmBy3Y2Z48OyMOEMW__mczpT4YRw2w-7sUtAvryWgLnYMUo_VkOxYs6DqYzXyno1pRK7AGncM&_hsmi=71892724

Orcutt, M. (2019). Chain Letter #139: On social media-fueled coin delistings [Blog post]. *Cryptocurrency News Now!* https://cryptocurrency-news-now.blogspot.com/2019/04/139-on-social-media-fueled-coin.html

Perez, S. (2020). Coalition for App Fairness, a group fighting for app store reforms, adds 20 new partners. *TechCrunch*. https://techcrunch.com/2020/10/21/coalition-for-app-fairness-a-group-fighting-for-app-store-reforms-adds-20-new-partners/

Poell, T., Nieborg, D., & van Dijck, J. (2019). Platformisation. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1425

Reuver, M. de, Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. *Journal of Information Technology*, *33*(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

Sattarov, F. (2019). Power and technology: A philosophical and ethical analysis. Rowman et Littlefield.

Shilton, K. (2012). Values Levers. *Science, Technology, & Human Values*, *38*(3), 374–397. https://doi.org/10.1177/0162243912436985

Shilton, K., & Greene, D. (2016, March 15). *Because privacy: Defining and legitimating privacy in ios development*. iConference 2016. https://doi.org/10.9776/16229

Shilton, K., & Greene, D. (2019). Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics*, *155*(1), 131–146. https://doi.org/10.1007/s10551-017-3504-8

Simon, J. (2016). Values in Design. In J. Heesen (Ed.), *Handbuch Medien- und Informationsethik* (pp. 357–364). J.B. Metzler.

Simon, J., Wong, P. -H., & Rieder, G. (2020). Algorithmic bias and the Value Sensitive Design approach. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1534

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First edition.). O'Reilly.

Tiwana, A., & Konsynski, B. (2010). Complementarities Between Organizational IT Architecture and Governance Structure. *Information Systems Research*, *21*(2), 288–304. https://doi.org/10.1287/isre.1080.0206

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research Commentary—Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics. *Information Systems Research*, *21*(4), 675–687. https://doi.org/10.1287/isre.1100.0323

van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001

van House, N. A. (2004). Science and technology studies and information studies. *Annual Review of Information Science and Technology*, *38*, 3–86. https://doi.org/10.1002/aris.1440380102

Waddell, P., Wang, L., & Liu, X. (2008). UrbanSim: An evolving planning support system for evolving communities. In R. K. Brail (Ed.), *Planning Support Systems for Cities and Regions* (pp. 103–138). Lincoln Institute for Land Policy.

Walch, A. (2019). In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), *Regulating Blockchain: Techno-Social and Legal Challenges* (pp. 58–82). Oxford University Press. https://doi.org/10.1093/oso/9780198842187.003.0004

Walton, R., & DeRenzi, B. (2009). Value-Sensitive Design and Health Care in Africa. *IEEE Transactions on Professional Communication*, *52*(4), 346–358. https://doi.org/10.1109/TPC.2009.2034075

Warnier, M., Dechesne, F., & Brazier, F. (2015). Design for the Value of Privacy. In J. Hoven, V. P. E., & I. van de Poel (Eds.), *Handbook of ethics, values, and technological design: Sources, theory, values and application domains* (pp. 431–445). Springer. https://doi.org/10.1007/978-94-007-6970-0_17

Weber, M. (2019). *Economy and Society: A New Translation*. Harvard University Press.

Werbach, K. (2018). The Blockchain and the New Architecture of Trust. MIT Press.

Winkler, T., & Spiekermann, S. (2018). Twenty years of value sensitive design: A review of methodological practices in VSD projects. *Ethics and Information Technology*, *18*(4), 185. https://doi.org/10.1007/s10676-018-9476-2

Wright, A., & De Filippi, P. (2015). *Decentralized blockchain technology and the rise of lex cryptographia*. https://doi.org/10.2139/ssrn.2580664

Yoo, D., Derthick, K., Ghassemian, S., Hakizimana, J., Gill, B., & Friedman, B. (2016). Multi-lifespan Design Thinking. In J. Kaye, A. Druin, C. Lampe, D. Morris, & J. P. Hourcade (Eds.), *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 4423–4434). https://doi.org/10.1145/2858036.2858366

15 Article No. 7 (Burmeister et al. 2021)

Burmeister, F., Kurtz, C., Vogel, P., Drews, P., and Schirmer, I. Unraveling Privacy Concerns in Complex Data Ecosystems with Architectural Thinking. Proceedings of the 42nd International Conference on Information Systems (ICIS), Austin (USA), 2021.

Abstract

Privacy violations increasingly result from personal-data processing by a convoluted set of actors that collaborate in complex data ecosystems. These data ecosystems comprise numerous socio-technical elements and relations, and their opacity often obscures the manifold reasons for privacy violations. Therefore, researchers and practitioners call for systematic approaches that allow for decomposing data ecosystems in order to receive transparency about the opaque data flows and processing mechanisms across actors. This paper positions architectural thinking as a reasonable means for this need. By collecting key privacy concerns of business and regulatory stakeholders and developing a corresponding data ecosystem architecture meta-model, we provide first steps for extending the scope of architectural thinking to the privacy context. Our results are based on a mixed methods approach, which triangulates data received from a multiple case study of privacy scandals and from 14 expert interviews.

15.1 Introduction

With the increasing need to transform data into economic value, businesses today collaborate in complex data ecosystems where they acquire, share, process, and consume data via interwoven information systems (IS) (Oliveira et al. 2019). In data ecosystems, businesses trade data like a commodity to co-create value, whether businesses jointly provide data-driven services or a single business offers a platform where actors can buy and sell data (Attard et al. 2016). Although data handled in data ecosystems may stem from sensors or machines, an ever-increasing portion is personal data created by individuals through the usage of smart devices, social media, or mobile apps, raising serious privacy concerns businesses must consider (Gopal et al. 2018). Moreover, the deluge of personal data and related allure of monetization through instruments like personalized advertising are accompanied by extensive privacy violations (e.g., Facebook and Cambridge Analytica) and intensified privacy regulations (e.g., General Data Protection Regulation (GDPR)). In fact, from July 2018 to August 2021, the GDPR imposed fines totaling 1.1 billion euros (GDPR Tracker 2021).

The need to balance benefits of personal-data processing against privacy risks requires businesses to remain transparent about intra-organizational data flows and processing activities. Moreover, the dependence on collaboration in increasingly complex data ecosystems challenges businesses in keeping track of interfaces with partners and individuals (Tene and Polonetsky 2013; Crain 2018). Similarly, legal experts such as data protection officers (DPO), legislators, or privacy lawyers (hereinafter termed regulatory stakeholders) need more detailed insights into data ecosystems to more efficiently assess privacy violations or align privacy statements and regulations if necessary (Conger et al. 2013; Kurtz et al. 2018). Therefore, privacy and IS researchers call for novel approaches that help to unravel the manifold socio-technical relations constituting data ecosystems and thereby foster the anticipation, prevention, and analysis of privacy violations (Crain 2018; Nissenbaum 2019; Oliveira et al. 2019). Scholars also criticize that privacy-related IS research often focuses on studying the behavior of individuals, but lacks a design science orientation to deliver IS artifacts that help to address the challenges “practitioners or policymakers truly experience in reality” (Bélanger and Xu 2015, p. 577). Therefore, IS researchers should “move beyond the existing theoretical frameworks, levels of analysis and traditional approaches to information privacy research” (Bélanger and Xu 2015, p. 575).

Against this background, this study draws on the paradigm of architectural thinking (AT) (Winter 2014) to help business and regulatory stakeholders cope with the growing complexity of data ecosystems in privacy-related tasks and decision-making. For business stakeholders (e.g., CEOs, app developers), these tasks and decisions may refer to personal-data sharing or third-party service integration. For regulatory stakeholders, they may refer to the assessment of privacy violations or the analysis of privacy compliance. We argue that the intertwinement of organizations in data ecosystems, comprising interlaced privacy statements, opaque data flows between actors, and mixed information technology (IT) landscapes processing personal data, calls for AT that encourages stakeholders to "think and act architecturally" (Winter 2014, p. 362) to manage privacy concerns in increasingly nontransparent data ecosystems. So far, AT has been discussed in the intra-organizational context and is defined as "the way of thinking and acting throughout an organization that considers holistic, long-term system aspects as well as fundamental system design and evolution principles in everyday decision making, which is not restricted to architects" (Aier et al. 2015, p. 390). Since AT should enable stakeholders to systematically analyze and decompose socio-technical relations, Winter (2014) and Sandkuhl et al. (2018) suggest that an approach for leveraging AT is to build up modeling competences. Such modeling competences typically require a holistic meta-model that fosters a common language among stakeholders and indicates "what to model" by covering key elements and relations (Frank 2014). Therefore, as a first step to extend the scope of AT to data ecosystems and the privacy context alike, this study aims to develop a data ecosystem architecture meta-model that supports business and regulatory stakeholders in handling privacy concerns from an organizational perspective. Our research questions are as follows:

RQ1: *What are key concerns of business and regulatory stakeholders about privacy in data ecosystems?*

RQ2: *Which elements and relations should be integrated in a data ecosystem architecture meta-model to address the identified concerns and thereby leverage architectural thinking in the privacy context?*

Recently, modeling ecosystems was highlighted as a viable lens of analysis for the privacy field (Kurtz et al. 2018; Elrick 2021). However, existing ecosystem meta-models (Oliveira et al. 2018; Burmeister et al. 2019a) do not focus on privacy concerns and the underlying socio-technical relations for personal-data exchange. Moreover, there is a great lack of research clarifying how scholars and practitioners can apply the ecosystem perspective to cope with increasingly complex privacy concerns. We contribute to these research gaps by extending the scope of AT through a data ecosystem architecture meta-model as well as positioning AT as a reasonable approach for the privacy field. Our work also complements existing theories, such as the theory of contextual integrity (Nissenbaum 2011), and privacy models (Conger et al. 2013; Benson et al. 2015), which are limited to the classification of actors and their dyadic relationships. Following the stakeholder-oriented meta-modeling approach (Lagerström et al. 2009), we start with identifying key concerns (Niemi 2007), which in our context are privacy-related information needs of business and regulatory stakeholders. For this purpose, we triangulate qualitative data received from a multiple case study (Yin 2009) and from 14 expert interviews (Myers and Newman 2007). Based on the concerns, we develop meta-model fragments and integrate them into one coherent meta-model.

The remainder of this paper is structured as follows. In the next section, we review related research. Then, we clarify our methodology. Subsequently, we present the key concerns and demonstrate our meta-model. Finally, we discuss our results and draw a conclusion.

15.2 Related Research

15.2.1 Personal Data, Data Ecosystems, and Privacy

According to the GDPR (2016), personal data are "any information relating to an identified or identifiable natural person ('data subject')" (Art. 4 (1)). Personal data exist in various types (e.g., contact, health, location data) and are processed by organizations for manifold purposes, such as profiling users, analyzing customer behavior, enabling personalized service experiences, or complying with legal requirements (Acquisti et al. 2016; Purtova 2018). Moreover, organizations monetize personal data through direct sales to third parties, such as advertisers or data brokers (Gopal et al. 2018; Myers West 2019). Conversely, organizations acquire personal data to deepen their customer knowledge or even de-anonymize individuals (Crain 2018).

The manifold ways in which personal data are processed and shared clarify the shift away from the dyadic relationship between individuals and service providers toward data ecosystems that involve various actors co-creating value from personal data. Originated in the concept of business ecosystems (Moore 1996; Iansiti and Levien 2004), data ecosystems are defined as "a loose set of interacting actors that directly or indirectly consume, produce, or provide data and other related resources (e.g., software, services, and infrastructure). Each actor performs one or more roles and is connected to other actors through relationships, in such a way that actors by collaborating and competing with each other promote data ecosystems" (Oliveira et al. 2019, p. 604). According to Gelhaar et al. (2021), the focus of data ecosystems is on "the cross-actor generation, processing, and use of data with the goal to create added value for all actors involved" (p. 6114). Research on data ecosystems is scarce and mainly discusses their economic purposes, such as the enabling of open data communities, especially in the public sector, or supporting data-driven business models (Zuiderwijk et al. 2014; Attard et al. 2016; Shah et al. 2020). Latest research created a morphology (Azkan et al. 2020) and a taxonomy (Gelhaar et al. 2021) that allow characterizing data ecosystems in different settings. However, there is a great lack of research on embedding the data ecosystem concept in the privacy context (Tene and Polonetsky 2013; Elrick 2021). Moreover, in their literature analysis, Oliveira et al. (2019) conclude that research on data ecosystems must evolve in theory, modeling, and engineering, as many papers focus on selected components (e.g., Hadoop as an analytics tool) and only reflect a small part of the research field.

Data ecosystems enhance the opportunity to co-create value but also increase the risk of privacy violations, as various actors may gain access to personal data. Privacy is defined as "the ability of individuals to control the terms under which their personal information is acquired and used" (Culnan and Bies 2003, p. 326). Informed consent, as the predominant legal basis that organizations rely on when processing personal data (GDPR 2016, Art. 6), implies that individuals have transparency about all relevant details of data processing, including third-party recipients and their purposes, when deciding what personal data can be collected, shared, analyzed, or otherwise processed. However, the assumption of creating transparency via privacy statements is doubtful, as information about third parties is often hidden in unclear statements (Cate and Mayer-Schönberger 2013; Gopal et al. 2018). Only a few privacy models address this issue by generalizing what kinds of actors may gain access to personal data (Conger et al. 2013; Benson et al. 2015). Moreover, there is a lack of research specifying the socio-technical relations between these actors that ultimately lead to privacy violations (Ananny and Crawford 2018; Kurtz et al. 2018). Privacy violations result in adverse consequences for individuals and comprise social, physical, psychological, prosecution-, career-, resource-, or freedom-related consequences (Karwatzki et al. 2017). For example, social consequences negatively affect relationships and freedom-related consequences manipulate personal behavior and opinion. According to Nissenbaum's (2011) theory of contextual integrity, privacy is violated when data flows are not appropriate. Appropriateness is given when a data flow conforms with contextual information norms, which refer to five parameters: data subject, sender, recipient, data type, and transmission principle. The latter determines the constraints under which data flow, such as "consent is given" or "required by law" (Nissenbaum 2019).

15.2.2 Architectural Thinking and Meta-Model Extensions

Architecture is defined as "the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution" (ISO 2011, p. 2). To capture the enterprise architecture (EA), where the "system" represents an organization, research and frameworks from practice suggest relying on EA meta-models that structure the elements of EA along logical layers. For example, the meta-model of the EA framework TOGAF proposes four layers with related elements: business (e.g., goals, processes), data (e.g., data entities), application (e.g., IS services), and technology (e.g., physical components) (The Open Group 2018). In general, a meta-model is "the description of the set of notations and concepts used to define a model" (ISO 2002, p. 4). EA meta-models provide a template to derive as-is and to-be EA models that address stakeholder concerns, which are "interests related to the development of EA, its use and any other aspects that are important to one or more stakeholders" (Niemi 2007, p. 2). By using EA models, the EA management (EAM) performs tasks related to strategic planning or improving business IT alignment (Saat et al. 2010).

However, scholars state that EAM cannot develop its full potential, as its influence is often limited to IT departments (Winter 2014; Aier et al. 2015). Therefore, EAM should move forward to AT as a less formalized and utility-centered approach that supports people outside the IT function to analyze, plan, and transform fundamental structures (Winter 2014). Research on AT is scarce and has so far focused on the intra-organizational level. For example, Aier et al. (2015) examine the major determinants, challenges, and adoption mechanisms of AT within an organization in the financial sector.

Because we focus on architectural meta-models, previous work on extending their scope from the privacy-, data-, or ecosystem-oriented perspective is particularly worth mentioning. For example, in the knowledge management field, Fill and Johannsen (2016) suggest aligning enterprise modeling and big data analytics based on meta-modeling. Erraissi and Belangour (2018) suggest meta-models of data source and ingestion layers using Hadoop. Whereas the data source layer covers data types (e.g., GPS) and formats (un-, semi-, structured), the ingestion layer reflects the data analytics steps (e.g., compression, filtration). Other authors modeled key components along the big data lifecycle, including analytics tools, cloud services, and access control (Demchenko et al. 2014). To support GDPR compliance, Burmeister et al. (2019b) propose a privacy-driven EA meta-model by adding data processing and security layers to the business and IT layers of EA. These layers include algorithms, de-identification methods, or authentication services. However, modeling socio-technical relations and data exchange between actors is strongly limited by the intra-organizational lens of EA. Hence, Burmeister et al. (2019a) propose a meta-model for digital transformations in business ecosystems, which covers domain (e.g., influences), actor (e.g., actor classes), collaboration (e.g., services), and IT (e.g., interfaces) layers. Feltus et al. (2017) propose a service ecosystem meta-model with elements like ecosystem goals and capabilities to increase the scope of risk governance. Oliveira et al. (2018) provide first steps for a data ecosystem meta-model by suggesting actors, roles, relationships, and resources as main elements of data ecosystems. However, their research does not focus on privacy concerns and personal-data exchange with third parties. Key enablers for the latter, according to the concept of boundary resources, are application programming interfaces (API) and software development kits (SDK) (Eaton et al. 2015).

Summing up, research on both AT and data ecosystems is still in its infancy. In particular, no previous work embeds AT in the inter-organizational privacy context, as in our case through a data ecosystem architecture meta-model that helps business and regulatory stakeholders handle complex privacy concerns. While some research considers privacy from the EA perspective (Burmeister et al. 2019b), existing ecosystem meta-models do not focus on the detailed modeling of privacy-related socio-technical relations between actors.

15.3 Methodology

In our study, we followed the stakeholder-oriented meta-modeling approach according to Lagerström et al. (2009), which draws on stakeholder concerns to create architectural fragments and integrate these into a meta-model. To identify privacy concerns from an organizational perspective and to increase the external validity of our results, we triangulated data received from an explorative multiple case study (Benbasat et al. 1987; Yin 2009) and expert interviews (Myers and Newman 2007). We then demonstrated and evaluated our results through practical application and focus groups. Figure 1 illustrates the steps of our methodology.

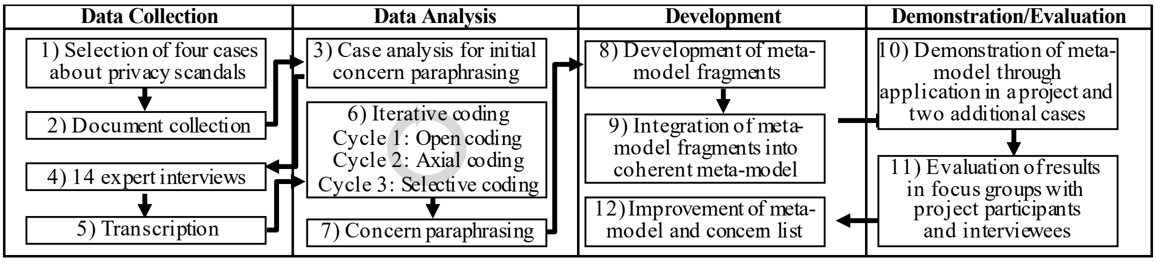

Data Collection
Data Analysis
Development
Demonstration/Evaluation
1) Selection of four cases about privacy scandals
2) Document collection
4) 14 expert interviews
5) Transcription
3) Case analysis for initial concern paraphrasing
6) Iterative coding Cycle 1: Open coding Cycle 2: Axial coding Cycle 3: Selective coding
7) Concern paraphrasing
8) Development of meta-model fragments
9) Integration of meta-model fragments into coherent meta-model
12) Improvement of meta-model and concern list
10) Demonstration of meta-model through application in a project and two additional cases
11) Evaluation of results in focus groups with project participants and interviewees

Figure 1. Methodology

15.3.1 Data Collection

As part of a long-term study where we collected privacy scandals (hereinafter termed cases) in a case study database to research deficits in regulations (e.g., GDPR) and responsible data handling, we started our work by analyzing some of these cases to initially get an overview of privacy-critical, socio-technical relations in data ecosystems. To select meaningful and representative cases, we relied on theoretical replication logic, where cases are predicted to provide contradictory results (Benbasat et al. 1987; Yin 2009). Theoretical replication allowed us to consider cases with heterogeneous characteristics (e.g., different types of actors, varying data types, diverse adverse consequences) and thus to increase the generalizability of our study. Table 1 outlines each case with the number of documents collected and a link to an exemplary news article.

Table 1. Case Overview

No.	Title	Description
1	Facebook and Cambridge Analytica	The developer of the Facebook app This Is Your Digital Life (TIYDL) indicated to collect profile data for research purposes but sold the data to Cambridge Analytica that processed the data to target over 87 million Facebook users with political ads (documents: 35, link: cnet.co/3k5c7ci).
2	Red Shell and gaming software	Device fingerprints collected by the spyware Red Shell, which is integrated in dozens of games such as Civilization VI and The Elder Scrolls Online, are used to measure the

		effectiveness of ads displayed in the web browsers of players (documents: 21, link: bit.ly/355nhcM).
3	Healthcare app Ada	The provider of the healthcare app Ada stated that health data would not be shared with third parties, but a network traffic analysis revealed that data on symptoms and devices had been transmitted to companies like Amplitude or Facebook (documents: 12, link: bit.ly/2zREn0y).
4	Waitlist app OpenTable	The waitlist app OpenTable, used by more than 47,000 restaurants, shares personal data like contact details, location data, and user preferences with other Priceline-owned sister companies, such as Kayak and Booking.com, and with advertisers (documents: 13, link: cnet.co/3eAXr3b).

We selected these four cases as representative examples for our research for several reasons. First, they all describe data ecosystems heavily reliant on personal data while exhibiting very different characteristics, including a wide range of industries (e.g., health sector, gaming industry), diverse practices causing privacy violations (e.g., misuse of defined purposes, technically via spyware), and various actor types and roles (e.g., Facebook as platform provider, restaurants as service providers). Second, they represent data ecosystems of large scale, i.e., they consist of thousands of users and dozens of third parties, which may reveal a great variety of socio-technical relations from an architectural point of view. Third, they were widely discussed in the public media, offering considerable research material that may provide detailed insights into the cases.

For each case, we aggregated data by searching for related news articles on widespread news platforms (The New York Times, Wired UK, BBC, CNet, ZDNet) and extracting the content of these articles. In addition, we enriched the data material per case by performing a backward search via the links in each article, providing us with additional documents from other platforms. Over all cases, we collected 81 documents, comprising 71 news articles, 2 official responses of actors, 5 blog entries, and 3 technical reports. Analyzing this data material gave us a first impression of important socio-technical elements and relations in data ecosystems and allowed us to anticipate related privacy concerns (see section Data Analysis). However, these insights were biased by subjectivity and may not have reflected real stakeholder concerns. To reduce this bias, we performed 14 expert interviews (Myers and Newman 2007) with different kinds of business and regulatory stakeholders (see Table 2). To identify a wide spectrum of concerns, we selected the interviewees based on their role (e.g., advisory, managerial, or technical) and workplace (e.g., public or commercial), while also considering whether they have at least five years of experience, perform daily tasks related to personal data, and work in organizations embedded in data ecosystems (e.g., data-driven businesses, privacy law firms).

We used the data material and concerns from our case study as a discussion basis (e.g., to brainstorm about privacy using the cases) and drew on a semi-structured interview guide with open-ended questions to leave space for particular interests of the respondents. To not only identify concerns but also accentuate the need for AT, the guide included questions about the interviewees' role in data ecosystems, problems and solutions in ensuring privacy compliance, information needs related to personal-data processing, current practices in modeling data ecosystems, and AT as a solution to achieve transparency about data ecosystems. We shared the interview guide and a summary of our research objectives upfront to ensure a common understanding of our study (Myers and Newman 2007). All interviews were conducted, recorded, and transcribed by the same researcher. Subsequently, this and another researcher coded the data material using MAXQDA.

Table 2. Profiles of the Interviewees and Interview Details

No.	Interviewee Role	Industry	Main Topics of Interest/Longest Discussed	Length/Words
B1	Data analyst	Advertising	User profiling, personalization of ads, data acquisition	73 min./6,039
B2	CEO	Software	Distribution via app stores, data-driven business models	57 min./5,382
B3	Enterprise architect	Consumables	Personal data in EA models, support of GDPR compliance	61 min./5,481
B4	Data analyst	Finance	Processing of personal data in lending and online banking	34 min./3,092
B5	App developer	Software	Implementation of SDKs in apps, programming of APIs	72 min./5,756
B6	CIO	Public service	Problems in ensuring IT security, data exchange formats	54 min./4,782
B7	Enterprise architect	Railway	Modeling of interfaces, collaboration with departments	43 min./3,523
B8	App developer	Mobile games	In-app purchases and ads, restrictions through GDPR	39 min./3,184
R1	Privacy lawyer	Public service	Purpose limitation, general deficits of informed consent	69 min./5,531
R2	DPO	Healthcare	Storage of particularly sensitive data, IT security measures	48 min./4,727
R3	Privacy lawyer	Software	Purpose changes through third parties, loopholes in GDPR	52 min./4,823
R4	Privacy lawyer	Insurance	Processing of personal data to calculate insurance terms	43 min./4,241
R5	DPO	Mobile games	Contract design, lack of transparency in privacy statements	28 min./2,755
R6	Legal adviser	Consulting	Barriers to privacy compliance, usefulness of modeling	35 min./3,012

15.3.2 Data Analysis

The aim of the data analysis was to gain a comprehensive understanding of the socio-technical elements and relations constituting data ecosystems and to identify major privacy-related concerns of business and regulatory stakeholders. The two researchers triangulated data by conducting a qualitative content analysis (Mayring 2014) of the data material received from both the case study and the transcriptions. Starting with the case study, the researchers separately reviewed the data material collected for each case and inductively coded socio-technical elements, such as actor types (e.g., “platform provider”, “data broker”), personal-data types (e.g., “health data”, “location data”), or technical components (e.g., “iPhone”, “server”). Relations were open-coded as well (e.g., “shared with third parties”, “contractual agreement”). In addition, a priori codes from the literature (e.g., adverse consequences, boundary resources) deductively guided the analysis. With only a few initial coding differences, the researchers discussed and refined the codes in multiple sessions and paraphrased them to obtain preliminary concerns (Niemi 2007). Although this first analysis was rather subjective, the results gave us an overview of privacy-critical data ecosystems and supported the interviews.

Following Saldaña’s (2015) advice that multiple coding cycles are required to ensure rigorous analysis of qualitative data, the same two researchers subsequently analyzed the transcriptions in three coding cycles. The first coding cycle was inspired by the case analysis, as induction and deduction were combined as well. A coding scheme (Mayring 2014) was set up, which included not only codes from the literature (e.g., “API” and “SDK” as boundary resources) but also the codes previously identified in the case material. While many text passages in the transcriptions could be coded via the scheme, the open coding revealed some codes not encountered yet, such as “purpose change” or “de-anonymization.” In the second coding cycle, axial coding was performed to group the codes into broader, theme-focused categories (Saldaña, 2015). This led to 14 categories, such as “collaboration” and “security measures.” For example, the codes “contractual agreement” and “service co-creation” were assigned to the category “collaboration.” In the third coding cycle, selective coding integrated the categories into more meaningful themes. “Selective coding continues axial coding at a higher level of abstraction” (Flick 2009, p. 310). For example, the categories “data acquisition” and “data analysis” were labeled as “data processing.” This resulted in four selective codes, which we call concern areas. Finally, per category of each concern area, the researchers summarized the respondents’ statements assigned to identical codes and paraphrased them as concerns (Niemi 2007). After each coding cycle, inter-coder agreement tests were conducted to reach a consensus by comparing the codes and recoding the data.

15.3.3 Development, Demonstration, and Evaluation

In line with the stakeholder-oriented meta-modeling approach (Lagerström et al. 2009), we created meta-model fragments that cover all the elements and relations mentioned within the concerns. More precisely, for each of the 14 categories, we created a fragment comprising all concerns of that category (see Figure 2). Subsequently, to obtain a coherent meta-model, we combined all fragments by relating them to each other and removing redundancies. Inspired by EA meta-models (e.g., TOGAF), we added layers to our meta-model by comparing and aligning the modeling elements. Referring to the concerns and our data material, we also equipped the elements with attributes to allow more fine-granular modeling. We demonstrated and evaluated the meta-model from the perspectives of both business and regulatory stakeholders. Taking the business perspective, we supported privacy-related design decisions in an app development project through practical application of AT. In multiple focus groups (Bélanger 2012) with project participants, we modeled the data ecosystems relevant to design decisions based on our meta-model and list of concerns. The practical application of AT resulted in some improvements to the meta-model, e.g., we added the attribute "priority" to the element "purpose" and self-referencing to the element "application." From the regulatory perspective, we modeled two additional cases not studied so far by using our meta-model as a template. In a focus group session with three interviewees (R2, R3, and R6), we discussed the case models, the concerns, and the meta-model, which led to further improvements. For example, to reduce the complexity of our meta-model, we removed the "data batch" and "data type" elements and adjusted related concerns, as these elements could be covered through attributes of other elements. Overall, the evaluation partners appreciated the variety of concerns and the layered structure of the meta-model. They perceived AT based on the meta-model as useful for making data ecosystems transparent and suggested to predefine task-specific models as a next step.

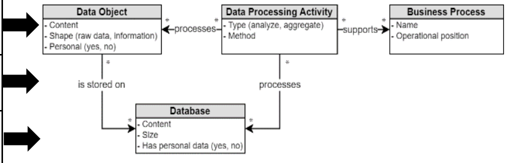
Concern Area	Category	Concerns	Meta-Model Fragment
Data processing	Data analysis	"Which types of data are aggregated within a database?"	 Data Object - Content - Shape (raw data, information) - Personal (yes, no) processes Data Processing Activity - Type (analyze, aggregate) - Method supports Business Process - Name - Operational position is stored on processes Database - Content - Size - Has personal data (yes, no) *
		"Which methods does an actor use to analyze personal data?"	
		"Which business processes profit from data processing activities?"	

Figure 2. Meta-Model Fragment Derived from Exemplary Concerns

15.4 Results

Our results provide first steps for leveraging AT in the privacy context and extending the scope of AT to the level of data ecosystems. In the following, we present the stakeholder concerns (RQ1) using examples from the case study and demonstrate the application of AT based on our meta-model (RQ2) as indicated above.

15.4.1 Privacy Concerns of Business and Regulatory Stakeholders

The concern areas revealed by the data analysis include privacy concerns related to (1) actor composition, (2) data processing, (3) technical interfaces, and (4) regulatory compliance in data ecosystems (see Table 3). Each concern area comprises multiple categories obtained via the axial coding.

Actor Composition

Addressing privacy concerns from an architectural perspective can support several scenarios. This may be the planning of an organization's data-driven transformation, the integration of external data sources into an analytics process, or the assessment of a privacy violation. Thus, stakeholders performing AT must define the boundaries of the data ecosystem they are observing or planning to change. In the first place, this can be done by identifying the actors relevant to a given scenario (C1), such as a specific organization or a group of organizations or individuals. Capturing the role of actors (C2) is essential to recognize their viewpoint and legal obligations. A respondent stated: "*The GDPR divides companies into data controllers and data processors. This provides a basis for legal assessment. However, sometimes companies are both. For example, we use cookies from Google Analytics to measure our website traffic. They only process the data for us, so we are the data controller. If we sold the data to Google, we both would be the controller and they would still be the processor for us. It strongly depends on the situation*" (B2). Estimating the extent to which an actor's business model depends on personal data (C3) supports the identification of an actor's role and provides evidence for other concerns. Our case study shows that privacy violations not only occur in the dyadic relationship between an individual and a service provider but also often result from data sharing and processing practices by a chain of actors. Hence, understanding data ecosystems requires insights not only into intra-organizational data processing but also into the collaboration of actors. This can be seen most clearly in the contractual relationships (C5), which are influenced by the legal framework applicable in the countries where the actors are incorporated (C4). From the perspective of regulatory stakeholders, access to contracts (GDPR 2016, Art. 58 (1)) is important to obtain information about the provided services (C6) and intended activities of users (C7). However, a privacy lawyer added: *"Contracts are certainly a good source of information on how data sharing transactions are carried out. Unfortunately, privacy scandals are often caused by cooperation with hidden third parties. For a legal assessment of such scandals, it is necessary to read between the lines and gather much more information to understand the whole context of a data processing act"* (R3). According to the interviewees, capturing the distribution channels provided by an actor can be a good starting point to retrace privacy violations (C8). The interviewees also emphasized the need to reconstruct how platforms are embedded in a data ecosystem (C9), as these often trigger the collaboration between actors. Case 4 clarifies the relevance of this concern area. The waitlist app OpenTable collects diverse personal data of users, including restaurant preferences, contact data, and location data. OpenTable shares these data with a vast amount of actors not limited to restaurants and their affiliates but including business partners such as Kayak and Booking.com as well as advertisers and social networks.

Table 3. Privacy Concerns of Business and Regulatory Stakeholders

Concern Area	Category	No.	Stakeholder Concern	Source	
				B	R
Actor composition	Actors	C1	Which actors are interacting in a focal data ecosystem?	All	All
		C2	Which roles do specific actors in the data ecosystem have?	All	All
		C3	Whose business model is heavily reliant on personal data?	1-3,5,8	2,5
		C4	In which country does an actor have its legal seat?	2,5	All
	Collaboration	C5	How are actors contractually interconnected?	All	All
		C6	Which services are co-created by which actors?	1-3,5-7	1,2,4
		C7	To what extent do services deviate from users' intended actions?		3,5
		C8	How do actors distribute applications and services?	2,4,5,8	1,4,5
		C9	To what extent are platforms involved in the data ecosystem?	1-5,8	1,3-6
Data processing	Data types	C10	Which types of personal data are processed by which actors?	All	All
		C11	Which information can be inferred from selected data types?	1,4	2,4
	Data acquisition	C12	Which kind of personal data does a specific actor collect?	All	All
		C13	From what data sources does an actor acquire personal data?	All	All
		C14	Where does an actor store personal data?	All	All
	Data analysis	C15	Which types of data are aggregated within a database?	1,3-5	2,4,6
		C16	Which methods does an actor use to analyze personal data?	1,4,6	2-5
		C17	Which business processes profit from data processing activities?	1-3,6-8	3,6
	Data sharing	C18	With whom does an actor share which type of personal data?	All	All
		C19	How often does data sharing between two actors take place?	1,2,4,7	1-3,5
		C20	Has consent been given for a specific form of data sharing?	1,4,5,8	All
IT landscape	Applications	C21	Which analytics tools trigger which data processing activities?	1,3,4,7	1,2,4,5
		C22	Which privacy settings are included in provided applications?	2,5,8	3-5
	Devices	C23	Which devices are involved in a data processing activity?	1-3,6	2,5
		C24	To whom are which data transmitted from individuals' devices?		4
	Technical interfaces	C25	Which technical interfaces does a data processing activity use?	4,3,6	
		C26	Which infrastructure components communicate via which API?	5	
		C27	Which SDKs are integrated in which applications?	5,8	
Regulatory compliance	Legal framework	C28	Which privacy regulations apply to the data ecosystem?	2-4,8	1,2,4,6
		C29	Who is responsible for enforcing which regulation?	2	1,2,6
	Purpose limitation	C30	Which purpose does a selected data processing activity have?	All	All
		C31	Which data processing activities deviate from defined purposes?	1,3,4	All
		C32	To what extent do third parties infringe original purposes?	1	1,3
	Security measures	C33	How does an actor ensure that personal data are anonymized?	1,3-6	All
		C34	How does an actor ensure that personal data are stored securely?	2,3,5,6	2,3
		C35	Is a specific actor capable of de-anonymizing personal data?		2,3,6
	Privacy statements	C36	Is a data processing activity not defined in a privacy statement?		All
		C37	Are all purposes of data processing listed in a privacy statement?	1,4	All
		C38	Which third parties are not listed in a privacy statement?	1,4,5,7	1,3-5
	Ethical values	C39	To what extent do processing activities contradict ethical values?	1	3,4,6
		C40	What are the adverse consequences of a data ecosystem?	8	5,6

Data Processing

Data processing today is no longer a merely intra-organizational matter but rather takes place between actors collaborating in data ecosystems, as analytics processes are increasingly outsourced and data have become a commodity. AT provides transparency about data ecosystems by enabling a decomposition of the underlying socio-technical relations. The interviewees mentioned multiple concerns that provide a basis for this task. Recognizing what types of personal data are processed and shared in a data ecosystem (C10) helps to anticipate privacy violations and what kind of information may be inferred and disclosed (C11). To legally assess the behavior of a specific actor, it is essential to know what personal data that actor collects (C12) and from which data sources (C13). A data protection officer stated: *"In my opinion, modeling data types is essential to enable a comparison of data sharing networks. If a certain actor buys different data types from different actors, it may be possible to identify a black sheep that seeks to de-anonymize personal data"* (R2). In this regard, it is necessary to retrace with whom actors share personal data (C18), how often this data sharing takes place (C19), and, most importantly, if consent of individuals is obtained (C20). Some respondents also mentioned concerns related to the extent to which data are aggregated (C15), the methods an actor uses to analyze personal data (C16), and the location where personal data are stored (C14), which may determine the legal framework to be applied. However, addressing the latter concerns requires deep knowledge of organizations that may not be easily accessible to regulatory stakeholders. The interviewees also emphasized that business processes enhanced through data analytics should be captured (C17), as this clarifies purposes of data processing and supports creating the record of processing activities (GDPR 2016, Art. 30). An enterprise architect acknowledged: "*We here in the EA department often help out when it comes to updating the record of processing activities. However, with all the data exchange with partners that the departments initiate on the fly, we increasingly lose track of which processes actually collect, share, or analyze personal data. We have to broaden our scope and consider partners and external data sources. The internal EA mindset is no longer sufficient today"* (B3). Case 3 exemplifies the relevance of this concern area. The healthcare app Ada shared personal data such as symptoms, names of users' health insurances, and device data with third parties such as Amplitude or Facebook, which also exchange data with numerous other applications. These different data sources lead to the risk of sensitive personal data about an individual being aggregated and de-anonymized using the unique identifiers of devices.

IT Landscape

Decomposing data ecosystems from an architectural perspective requires an in-depth understanding of the IT components on which data processing is based. These can initially be recognized in the software that triggers data processing (C21) and is used by both organizations (e.g., analytics tools) and individuals (e.g., mobile apps). Checking the possible privacy settings of an application (C22) and relating these to frequent data flows captured in architectural models can support evaluating an organization's compliance with privacy by default (GDPR 2016, Art. 32). In addition, the respondents underlined that the modeling of data ecosystems needs to reflect the diversity of the devices involved in data processing activities (23), what personal data are transmitted by these devices and to whom in a specific case (C24), and what interfaces are involved in these data transactions (C25). In this context, a developer stated: *"Many privacy violations result from a misuse of location data or a user's advertising ID transmitted via smartphones. These data are shared with advertisers or other third parties, allowing a form* *of tracking that is often not visible to users. So I would suggest that modeling and relating these devices to other elements is inevitable"* (B5). Regarding this issue, some respondents emphasized that most applications communicate via APIs (C26) and integrate predefined functions of SDKs (C27) offered by platforms such as Facebook. However, these platforms often provide SDKs to access personal data without getting consent. Case 2 clarifies the technical possibilities constituting privacy violations. Diverse gaming software embedded the Red Shell SDK, which creates device fingerprints when users interact with adverts. To create the fingerprints, Red Shell collects data such as a user's IP address, browser version, language, installed fonts, screen resolution, time zone, and in-game ID. When people buy and start a new game, the parameters are matched. With the matching two fingerprints, game developers can identify a user's device and measure the effectiveness of adverts. Moreover, Red Shell keeps the data on its servers for several months to track users.

Regulatory Compliance

To assess organizations' privacy compliance in data ecosystems, it is first necessary to identify the applicable regulations (C28) and the actors responsible for their enforcement (C29). For businesses, this identification is important for recognizing the obligations to be fulfilled, e.g., the GDPR demands special guarantees for data transmissions to actors outside the European Union (2016, Art. 44). According to the respondents, capturing the purpose of data processing activities (C30) in architectural models helps to evaluate whether actors comply with the purpose limitation principle (GDPR 2016, Art. 5 (1)). By relating business processes, services, or data objects to data processing activities, deviant purposes can be revealed (C31). Furthermore, modeling how personal data are shared between actors and processed in manifold ways can illustrate the extent to which defined purposes are not met (C32). A privacy lawyer approved: "*With all the data exchange between companies, it is very difficult to retrace the original purpose. Take, for example, all those fitness apps. A provider anonymizes and shares the data with an analytics firm, which then shares these data with an advertiser and another company and so on. In the meantime, one company even de-anonymizes the data. My point is, without capturing all these data flows and elements, it is quite impossible to exactly understand where privacy violations actually occur"* (R4). Some respondents also emphasized the need to model security measures related to the anonymization (C33) and storage (C34) of personal data, as this can reveal whether actors adequately ensure data protection and privacy by design, as obliged by the GDPR (2016, Art. 32). Moreover, capturing the data an actor collects helps anticipate the risk of de-anonymization of personal data (C35). The participants added that comparing data processing activities (C36) and their purposes (C37) with those listed in a privacy statement can reveal gaps and evidence of non-compliance. This is especially critical when the modeling discloses third parties not listed in a privacy statement (C38). Besides regulatory compliance, ethical values (e.g., social welfare) must be considered in the assessment of privacy violations or actors' behaviors (C39). For example, although the use of personal health data for research purposes may not be part of consent, such data flow is often considered appropriate. In contrast, giving consent can result in adverse consequences that are immoral and not appropriate from an ethical point of view (C40). In case 1, for example, users of the personality quiz app TIYDL disclosed their personal data and the opportunity to access profile data of their friends on Facebook. Facebook gave the developer of TIYDL access to these data for research purposes. However, the developer sold the data to Cambridge Analytica, which processed the data to build personality profiles and support political advertising.

15.4.2 Data Ecosystem Architecture Meta-Model

Integrating the architectural fragments resulted in a coherent meta-model (see Figure 2) comprising five horizontal and three vertical layers that cover elements and relations described in the identified stakeholder concerns. The meta-model is intended to leverage AT in the privacy context by providing a template that illustrates significant socio-technical elements and relations in data ecosystems. Business and regulatory stakeholders can slice (horizontally, vertically, or diagonally) and instantiate the meta-model to obtain architectural models that address selected concerns during privacy-related tasks and decision-making.

As the topmost horizontal layer, the data ecosystem layer includes elements such as regulations (e.g., GDPR) and ethical values that influence a data ecosystem's actors. The actors represent, as clarified in the first concern area, organizations such as platform providers as well as groups of individuals such as app users. Next, the business layer contains business models and processes, collaboration-related elements such as services, and also individuals' activities and adverse consequences resulting from a data ecosystem. The legal layer covers the consents of individuals, contracts and privacy statements between actors, as well as purposes of data processing. Besides data processing activities and data objects that represent the data, the data layer includes elements on which data objects are stored or aggregated. The last layer covers the underlying IT infrastructure comprising software and hardware, interfaces, and security measures.

The vertical layers realize both intra- and inter-organizational perspectives on a data ecosystem. For the intra-organizational perspective, the meta-model distinguishes between the organizations' EA and the individuals' architecture (IA). Whereas the EA focuses on elements relevant to organizational personal-data processing, the IA abstracts involved elements of a group of affected people. For the inter-organizational perspective, the meta-model proposes a boundary architecture (BA), which we define as the intersection of two organizations collaboratively processing or sharing personal data, of individuals and one organization co-creating data-driven services, and of individuals exchanging data with each other. In comparison to the elements of the EA and IA, the elements of the BA are shared, i.e., jointly used by two actors and enabling collaboration. According to our meta-model, an actor has exactly one EA or IA but any number of BAs, i.e., one with each collaboration partner. We argue that the distinction between these architectures is necessary to fully comprehend the complexity of data ecosystems and take into account today's interconnectedness and coalesced IS between organizations and individuals. Although these types of architectures can be used separately to address either intra- or inter-organizational concerns, most of the identified concerns show that AT in the privacy context requires a combination of both perspectives. To highlight the elements and relations that are considered particularly privacy-critical in a given scenario or have been part of a privacy violation, a "critical issue" mark can be attached. In instantiations of the meta-model, when this mark is attached to elements or relations, it is symbolized through a flash.

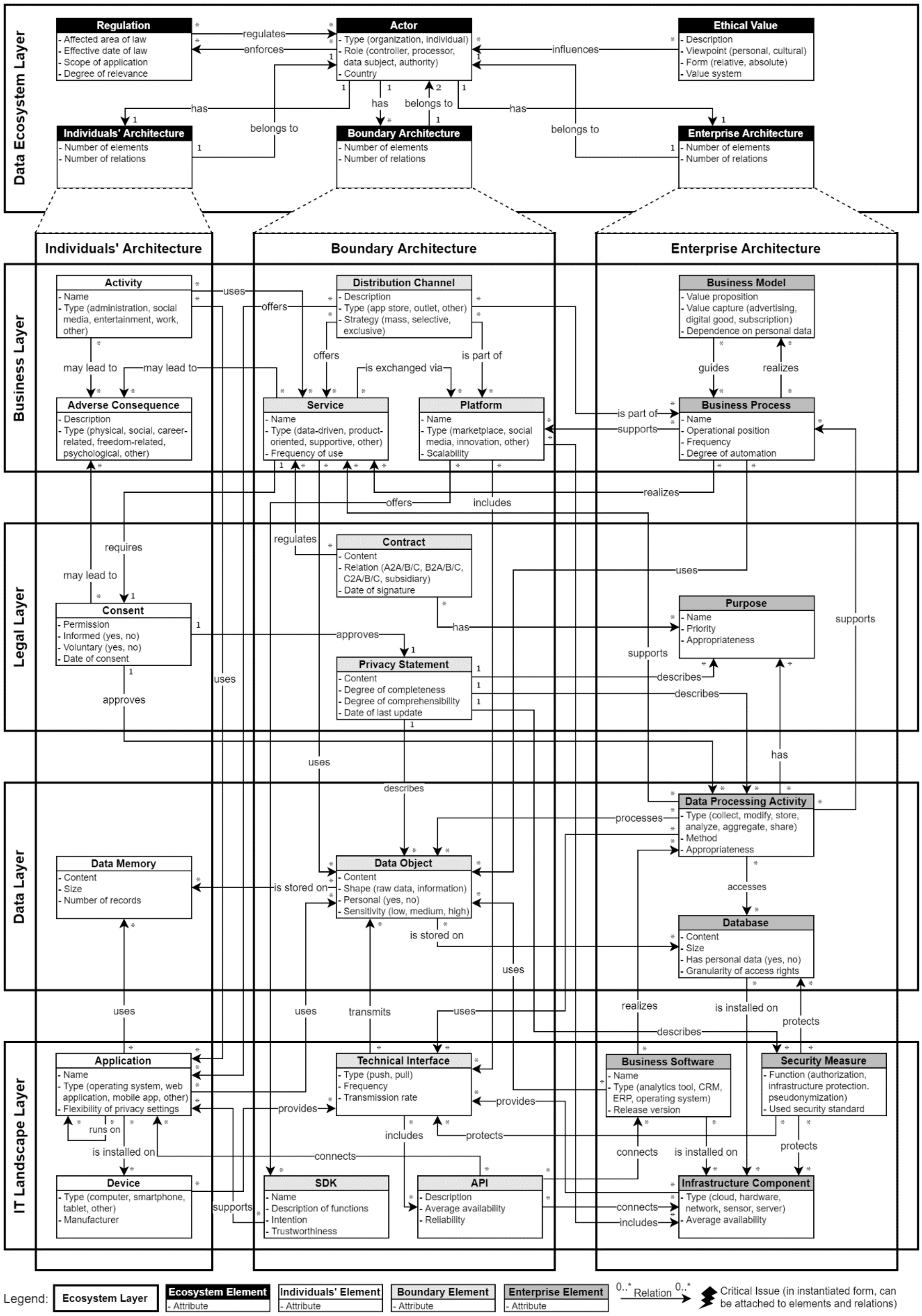


Figure 3. Data Ecosystem Architecture Meta-Model

15.5 Demonstration of Architectural Thinking based on the Meta-Model

The privacy concerns of business and regulatory stakeholders (see Table 3) refer to both analysis (as-is) and planning (to-be) scenarios. In the following, we demonstrate that AT based on our meta-model is capable of supporting these scenarios by providing transparency about increasingly complex data ecosystems.

15.5.1 Business Perspective

To demonstrate the usefulness of AT from the perspective of business stakeholders, we participated in a project in which we practically applied AT to support privacy-related design decisions. The aim of this project we call NeighborBook (NB) is to develop an online neighborhood social network in the context of smart cities and healthy urban communities. Its functionality comprises an activity stream for sharing news, requests for assistance, a private messaging system, a neighborhood calendar, neighbor profiles, and a directory of registered neighbors. Users access NB via desktop or mobile devices using a web application. As opposed to traditional online social networks with similar features, NB separates users into isolated sub-communities based on their residential address. To enforce this requirement, neighbors must provide their address during the signup and receive a physical letter with a verification code to enter upon their first login. Correctness and precision of the address data provided by users is key to successfully verifying their address. Therefore, the implementation of a third-party address autocompletion service was considered during development. Offered by an address autocompletion provider (AAP) located in the United States and embedded in the NB web application via an external JavaScript tag, this service is able to provide real-time address completion based on the characters entered by users in the address field. The service is offered free of charge and its technical implementation requires no more than two lines of code.

To assess potential privacy impacts regarding the design decision of implementing this third-party service, the corresponding data ecosystem was modeled based on our meta-model. The resulting model reveals a number of issues (1a–3c in Figure 4) related to the list of concerns (see Table 3). Issue 1a illustrates that the address autocomplete script directly transmits data from the NB web application to the AAP without the involvement or control of the NB provider (C24, C25). As issue 1b shows, with this transmission, the AAP gains technical data, including the IP address, of the user's device and the partial address data entered (C10, C12). Modeling the AAP's EA reveals some issues pertaining to data processing activities. The identification of these issues is based on an analysis of the AAP's privacy policy, which reveals several BAs to third-party data buyers and sellers. Issue 2a shows that the AAP enriches the technical and address data of users by purchasing complementary data (C13). Issue 2b clarifies that the AAP aggregates the collected data to create user profiles (C15, C30). Issues 2c and 2d show that the AAP analyzes the profiles to identify usage patterns (e.g., for ads or service improvement) and for other purposes (C30). Issue 2e shows that the AAP also shares the collected data with data buyers (C18). The concrete identities of third-party buyers and sellers remain unspecified (C38). Albeit these purposes can be extracted from the AAP's privacy policy, their relation to the core address autocompletion service is not immediately clear (C7, C31, C32). The model also identifies issues pertaining to additional effort required as part of the service's implementation. Issue 3a shows the need for a data processing agreement to be established between the AAP and NB (C5). As issue 3b indicates, NB must adapt its privacy statement to include the AAP as third-party data processor (C36–C38). Finally, following issue 3c, NB would need to gain consent from its users before the script is loaded on their device (C20).

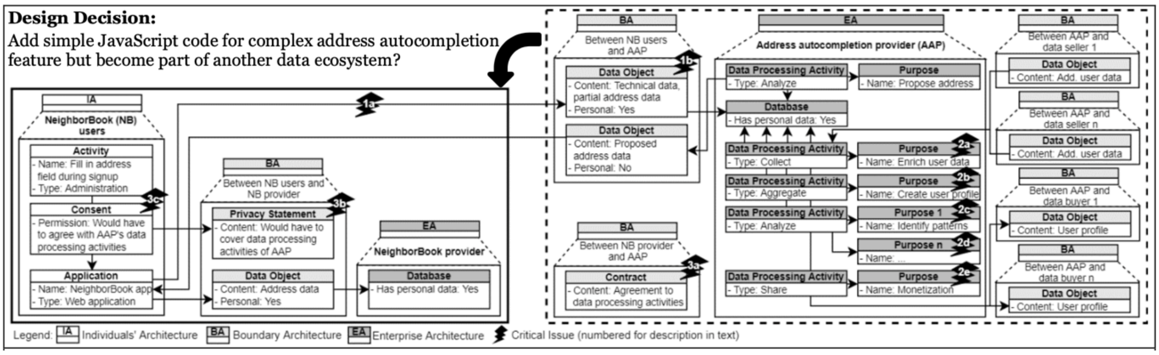

Design Decision:
Add simple JavaScript code for complex address autocompletion feature but become part of another data ecosystem?
IA
NeighborBook (NB) users
Activity
- Name: Fill in address field during signup
- Type: Administration
Consent
- Permission: Would have to agree with AAP's data processing activities
Application
- Name: NeighborBook app
- Type: Web application
3c
1a
BA
Between NB users and NB provider
3b
Privacy Statement
- Content: Would have to cover data processing activities of AAP
Data Object
- Content: Address data
- Personal: Yes
EA
NeighborBook provider
Database
- Has personal data: Yes
BA
Between NB users and AAP
1b
Data Object
- Content: Technical data, partial address data
- Personal: Yes
Data Object
- Content: Proposed address data
- Personal: No
BA
Between NB provider and AAP
3a
Contract
- Content: Agreement to data processing activities
EA
Address autocompletion provider (AAP)
Data Processing Activity
- Type: Analyze
Purpose
- Name: Propose address
Database
- Has personal data: Yes
Data Processing Activity
- Type: Collect
Purpose
- Name: Enrich user data
2a
Data Processing Activity
- Type: Aggregate
Purpose
- Name: Create user profile
2b
Data Processing Activity
- Type: Analyze
Purpose 1
- Name: Identify patterns
2c
Purpose n
- Name: ...
2d
Data Processing Activity
- Type: Share
Purpose
- Name: Monetization
2e
BA
Between AAP and data seller 1
Data Object
- Content: Add. user data
BA
Between AAP and data seller n
Data Object
- Content: Add. user data
BA
Between AAP and data buyer 1
Data Object
- Content: User profile
BA
Between AAP and data buyer n
Data Object
- Content: User profile
Legend: IA Individuals' Architecture BA Boundary Architecture EA Enterprise Architecture Critical Issue (numbered for description in text)

Figure 4. Instantiation of the Meta-Model for a Design Decision in App Development

Modeling the presented data ecosystem allows for a holistic design decision that considers potential privacy risks, mitigation, and implementation effort as well as expected benefits for NB users resulting from service implementation. In the present case, risk and effort were assessed to outweigh the benefits of improving the quality of address data. Consequently, the address autocompletion service was not implemented in NB. Similar design decisions, facilitated through instantiations of the meta-model, were made in case of an interactive mapping service, third-party email and physical mail services, as well as hosting providers.

15.5.2 Regulatory Perspective

To cover the perspective of regulatory stakeholders, we demonstrate AT based on our meta-model using two additional privacy scandals selected from our case study database. Similar to the approach in our previous multiple case study (see section Methodology), we collected and analyzed case-related news articles. The first of these cases refers to the gas station app GasBuddy (GB), which sold location data to Reveal Mobile, a geofencing marketing and analytics provider (exemplary link: cnet.co/33ai5CI), without the knowledge of its users. Reveal Mobile shared the location data with third-party companies, including data aggregators, insurances, or advertisers, resulting in adverse consequences such as location-based ads. In the second case, the weather app AccuWeather (AW) shared location data with Reveal Mobile as well. If users opted out of providing their location, the AW app transmitted the WiFi data and Bluetooth status of users' devices to Reveal Mobile, which approximated users' locations based on these data (exemplary link: zd.net/2RfoPfI). We chose these cases for demonstration because they both involve Reveal Mobile, providing the opportunity to capture both cases in one instantiation of the meta-model and to illustrate the data ecosystem of an actor operating in the background of apps, which may lead to important insights from a regulatory perspective.

The resulting model highlights a number of issues (1a–3 in Figure 5) related to the concerns (see Table 3). Regarding the GB case, issue 1a shows that the privacy statement between GB and its users does not mention Reveal Mobile as third-party recipient, despite recipients such as Foursquare being listed in connection with location data (C20, C36, C38). As shown by issues 1b and 1c, the GB provider shares collected user data for monetization purposes (C30, C37). Issue 1d clarifies that the GB provider not only shares location data with Reveal Mobile, but also the advertising ID and IP address of users' devices (C24). Issue 1e shows the contract between the GB provider and Reveal Mobile, about which users have not been informed (C5, C7). To highlight the critical issues in the AW case, we only modeled the opt-out alternative of users. Here, issue 2a shows that the AW app includes the Reveal Mobile SDK (C27). Issues 2b and 2c clarify that the AW app transmits users' WiFi data and Bluetooth status received from the iOS operating system to Reveal Mobile via the SDK (C18, C20). Issue 2d illustrates that Reveal Mobile stores these data on its servers (C14). Based on the stored WiFi data and Bluetooth status, Reveal Mobile approximates AW users' locations (C11), as shown by issues 2e and 2f. Finally, issue 3 points out that the location data, whether received directly as in the GB case or approximated based on technical data as in the AW case, is shared with third parties (C18). Moreover, according to a news article linked above, more than 500 other apps use the Reveal Mobile SDK.

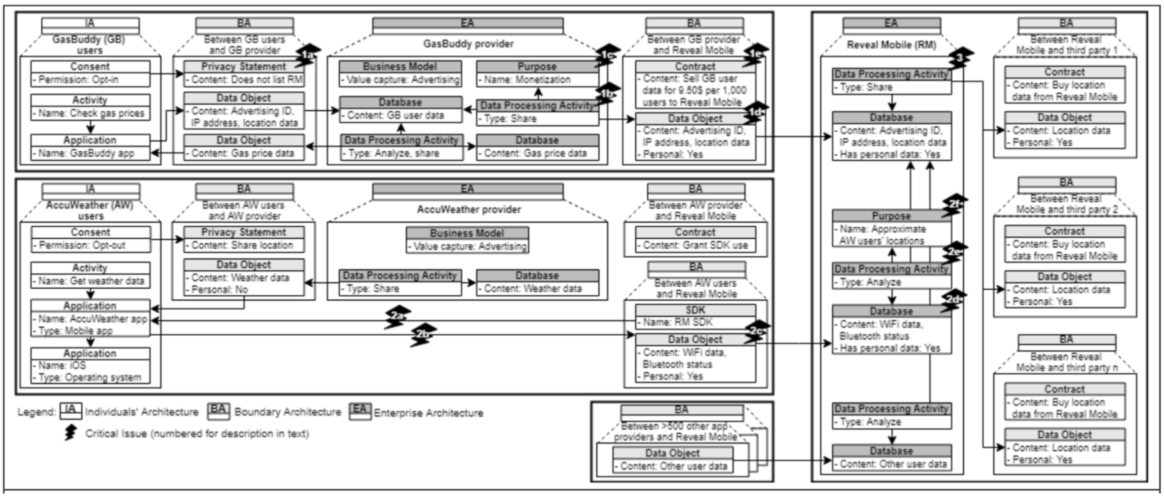


Figure 5. Instantiation of the Meta-Model for Analyzing Reveal Mobile's Data Ecosystem

The presented model reveals some interesting discussion points from a regulatory perspective that require further consideration. First, the model indicates the different ways in which data aggregators such as Reveal Mobile acquire personal data, as in our cases via inadequately informed consent or technically hidden via SDK. In the GB case, it is highly questionable to what extent users' consent was informed, as Reveal Mobile was not mentioned in the privacy statement. The AW case challenges the concept of informed consent as well, as user locations could be identified by processing other data types, despite users opting out of sharing their locations. Legislators must pay greater attention to such technical backdoors, often enabled by third-party components like SDKs, and to the inexplicitly defined associated responsibilities. Second, the model shows the numerous apps from which a data aggregator receives personal data and the numerous partners to which data flow back. These apps and partners are connected to further actors with whom they share personal data and so forth. Hence, defining the boundaries of a data ecosystem is a challenging task that needs future research. For example, Figure 5 suggests an intersection, i.e., Reveal Mobile's data ecosystem receives data from each app provider's data ecosystem. Third, while regulations such as the GDPR focus on dyadic relationships between data subjects and data controllers, they also allow joint-controllerships where multiple controllers have respective responsibilities (GDPR 2016, Art. 26). However, to comprehend areas of responsibility among joint controllers, transparency is needed about their integration in data ecosystems. At this point, AT helps to capture the socio-technical relations of controllers, especially by modeling BAs.

15.6 Discussion

Recently, scholars have called for research to "open up new domains for EM [enterprise modeling] – e.g., for conceptualizing modeling methods for the legal/compliance domain" (Sandkuhl et al. 2018, p.

77). Following this call and drawing upon the paradigm of AT, we collected privacy concerns of business and regulatory stakeholders (RQ1) to develop a data ecosystem architecture meta-model (RQ2). As exemplified by our case study, recent privacy scandals illustrate the need for making data ecosystems more transparent and manageable (Crain 2018; Nissenbaum 2019). AT provides a reasonable means for this task by allowing a structured decomposition of socio-technical relations in data ecosystems. The concerns and meta-model equip AT by enabling systematic switching between actor-, concern-, and layer-oriented perspectives.

The results of this study contribute to research and practice alike. From an academic point of view, they contribute to both IS and privacy research. While existing privacy models generalize the actors involved in personal-data sharing (Conger et al. 2013; Benson et al. 2015), AT based on our meta-model allows not only a flexible classification of actors but also to capture the manifold data flows between them by relating socio-technical elements across the different architectures (EA, IA, and BA) constituting data ecosystems. Owing to the generalizability of our results, achieved by involving several experts and cases, AT can be applied to case study research in the privacy field and support the in-depth analysis and comparison of different types of privacy violations. For example, considering selected concerns in a cross-case analysis can reveal patterns of socio-technical relations commonly leading to privacy violations, such as recurring flows of personal data between actors or technical backdoors (e.g., achieve data via SDK). Moreover, modeling data ecosystems can show gaps in data flows or indicate whether actors purposely obfuscated parts (e.g., unclear data sources of a processing activity). Thus, from a regulatory perspective, it becomes clear which questions are open and which actors need to be scrutinized. In this regard, by enabling the identification of patterns and gaps in data ecosystems, AT complements analytical frameworks in the privacy field (Kurtz et al. 2018) that aim to specify the reasons for privacy violations. Furthermore, AT supports the application of Nissenbaum's (2011) theory of contextual integrity, which states that privacy is given when data flows are appropriate. On the one hand, instantiations of our meta-model make data flows visible and thus enable a legal assessment using the theory. On the other hand, modeled socio-technical elements help fill the parameters that make up the appropriateness. In particular, defining the transmission principle, which refers to constraints like "stolen" or "sold" (Nissenbaum 2019), needs detailed architectural insights. Above all, there is a lack of research on extending meta-models with a privacy-, data-, or ecosystem-oriented lens. Albeit some meta-models suggest data source (Erraissi and Belangour 2018) or data processing layers (Burmeister et al. 2019b), they are limited by the intra-organizational lens of EA. In contrast, ecosystem meta-models do not focus on privacy concerns (Feltus et al. 2017; Oliveira et al. 2018; Burmeister et al. 2019a). Our meta-model contributes to this research gap by combining the intra- and inter-organizational perspectives with business, legal, data, and IT landscape layers. Hereby, we follow Sandkuhl et al.'s

(2018) call for extending the scope of enterprise modeling. By addressing privacy concerns of business and regulatory stakeholders about data ecosystems, we contribute to the concern, stakeholder, and model scope dimensions proposed by Sandkuhl et al. (2018).

Our results also have several practical implications. Business and regulatory stakeholders can perform AT based on the concerns and meta-model to obtain transparency about data ecosystems at different levels of detail during both analysis (as-is) and planning (to-be) scenarios. For example, AT can support business stakeholders in optimizing personal-data flows for specific business processes or in strategically planning to initiate or join a data ecosystem taking into account privacy constraints. Businesses can also rely on the meta-model to recall interdependencies critical to privacy and foresee challenges when sharing personal data with third parties. Moreover, businesses can draw on meta-model instantiations to complete the record of processing activities (GDPR 2016, Art. 30), identify privacy risks and improve related measures, as well as proactively prove privacy compliance to individuals, e.g., through simplified architecture visualizations. Regulatory stakeholders can apply AT for the in-depth assessment of privacy violations or the anticipation of adverse consequences when balancing legal provisions and benefits of personal-data use in rulemaking. For example, AT can be used to simulate and compare scenarios where certain laws are not met. AT assists regulatory stakeholders in identifying the socio-technical relations causing privacy violations and, based on the architectural insights, in revising regulations or privacy statements. This need is underlined by the cases of GB and AW, as certain third parties may not be listed in privacy statements or may gain hidden access to data via technical components like SDKs. Furthermore, practitioners can use and extend our list of concerns to consider essential questions about privacy in data ecosystems or customize the meta-model according to their specific needs. The demonstrated models (see Figures 4 and 5) also clarify that only selected elements of the meta-model may be used, depending on the concerns stakeholders have. In other words, not all elements of the meta-model must be instantiated to support privacy-related tasks or decisions. Through its holistic view on data ecosystems, AT complements existing methods or tools practitioners use to detect and document privacy challenges, such as checklists or evaluation procedures. For example, as shown by the NB project, insights from modeling potential third-party integration can significantly affect decision-making.

This study is not without limitations. First, the results are grounded in public data on privacy scandals and 14 expert interviews. Although this mixed methods approach helped us triangulate data and reduce possible bias, additional cases and interviews may have revealed other relevant privacy concerns. Second, to inform the interviews through privacy-critical practices, we analyzed scandalous data ecosystems. Future research should look at cases of data ecosystems where privacy was not violated to compare best and worst practices. Third, owing to our organizational perspective on data ecosystems, we interviewed business and regulatory stakeholders. Although the interviewees considered the perspective of individuals whose personal data are processed, additional surveys with individuals may lead to further insights, for example, to refine elements of the IA. Fourth, AT aims to increase the impact and scope of EAM by being less formalized and more lightweight (Winter 2014; Aier et al. 2015). However, regarding the privacy context, our study revealed a variety of stakeholder concerns that require a rather complex and comprehensive meta-model. To address this paradox, future research should use our meta-model to predefine simplified models for specific privacy-related tasks, as also suggested by the respondents as an outcome of the evaluation. Finally, although we demonstrated AT through application in a project and based on two additional cases, more iterations of research are required to evaluate the practical realization of AT in the privacy context and refine our results.

15.7 Conclusion

In times of obfuscated personal-data sharing and exploitation in increasingly complex data ecosystems, business and regulatory stakeholders face the challenge of maintaining transparency about the various data flows between actors and their related processing mechanisms (Crain 2018; Kurtz et al. 2018; Elrick 2021). This transparency is necessary to balance the benefits of personal-data processing with privacy risks, from both the individuals' and organizations' viewpoints, and to understand the manifold triggers for privacy violations in order to adjust regulations if applicable (Nissenbaum 2011; Tene and Polonetsky 2013). In this regard, AT provides a reasonable approach to obtaining transparency by supporting the systematic analysis and decomposition of socio-technical elements and relations. By collecting key privacy concerns of business and regulatory stakeholders and developing a corresponding data ecosystem architecture meta-model, this study provides first steps for extending the scope of AT to the privacy context. Researchers and practitioners can rely on our results to understand the causalities in data ecosystems from a socio-technical perspective, identify privacy-critical issues from both an intra- and an inter-organizational point of view, and equip their manifold privacy-related tasks and decisions with architectural models at the appropriate level of detail. Building on the architectural lens on data ecosystems, future research should focus on studying the systemic effects resulting from data ecosystems and on identifying the associated deficiencies in existing regulations.

15.8 References

Acquisti, A., Taylor C., and Wagman, L. 2016. "The Economics of Privacy," *Journal of Economic Literature* (54:2), pp. 442-492.

Aier, S., Labusch, N., and Pähler, P. 2015. "Implementing Architectural Thinking: A Case Study at Commerzbank AG," in *Trends in Enterprise Architecture Research – CAiSE 2015 International Workshops*, A. Persson and J. Stirna (eds.), Berlin/Heidelberg: Springer, pp. 389-400.

Ananny, M. and Crawford, K. 2018. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability," *New Media & Society* (20:3), pp. 973-989.

Attard, J., Orlandi, F., and Auer, S. 2016. "Data Value Networks: Enabling a New Data Ecosystem," in *Proceedings of the 2016 International Conference on Web Intelligence*, Omaha, NE, USA, pp. 453-456.

Azkan, C., Möller, F., Meisel, L., and Otto, B. 2020. "Service Dominant Logic Perspective on Data Ecosystems - A Case Study based Morphology," in *Proceedings of the 28th European Conference on Information Systems*, virtual AIS conference.

Bélanger, F. 2012. "Theorizing in Information Systems Research Using Focus Groups," *Australasian Journal of Information Systems* (17:2), pp. 109-135.

Bélanger, F. and Xu, H. 2015. "The Role of Information Systems Research in Shaping the Future of Information Privacy," *Information Systems Journal* (25:6), pp. 573-578.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3), pp. 369-386.

Benson, V., Saridakis, G., and Tennakoon, H. 2015. "Information Disclosure of Social Media Users: Does Control over Personal Information, User Awareness and Security Notices Matter?" *Information Technology & People* (28:3), pp. 426-441.

Burmeister, F., Drews, P., and Schirmer, I. 2019a. "An Ecosystem Architecture Meta-Model for Supporting Ultra-Large Scale Digital Transformations," in *Proceedings of the 25th Americas Conference on Information Systems*, Cancún, Mexico.

Burmeister, F., Drews, P., and Schirmer, I. 2019b. "A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Wailea, HI, USA, pp. 6052-6061.

Cate, F. H. and Mayer-Schönberger, V. 2013. "Notice and Consent in a World of Big Data," *International Data Privacy Law* (3:2), pp. 67-73.

Conger, S., Pratt, J. H., and Loch, K. D. 2013. "Personal Information Privacy and Emerging Technologies," *Information Systems Journal* (23:5), pp. 401-417.

Crain, M. 2018. "The limits of transparency: Data brokers and commodification," *New Media & Society* (20:1), pp. 88-104.

Culnan, M. J. and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323-342.

Demchenko, Y., de Laat, C., and Membrey, P. 2014. "Defining architecture components of the Big Data Ecosystem," in *Proceedings of the 2014 International Conference on Collaboration Technologies and Systems*, Minneapolis, MN, USA, pp. 104-112.

Eaton, B., Elaluf-Calderwood, S., Sorensen, C., and Yoo, Y. 2015. "Distributed tuning of boundary resources: the case of Apple's iOS service system," *MIS Quarterly* (39:1), pp. 217-243.

Elrick, L. E. 2021. "The ecosystem concept: a holistic approach to privacy protection," *International Review of Law, Computers & Technology* (35:1), pp. 24-45.

Erraissi, A. and Belangour, A. 2018. "Data sources and ingestion big data layers: meta-modeling of key concepts and features," *International Journal of Engineering & Technology* (7:4), pp. 3607-3612.

Feltus, C., Grandry, E., and Fontaine, F.-X. 2017. "Capability-Driven Design of Business Service Ecosystem to Support Risk Governance in Regulatory Ecosystems," *Complex Systems Informatics and Modeling Quarterly* (10), pp. 75-99.

Fill, H.-G. and Johannsen, F. 2016. "A Knowledge Perspective on Big Data by Joining Enterprise Modeling and Data Analyses," in *Proceedings of the 49th Hawaii International Conference on System Sciences*, Koloa, HI, USA, pp. 4052-4061.

Flick, U. 2009. An Introduction to Qualitative Research, Thousand Oaks: Sage.

Frank, U. 2014. "Multi-perspective enterprise modeling: foundational concepts, prospects and future research challenges," *Software & Systems Modeling* (13:3), pp. 941-962.

GDPR Tracker. 2021. *Enforcement Tracker*, https://www.enforcementtracker.com, accessed 2021/09/06.

GDPR. 2016. "General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union* (111).

Gelhaar, J., Groß, T., and Otto, B. 2021. "A Taxonomy for Data Ecosystems," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, virtual conference, pp. 6113-6122.

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., and Zhdanov, D. 2018. "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas," *MIS Quarterly* (42:1), pp. 143-164.

Iansiti, M. and Levien, R. 2004. The Keystone Advantage: What the New Dynamics of Business Ecosystems Mean for Strategy, Innovation, and Sustainability, Boston: Harvard Business School Press.

ISO/IEC. 2002. "Information technology - CDIF framework - Part 1: Overview," standard 15474-1:2002.

ISO/IEC/IEEE. 2011. "Systems and software engineering – architecture description," standard 42010:2011.

Karwatzki, S., Trenz, M., Tuunainen, V. K., and Veit, D. 2017. "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence," *European Journal of Information Systems* (26:6), pp. 688-715.

Kurtz, C., Semmann, M., and Schulz, W. 2018. "Towards a Framework for Information Privacy in Complex Service Ecosystems," in *Proceedings of the 39th International Conference on Information Systems*, San Francisco, CA, USA.

Lagerström, R., Saat, J., Franke, U., Aier, S., and Ekstedt, M. 2009. "Enterprise Meta-Modeling Methods – Combining a Stakeholder-Oriented and a Causality-Based Approach," in *Enterprise, Business-Process and Information Systems Modeling, LNBIP (29)*, T. A. Halpin, J. Krogstie, S. Nurcan, E. Proper, R. Schmidt, P. Soffer, and R. Ukor (eds.*)*, Berlin/Heidelberg: Springer, pp. 381-393.

Mayring, P. 2014. Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution, Weinheim: Beltz.

Moore, J. F. 1996. The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems, New York: Harper Business.

Myers West, S. 2019. “Data Capitalism: Redefining the Logics of Surveillance and Privacy,” *Business & Society* (58:1), pp. 20-41.

Myers, M. D. and Newman, M. 2007. “The qualitative interview in IS research: Examining the craft,” *Information and Organization* (17:1), pp. 2-26.

Niemi, E. 2007. “Enterprise Architecture Stakeholders - a Holistic View,” in *Proceedings of the 13th Americas Conference on Information Systems*, Keystone, CO, USA.

Nissenbaum, H. 2011. “A Contextual Approach to Privacy Online,” *Daedalus* (140:4), pp. 32-48.

Nissenbaum, H. 2019. “Contextual Integrity Up and Down the Data Food Chain,” *Theoretical Inquiries in Law* (20:1), pp. 221-256.

Oliveira, M. I. S., de Fátima Barros Lima, G., and Lóscio, B. F. 2019. “Investigations into Data Ecosystems: A Systematic Mapping Study,” *Knowledge and Information Systems* (61:2), pp. 589-630.

Oliveira, M. I. S., Oliveira, L. E. R. A., Batista, M. G. R., and Lóscio, B. F. 2018. “Towards a Meta-model for Data Ecosystems,” in *Proceedings of the 19th Annual International Conference on Digital Government Research*, Delft, The Netherlands.

Purtova, N. 2018. “The law of everything. Broad concept of personal data and future of EU data protection law,” *Law, Innovation and Technology* (10:1), pp. 40-81.

Saat, J., Franke, U., Lagerström, R., and Ekstedt, M. 2010. “Enterprise Architecture Meta Models for IT/Business Alignment Situations,” in *Proceedings of the 14th IEEE EDOC*, Vitoria, Brazil, pp. 14-23.

Saldaña, J. 2015. The Coding Manual for Qualitative Researchers, Thousand Oaks: Sage.

Sandkuhl, K., Fill, H.-G., Hoppenbrouwers, S., Krogstie, J., Matthes, F., Opdahl, A., Schwabe, G., Uludag, Ö., and Winter, R. 2018. “From Expert Discipline to Common Practice: A Vision and Research Agenda for Extending the Reach of Enterprise Modeling,” *Business & Information Systems Engineering* (60:1), pp. 69-80.

Shah, S. I. H., Peristeras, V., and Magnisalis, I. 2020. “Government (Big) Data Ecosystem: Definition, Classification of Actors, and Their Roles,” *International Journal of Computer and Information Engineering* (14:4), pp. 102-114.

Tene, O. and Polonetsky, J. 2013. “Big Data for All: Privacy and User Control in the Age of Analytics,” *Northwestern Journal of Technology and Intellectual Property* (11:5), pp. 239-273.

The Open Group. 2018. TOGAF standard, version 9.2.

Winter, R. 2014. “Architectural Thinking,” *Business & Information Systems Engineering* (6:6), pp. 361-364.

Yin, R. K. 2009. *Case Study Research: Design and Methods*, Thousand Oaks: Sage.

Zuiderwijk, A., Janssen M., and Davis, C. 2014. “Innovation with open data: Essential elements of open data ecosystems,” *Information Polity* (19:1), pp. 17-33.

16 Article No. 8 (Kurtz et al. 2021)

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. Accountability of platform providers for unlawful personal data processing in their ecosystems–A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR. Journal of Responsible Technology, 2021.

Abstract

Billions of people interact within platform-based ecosystems containing the personal data of their daily lives, which have become rigorously creatable, processable, and shareable. Platform providers facilitate interactions between users, service providers, and third parties in these socio-technical ecosystems. Platform providers influence their platform ecosystems to promote the contributions of the service providers and exercise control by utilizing boundary resources investigated in the information systems field. In a socio-techno-legal analysis of two high-profile cases and consideration of the General Data Protection Regulation (GDPR), we show that the boundary resource design, arrangement, and interplay can influence whether and to what extent platform providers are accountable for platform providers unlawful personal data processing in platform ecosystems. The findings can have a huge impact to account actors for personal data misusage in platform ecosystems and, thus, the protection of personal liberty and rights in such socio-technical systems.

16.1 Introduction

Countless and manifold digital interactions take place in platform ecosystems. Platform providers facilitate value-co-creation between various groups in the form of users, service providers, and related third parties (Constantinides, Henfridsson, & Parker, 2018; Ghazawneh & Henfridsson, 2013; Van Alstyne, Parker, & Choudary, 2016). However, the Facebook and Cambridge Analytica scandal was an exemplary event in the history of privacy violations within a platform ecosystem. Sharing personal data and performing analytics across interconnected parties enabled a new degree of manipulation (Cadwalladr & Graham-Harrison, 2018). Approximately 87 million Facebook users were affected by the invasive access to their personal data (Frier, 2018). As Jirotka and Stahl (2020) made clear, this scandal of social media data used for unintended purposes had a significant impact on information privacy and political processes.

However, the discussions around large amounts of data, data processing, and ethical components also inspired far-reaching policy development (Jirotka & Stahl, 2020). In this article, we will make us of the GDPR that came into force in May 2018 intending to protect individuals of actors unlawfully processing their personal data, also to safeguard fundamental rights and freedoms of individuals. Using the GDPR, an assessment is possible to prove whether and to what extent an actor is accountable for (unlawful) personal data processing. In detail, the GDPR stipulates specific roles with clearly defined obligations regarding data protection (GDPR, 2016a). Being accountable requires companies to comply with the principles and related accountability mechanisms specified in the GDPR (Vedder & Naudts, 2017). Accountability means being accountable for the processing of personal data (i.e., for ensuring that all obligations are met during processing) and the obligation to be able to prove that this account has been met (Frenzel, 2018).

From the information systems field, we know that platform providers such as Facebook facilitate a platform and its included set of digital resources that enable digital interactions (Parker, Van Alstyne, & Choudary, 2016). In a platform ecosystem, platform providers use boundary resources as socio-technical indications to promote external contribution and exercise control (Ghazawneh & Henfridsson, 2013). Thus, platform providers have an influential position to control the ecosystem (Eaton, Elaluf-Calderwood, Sorensen, & Yoo, 2015). However, so far, the question remains open whether platform providers can be made accountable for data processing by other actors that were not lawful in their platform ecosystems. Thus, the aim of this study is (I) to determine how the boundary resources of the platforms affect the various actors in the platform ecosystems in privacy-violating processing and the sharing of personal data and (II) how novel regulations, especially the GDPR, can utilize these findings to legally obligate the platform providers to consider a platform design that is sensitive to data protection and thus, to the protection of personal liberty and rights in such socio-technical systems.

This study is conducted at the intersection of information systems research and law by using two well-documented cases of privacy violations in the platform ecosystems of Apple iOS and Facebook and begins with the foundations of platform ecosystems and the GDPR. Subsequently, we conduct a multiple-case study in which boundary resources as an analytical framework, such as data flows and activities of the actors involved, are investigated. We determine the influence of the platform providers on privacy violations in these cases based on the GDPR. In further legal assessment, we assess the allocation of accountability and the corresponding legal obligations. The findings of this analysis are generalized by describing the relationship between the platform's architecture, the related boundary resources, and the allocation of accountability according to the GDPR. Lastly, the practical, the research, and the regulative implications are detailed, which may have fundamental implications for the future protection of individuals by law.

16.2 Theoretical Framework

16.2.1 Platform Ecosystems

In information systems literature, diverse concepts and understandings of platforms exist (Constantinides et al., 2018; de Reuver, Sørensen, & Basole, 2018). We understand platforms as a software-based system with an extensible codebase that enables functionality for users through additional software subsystems in the form of modules provided by service providers (Baldwin & Woodard, 2009; de Reuver et al., 2018; Tiwana, Konsynski, & Bush, 2010). In the case of applications, the modules interoperate with the platform and enable the provision of functionality, service, or content (Constantinides et al., 2018). Platforms differ in their architecture type and their form of module provision. In closed platforms, the providers' control which modules are accessible by the controlled distribution of modules and their means of access, typically using app stores (Hein et al., 2019; Schreieck, Wiesche, & Krcmar, 2016; Tiwana et al., 2010). In open platform architectures, the platform providers do not control this distribution and leave the interaction paths more open (de Reuver et al., 2018; Tiwana et al., 2010). In addition, hybrid architectures exist where platform providers control distribution channels and make provisions for open distribution channels and interactions.

Platform providers represent intermediary groups in the structural arrangement of multi-group data processing. Typically, a platform ecosystem also includes third parties embedded by service providers, which have less been addressed in previous studies on platform ecosystems but are often involved in digital interactions.

16.2.2 Platform's Boundary Resources

The interaction between service providers and the platforms has been central to the concept of boundary resources in platform research (Constantinides et al., 2018; Tiwana et al., 2010). Designing and implementing boundary resources requires retaining control while allowing service providers to implement independent platform innovation (Eaton et al., 2015). To maintain balance, the boundary resources evolve and change over time (Eaton et al., 2015). Boundary resources can emerge from a process of negotiation between the platform provider and the service providers; Eaton et al. described this process as "tuning" (Eaton et al., 2015). They can also perform the functions of resourcing and securing (Ghazawneh & Henfridsson, 2013). Platform resourcing is defined as the mechanisms and the tools by which the scope and the diversity of a platform are enhanced, such as software development kits (SDKs) or application programming interfaces (APIs) (Ghazawneh & Henfridsson, 2013; Hagiu & Wright, 2015; Van Alstyne et al., 2016). The function of securing the platform enables control using the boundary resources (Ghazawneh & Henfridsson, 2013). For example, this securing can result in an application review process or mandatory developer agreements (Ghazawneh & Henfridsson, 2013).

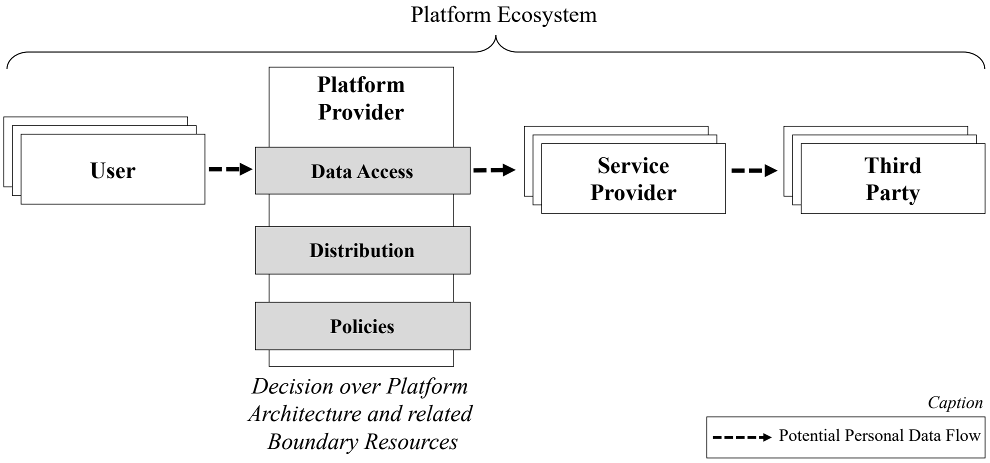


Figure 1. Platform Ecosystem and Boundary Resource Composition.

One boundary resource may contain several functions (Karhu, Gustafsson, & Lyytinen, 2018). Due to the convergence of several boundary resources in a platform ecosystem, this study is not focused on the functions of a single boundary resource but on the interaction of several boundary resources and how they complement each other (Figure 1). We characterize the composition of boundary resources of a platform provider as a configuration of the set of boundary resources that mutually depend on each other in their effects. While a focus on the design of a single boundary resource can be helpful, the focus on the composition is required for a complete overview regarding their effects; for example, on an individual's privacy.

Based on the platform providers' influence on the service providers and the third-party personal data processing, the boundary resource categories of data access, distribution, and policies are considered in this study (Table 1).

Table 1. Overview of Boundary Resources relevant for Privacy.

Boundary Resource Category	Boundary Resource	Description
Data Access	Data Interfaces	Enable service providers and third parties to access data via the platform
	User-Centered Configuration	Enables users to set configurations of the app data access
Distribution	Access to App's Privacy Statement	Describes the access to the terms of how the app wants to collect, use, share, and manage the transmitted data
	App Review Process	Reviews app compliance with platform policy and guidelines
	App Store	Provides the distribution channel for service providers
Policies	Platform Policies and Guidelines	Defines terms and conditions for service providers in developing, testing, distributing, maintaining, and running an app

Platform providers hold the position to independently design the boundary resources (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013). Such influence on the utilization of the platform and the means for data processing are associated with privacy implications and can trigger constraints on platform providers. We use the GDPR to understand when and under what circumstances platform providers can be subject to legal obligations and how far those obligations are applicable.

16.3 Legal Foundations

16.3.1 Applicability and Implications of the GDPR

Drafted in 2016 after a long discussion in the so-called trialogue (between the European Commission, European Parliament, and Council), the GDPR (GDPR, 2016b) was implemented in May 2018 after a two-year transitional phase. One of its important changes in comparison to the Data Protection Directive (DPD) that it replaced was an expanded scope of applicability, even binding companies outside of the EU when they process EU citizens' data (GDPR, 2016b, Art. 3 (2)). The GDPR as regulation is directly applicable and immediately binding for all 27 member states. The goal of the GDPR is to protect individuals regarding the processing of personal data relating to them (GDPR, 2016b, Art. 1 (1)) and at least to protect the information privacy of individuals. The GDPR defines "personal data" as follows:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (GDPR, 2016a, Art. 4 No. 1)

The GDPR also serves as a blueprint for privacy regulation across cultures worldwide, such as the California Consumer Privacy Act 2018 (de la Torre, 2018). The goal of the GDPR is to protect the personal data of individuals from being unlawfully processed (GDPR, 2016a, Art. 1 (1)). Under the GDPR, regulators can invoke substantial penalties of up to 4% of the annual worldwide revenues on companies for violating the data protection clauses (GDPR, 2016a, Art. 83 No. 5).

Primarily, the GDPR attempts to enforce data protection by offering a binary system of two opposing groups: a controller (entity processing the personal data) and a data subject (person to whom these data relate, namely the users in this study). However, just as platform ecosystems involve a more complex reality of actors, the GDPR is not limited to this traditional scenario and offers more possible roles.

16.3.2 Role of Controller

According to the GDPR (GDPR, 2016a, Art. 4 No. 7), a *controller* is any (natural or legal) person that alone or jointly determines the purposes and the means of processing personal data, that is, the "why" and the "how" of processing. The requirement for a company to be classified as a controller depends on the specific case. Some of the aspects that can typically only be covered by a controller are the decisions over whose data are being processed, which other parties can gain access to, and the length of their retention period (European Commission, 2010, p. 17).

It is a role that is always determined corresponding to a specific act or set of acts of processing (GDPR, 2016a, Art. 4 No. 2). These acts can include collection, recording, organization, structuring, storage, adaptation, usage, and disclosure. To limit risks from the acts of processing, the GDPR enjoins the controllers with certain obligations to safeguard the rights of data subjects. Most prominently, Art. 6 declares that every act of processing requires a legal basis, making it the controller's duty to ensure this basis and to declare which legal grounds are applicable.

Furthermore, certain organizational and technical measures must be taken to ensure that the controller complies with all specific data protection and data security provisions of the GDPR and can demonstrate this compliance at any given point, as Art. 24 declares. These obligations concretize Art. 5 (2), which establishes the principle of accountability as one of the cornerstones of lawful processing.

The measures to be taken by a controller depending on the scope, the context, and the purpose of the process; on the severity and the probability of the occurrence of risks to the rights of data subjects; and on the need to be "suitable" and "appropriate." Essentially, there is no general method of defining measures that every controller can take without considering the context and its specifics.

16.3.3 Role of Joint Controller

According to Art. 26, two or more actors can be *joint controllers* for an act of processing in which they jointly determine its purposes and means. This paragraph means that all the actors involved must have a decisive influence on the decisions made regarding the circumstances of the processing activity in question. That is, the act of processing must present itself as the object of the joint control of the group. For processing, this typically requires an agreement or a consultation of some kind, i.e., a shared understanding of the reasons and goals of the act, for example, a shared business model (Bot, 2018).

The regulatory idea behind this concept of allocating accountability to several groups at once for the lawfulness of a single act of data processing and compliance with the GDPR's rules and obligations regarding this act is as follows. Particularly in multi-group constellations, a latent risk of a vacuum of accountability is a possibility, where multiple groups play important roles in determining and structuring the context of personal processing data. An accountability vacuum tends to arise when the allocation of responsibilities is unclear, and the potential controllers do not claim accountability. The concept of joint controllership attempts to avoid such a vacuum by allocating accountability to all the groups that are sufficiently involved in cases of distributed actions and have influence over the acts of data processing. The primary goal is to provide sufficient clarity to allow and ensure effective application and compliance in practice (GDPR, 2016a, Art. 29).

The role of a *processor* has been specified according to Art. 4 No. 8. A processor is any natural or legal person, public authority, agency, or other body that processes data on behalf of the controller. A processor does not have agency and only acts upon the controller's instructions (Martini, 2018).

The investigation of the possibilities that a company has personal data processing in multi-actor constellations becomes legally relevant in two ways. Firstly, this investigation can determine which company - alone or jointly with others - exercises a level of control that classifies this enterprise as a data controller according to the GDPR. Secondly, the analysis helps a company assess the legal role to implement the regulations of the GDPR effectively. Understanding the design of platform ecosystems is crucial to assess the role and the associated obligations under the GDPR.

16.4 Methodology

In the following, a multiple-case study is conducted, and two cases that are paradigmatic for the phenomenon of interest are leveraged (Yin, 2009). Both cases, Facebook and iOS by Apple, involve large-scale platforms with a closed architecture. The platform providers do not seem comparable at first glance. Nevertheless, Apple and Facebook are providers of platforms in which boundary resources are used in different manifestations and in which the diffusion of personal data in each ecosystem has occurred. Therefore, we investigate the two cases, platform providers' role to the GDPR, and the extent of the platform provider obligations. Possible means of meeting the obligations are also assessed. The ways both platform providers changed their platforms in the wake of the previously investigated incidents have been analyzed.

We selected two publicly available cases which demonstrate the phenomena of privacy violations in platform ecosystems, but with different contexts (Albright, 2018; Cadwalladr & Graham-Harrison, 2018; Ribas, 2017; Rosenberg, Confessore, & Cadwalladr, 2018a, 2018b; Sherr, 2018; Strafach, 2017; Whittaker, 2017). Both the platforms are dominant in their respective fields, and each consists of numerous users and service providers. Due to this market coverage, a vast amount of analyzable data is available on the two platforms. The datasets analyzed in this study have a similar composition to those of other platform studies (Eaton et al., 2015; Ghazawneh & Henfridsson, 2013; Karhu et al., 2018) to analyze the circumstances of the cases and the corresponding boundary resources. Our dataset includes technology news articles, platform provider documents (platform release descriptions, platform policies, and descriptions of features), excerpts of developer discussion boards, apps privacy statements, as well as the hearing protocol and the response to questions asked by the National Association of Attorneys General, in the case of Facebook. This usage of various collected data ensures accuracy and reliability (Yin, 2009) and the possibility of data triangulation. Additionally, the multiple sources used in this study increase the robustness of the results (Paré, 2004). Diverse data sources reinforce the validity of the findings through cross-validation (Kaplan & Maxwell, 2005).

In a socio-techno-legal analysis (BLINDED), each case is examined in turn at the intersection of the research on information systems and the law, which builds upon and extends the prior interdisciplinary cases regarding privacy (Pavlou, 2011). This study utilizes the concept of boundary resources as an analytical framework and closely examines how the different types of boundary resources materialized in the two cases. Furthermore, it is analyzed how boundary resources affect the data processing acts and the privacy violations in both the platform ecosystems. Subsequently, the GDPR is considered a means to analyze these cases and their respective boundary resource designs. The legal implications for the platform providers and the architecture and design of their ecosystems can thus be derived.

16.5 Case I: Facebook, Digital Life, and Cambridge Analytica

This case has been widely covered in the media due to the hearing of the Facebook CEO, Mark Zuckerberg, before the United States House Committee on Energy and Commerce (Zuckerberg, 2018). At the case's onset, the developer, Aleksandr Kogan, built the personality quiz app Digital Life (This Is Your Digital Life) for the Facebook platform. In the app's terms of service, he specified how he wanted to use the accessed user and the usage data over the platform: "edit, copy, disseminate, publish, transfer, append, or merge with other databases, sell, license (by whatever means and on whatever terms) and archive your contribution and data" (Kogan, 2018; WashingtonPost, 2019). However, these terms conflicted with Facebook's platform policy for developers (WashingtonPost, 2019). Despite this conflict, the application passed the app review process of Facebook (WashingtonPost, 2019). After the review, the application was available for users in the platform's app store and was installed and used by 270,000 users (Rosenberg et al., 2018a).

When installing and using the application, users were asked to accept the requested data access by the application along with the app's terms of service. By accepting these conditions, users allowed the app to access their own data and the data of their Facebook friends (Facebook, 2018). This access was possible due to the design of the data access enabled for the service providers. The Graph API version 1.0 was implemented at that time (Facebook, 2018). Services in the form of apps could request a wide range of user and users' friends' data from Facebook servers through this API (Hartmans, 2018). While the users who consciously used the app were asked to accept the app's terms and by this act consent to its processing, the user's friends were not asked directly and thus had no chance to refuse. Instead, Facebook implemented the option of letting the app access the personal data as an option within the profile settings and kept it activated by default (Facebook, 2018; Hartmans, 2018).

Consequently, the app users' friends were forced to actively search for that option and disable it to opt-out of the sharing (McCausland & Schecter, 2018) without being informed while the information was being accessed. Many users' friends did not disable the setting, resulting in Facebook allowing the app to access their data. Here, the data access implementation led to divulging the data of 87 million

Facebook users to Digital Life (Frier, 2018), although only approximately 270,000 of those had actively used the app. Subsequently, Digital Life failed to comply with the platform policy to share such data. The app provider shared the data with the backend service, Cambridge Analytica, which used it to target users on Facebook to deliver individualized advertising (Rosenberg et al., 2018a).

From a legal point of view, one key aspect is that the data of the affected users were initially on the Facebook servers. By enabling access to the apps via Graph API version 1.0, Facebook established and structured apps' possibility to request this data. Thus, Facebook used a boundary resource that governed the means and the circumstances under which apps could gain access to user data to transmit data from Facebook to an app like Digital Life. In doing so, and by defining the limitations to the data access attempts, the app determined the means of processing.

Considering that the existence of apps on the Facebook platform and, by extension, the processing of the users' data by these apps is part of Facebook's business model, it is possible to attribute the determination of the purpose of this transmission to the platform and consequently classify Facebook as a controller of this act of processing. The determination of whether Facebook and Digital Life are joint controllers or not can be overlooked at this stage. Consequently, Facebook would have been entirely accountable for adhering to the provisions of the GDPR pertaining to these transmissions.

Digital Life directly collected two types of data: the profile data of users that installed the app and their friends' profile data that represented the critical data in this case, and the data that users provided as a conscious input when using the 'personality test' offered by the app (Hartmans, 2018). The profile data were already stored on Facebook's servers, while the second category of data was generated through the app's usage (and presumably saved by Facebook). In both cases, the service was entirely accountable for determining the purpose of the data requests. Because this was known to and approved by Facebook, a classification as a joint controller must be made, at least for the initial part of the processing (sharing of the data from Facebook to Digital Life).

16.6 Case II: iOS, AccuWeather, and Reveal Mobile

In the second case, the AccuWeather app had been added to the iOS AppStore after undergoing and passing Apple's App Store review process. Its privacy statement declared that the application and its implemented backend services could approximate the users' location. Moreover, the backend services were not named in detail (AccuWeather, 2017). When downloading the app, the users could acknowledge and read the privacy statement. Initially, a prompt was shown to the user regarding the permission to access the user's location (Apple, 2017b; Strafach, 2017). This access to the location services is explained in the iOS settings as follows: “Location Services uses GPS, Bluetooth, and crowd-sources WiFi hotspot and cell tower locations to determine your approximate location.” Some of the users who installed the app rejected this request. On Apple’s website (which corresponds to the iOS version of the case) regarding the location services in iOS, it was stated, “Tap ‘Don’t Allow’ to prevent access” (Apple, 2017b, 2018).

Based on this information, a user may infer that if they denied access to the location services requested by the applications, iOS would not provide any location data or the location approximation to the application. However, this was not the case, and the data access design by the platform provider, Apple, enabled access to critical data that would not be necessary for the application. In this case, the WiFi router name, the Basic Service Set Identification (BSSID), which corresponds to the media access control (MAC) address of the currently connected wireless access point, and the Bluetooth status, were available via an API in the iOS software. AccuWeather implemented the SDK of the third party, Reveal Mobile, which accessed the network data from the iOS platform (Strafach, 2017).

However, on a technical level, Apple’s statement still holds. Reveal Mobile did not gain any data directly through Apple’s location services. Instead, it bypassed this access channel and used another available data access point to approximate the users’ location. During a testing period of 36 hours, the data were sent 16 times to Reveal Mobile (Strafach, 2017). Thus, the company was able to determine the user's location by accessing the public databases of the stored locations of the wireless access points. In this instance, Reveal Mobile focused on mobile marketing by collecting and using the data of individuals (RevealMobile, 2017).

The legal classification, in this case, is more complex than in the first one. Since the affected data were directly transferred from the iOS platform to Reveal Mobile during the data accumulation, there was no active involvement by iOS apart at this specific point. The data were only stored on the user's phone, not on the Apple servers, and only during the data were requested by the app (or the Reveal Mobile SDK within the app). Nevertheless, Apple was indeed involved at an earlier point through the iOS platform's provision of the technical infrastructure to provide data access via APIs of both the location data and the network data. Specifically, it designed the location services API so that its usage was dependent on the users' permission.

In contrast, the APIs accessing the network data were designed more openly, allowing access to any app that requested these data. By extensively structuring the access APIs accordingly, Apple determined the means and the conditions in which the apps could access certain data types. Apple's developer program license agreement prohibited network data usage for location approximation, bypassing or overriding any user settings (Apple, 2017a). This statement indicates the usage of network data to determine the users' location if they have disabled the location services (Apple, 2017a). In addition, the way the existence of the apps is part of iOS's appeal to users is crucial for Apple and can be compared to the way Facebook offers apps access to the user data.

One significant difference from the first case concerns the type of data and the data transfer in the context of the users' actions (Table 2). The users explicitly declined the transmission of what Apple labeled "location data" to AccuWeather, thereby implicitly voicing their rejection of the transmission of any data that might be used to determine the user's location. It can also be stated that the accrual of WiFi and Bluetooth data are a technical necessity and are covered by the users' general intention of using a phone with all its features. However, these data would not be necessary for a functioning weather application. Requiring the user to manually check for the weather in a specific city or area may be less comfortable for the user, but it would be with the user's consent. In this case, the platform's involvement is smaller when compared to the first case. However, the deliberate design of the platform allows direct access to the specific data. The method by which Apple has changed this design can be observed in the deprecation of the access to MAC addresses in iOS 7 (Apple, 2017c). Nevertheless, access to the network data was still possible in iOS 10 (Ribas, 2017) and was only completely disabled in iOS 11 (Butts, 2017).

Table 2. Overview of Boundary Resource Manifestations in the Cases.

Boundary Resource Category	Boundary Resource	Manifestations in Case I	Manifestations in Case II
Data Access	Data Interfaces	The Graph API enabled data access to 270,000 app users and 87 million app users' friends stored on Facebook servers.	API for access to network data, which transmitted network data 16 times in 36 hours
	User-Centered Configuration	App users agreed to share data, resulting in their friends' data being accessed due to a configuration that enabled data access by default.	Users rejected sharing location data with the app, whereby no configuration options existed to disable network data access.
Distribution	App's Privacy Statement Access	Digital Life mentioned the intention to sell accessed data	Indicated applying methods for approximation of user locations
	App Review Process	Facebook reviewed the app and accepted the app along with the app's terms of service.	Apple reviewed the weather app and integrated network data requesting SDK of the third party and accepted the app and the given privacy statement.
	App Store	After the review, Digital Life was added to the App Store	After the review, AccuWeather was added to the App Store
Platform Policy	Platform Policy and Guidelines	Defined the rule to preclude a data sale for data accessed on Facebook	Indicated that provided APIs to access network data should only be used for network functionality

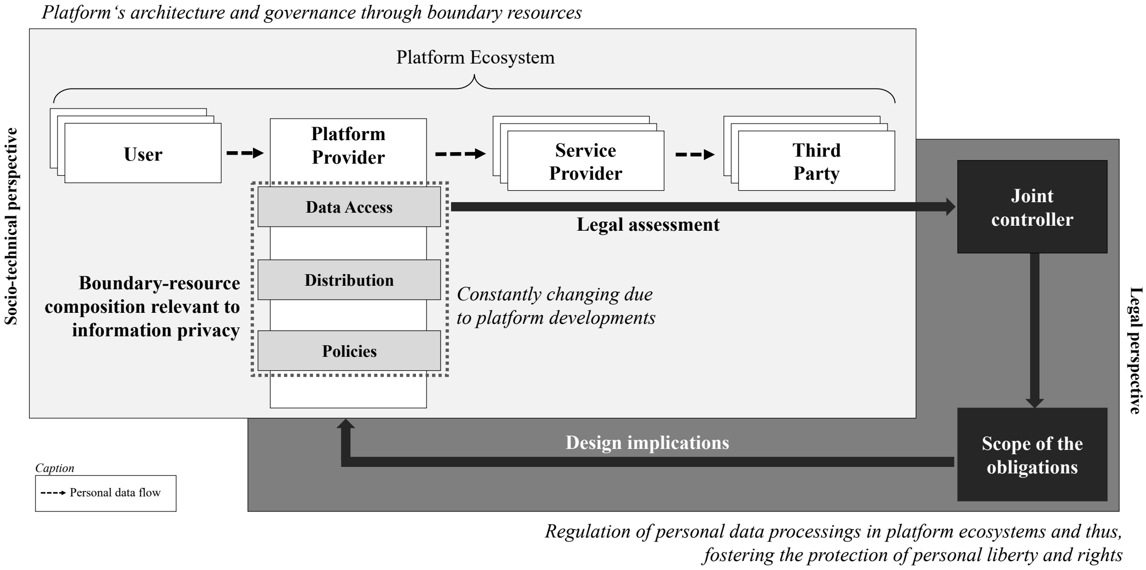
Apple has singularly determined and provided the means to process the data. Apple also determines the general purpose on a primary level by creating the possibility for the approved apps to access these data in the first place and gives service providers specific terms of use to sign, thereby specifying which purposes are allowed and which are not. The apps that violate the developer program license agreement are rejected and are not added to the App Store (Apple, 2019a). In some aspects, this ability to decide also distinguishes the degree of the openness of a platform, such as iOS, from a rather semi-open platform, like Android, where a user can freely install unverified programs. This level of involvement is still not typically associated with data controllers directly processing the user data.

Moreover, this involvement ends when the apps are approved for the app store and, for example, manage to gain a user's permission. Although the actions of different groups at the micro-level "appear to be disconnected, as each of them may have a different purpose," on the macro level, they can still be "pursuing a joint purpose or using jointly defined means" (European Commission, 2010, p. 20). This idea also applies to the ECJ's notion that, where several operators are jointly accountable, it is *not* required that they necessarily have access to the personal data concerned (ECJ, 2018). Therefore, Apple is classified as a joint controller of the data being accrued from the users' phones and also considering that iOS provided the platform that constituted the means for processing and consequently had the possibility of limiting the access.

16.7 Discussion

A central result of this study is the demonstration that the design of the boundary resources significantly influences unlawful personal data processing in a platform ecosystem, and thus, the accountability of a platform provider according to the GDPR. The boundary resources in their respective arrangements and interplay determine the platform provider's influence over the platform's behavior regarding the processing of personal data. As such, the boundary resources need to be considered to classify the role of platform providers as controllers. For example, controllership is unavoidable when the platform provider determines the only possible method of offering and using the applications and construes strict requirements for granting access to the applications. At the same time, the necessary level of influence can be retained if another boundary resource is designed more rigorously, such as in the case of Facebook, where the data are stored on the platform provider's own server.

Since such classification leads to a role burdened with various obligations, the next questions concerning the nature and extent of these obligations arise. It is important to closely examine the boundary resources at the individual level for two reasons. Firstly, because the threshold for allocating the joint controllership to a platform under the conditions mentioned above is relatively low, it is crucial to ensure that the extent of the conditions required of a platform provider depends on a detailed analysis of its unique possibilities. Therefore, the magnitude and the scope of obligation are contingent on the design of the boundary resources of data processing. For example, if iOS employs an open architecture to allow the installation of applications not offered in the App Store, their obligations would be lower. For a platform provider classified as a joint data controller, the degree of obligation follows from the platform architecture's design and the related boundary resources. Secondly, the joint controller obligations can be considered as normative requirements regarding the sensitive design of the specific boundary resources. The platform provider can be held accountable if the design decisions of the platform do not enforce the boundary resource consistently concerning user privacy. For example, when iOS asked for the users' permission regarding location data but still allowed access to other data that allowed the approximation, it can be considered as a breach of obligation. On another level, the results from assessing how joint controller obligations can be attributed in a flexible and scalable manner. The results can be used to circle back to the initial question of how open or closed a platform must be to classify the provider as a joint controller: The more flexible and scalable the obligations are, the lower the barrier for classifying even relatively open platforms as joint controllers.



Platform's architecture and governance through boundary resources
Platform Ecosystem
User
Platform Provider
Service Provider
Third Party
Data Access
Distribution
Policies
Legal assessment
Joint controller
Scope of the obligations
Design implications
Boundary-resource composition relevant to information privacy
Constantly changing due to platform developments
Socio-technical perspective
Legal perspective
Caption
Personal data flow
Regulation of personal data processings in platform ecosystems and thus, fostering the protection of personal liberty and rights

Figure 2. Relationship between Platform's Architecture, related Boundary Resource Composition, and the allocation of Controllership according to the GDPR.

In consequence, boundary resources can implement the functions of the operation of the platform providers on the platform and the regulation of the platforms by legal means. The architecture of a platform and the related manifestation of boundary resource composition (data access, distribution channel, and platform policy) affect user privacy. This composition is included in the core of the process, which involves the allocation of the legal controllership, determining the associated obligations, their scope, and the assessment of a possible breach of those obligations.

In Figure 2, it is shown that the relationship between the boundary resources, the controllership, and the obligations is reciprocal and interactive. The composition of the boundary resources can trigger controllership. The architecture and the design of the boundary resources then define the scope of the controller obligations. However, the exact scope of the obligations for platform providers depends on the individual case and must consider the platform provider's orientation and limitations. Here, cases such as the ones assessed earlier can offer valuable insights and help concretize the concept of the platform providers as joint controllers under the GDPR. Lastly, the specific controller obligations aim to efficiently influence the boundary resources' design to ensure user privacy. Thus, this cycle constantly fosters the protection of personal liberty and rights.

To summarise, we show with our socio-technical-legal analysis that platform providers can be subsumed under the joint controller role of the GDPR. Consequently, the platform providers must assume liability for the acts of data processing carried out by any groups and related actors within their platform ecosystems. Moreover, from an economic perspective, due to the potential scale of platforms, the penalties for any violations create a significant business risk for platform providers of up to 4% of the annual worldwide revenues (GDPR, 2016a, Art. 83 No. 5) for unlawful data processing. In both the analyzed cases, the platforms under consideration were composed of a closed architecture with a single distribution channel controlled by the respective platform provider. This finding suggests that using a closed architecture in a platform could generally lead to its classification as a joint controller.

Further analysis and discussion are required to determine the classification of platforms with a more open or hybrid architecture. In general, this can be confirmed, but it is observed that fewer obligations are required for this architecture. In addition, other platform understandings and related ecosystems such as Amazon Web Services (AWS) can be important for further investigations. In this context, several actors used artificial intelligence, which raised questions regarding the accountability of involved actors. Although various vulnerabilities and challenges are raised by artificial intelligence (Rodrigues, 2020), however, there are still actors behind artificial intelligence who develop or apply the technology and underly regulations such as the GDPR.

16.7.1 Implications for Practice

Platform providers should pay closer attention to the complex and continuous effort to balance generativity and data access limitations. Privacy-related motivations stemming from obligations derived from the GDPR or other legal frameworks can put more weight on the 'securing' side of the boundary resource rationale and lead the platform provider to design some resources in a more restrictive manner. Composition of the boundary resources that allows or even encourages unsanctioned acts or sends ambivalent signals regarding the constraints can increase their risk of violating legal obligations. Nevertheless, the inclusion of user interests and rights is very important must be considered.

In practice, platform providers must focus on the interplay of existing boundary resources to increase overall data protection. For example, platform providers can tune the data access boundary resource to better limit the processing activities to implement the platform policy or tune the app review process to verify whether an app's code falls within the regulations of the privacy statement. Potentially, it could also mean that entirely new boundary resources have to be created or enforced more rigorously when there are indications of evident misconduct by certain service providers or the third parties used by them. Because the obligations under the GDPR are sufficiently abstract and leave room for creative solutions by platform providers, they offer the potential to allow for innovation while still ensuring that the service providers and third parties maintain a privacy-friendly behavior.

While the GDPR applies to non-European companies only when processing data of the people within the EU (GDPR, 2016a, Art. 3 (2)), its effects as a role model for data protection legislation reach much further (Gordon & Ram, 2018). In 2018, California passed the California Consumer Privacy Act, a law heavily influenced by the GDPR (de la Torre, 2018). A platform provider that establishes a balanced composition of boundary resources can contribute to setting standards that are legally required. Conversely, in the long term, this approach can influence the definition and the range of constraints defined by the GDPR.

16.7.2 Implications for Regulation

The application of the law is not unilateral. The insights from the development of boundary resources facilitate the advancement of the legal understanding of the constituents of a controller and the obligations to be realized. The understanding of the boundary resources also aids in the legal assessment of the role of a given platform provider according to the GDPR. The realization that platform providers should be (joint) controllers regarding data processing acts carried out by other actors on a platform is not completely new (see, e.g. (European Data Protection Supervisor, 2018) regarding app stores). However, a systematic approach building on an established concept such as boundary resources has been missing so far.

Platform providers determine and control the general means of the processing of personal data through their platform by designing and tuning the boundary resources, such as APIs, that structure the means and constraints involved in the access of the specific types of user data by the services. Other types of boundary resources represent how platform providers influence the purposes for which personal data can be processed on the platform. An example is the process of vetting applications to certify that only those services adhering to the platform provider's rules, including those regarding access to personal data, are allowed on the platform.

A better understanding of the boundary resources concerning the dissemination of personal data helps platform providers assess GDPR-related risks. In the cases where a processing method, particularly one involving new technologies, is likely to result in a high risk to the data privacy of the users, the controller must assess the impact of the envisaged processing operations on the protection of personal data prior to processing the data (GDPR, 2016a, Art. 35). The type of analysis demonstrated in the case studies could help controllers identify the focal points for such an assessment, for example, the limits to the current set of boundary resources.

It is an important first step in concretizing and meeting notoriously abstract and unclear obligations stemming from the role of a controller by understanding the relationship between the architecture of the platform, the related boundary resources, and the level of control that the GDPR sets as the requirement for the classification of a group as a (joint) controller. For example, Art. 24 of the GDPR posits that controllers must "implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with [the GDPR]" (GDPR, 2016a). Considering the general risk-based approach of the GDPR (GDPR, 2016a), the extent of this obligation is particularly subject to the specific risk for the affected users. In addition, the general context of the data processing (in terms of what constitutes an "appropriate" measure) can vary. Furthermore, the scope of the obligation can be subject to the platform provider's overall influence and depends on the amount of risk for the user within the scope of the platform itself. Two important observations for regulation can be made based on the insight derived from the architecture and the composition of boundary resources of the platform.

Firstly, legal scholars and practitioners such as data protection authorities should consider the boundary resource literature to understand better the genesis and development of the boundary resources on the platforms. This knowledge can be helpful to elaborate on abstract obligations such as Art. 24 of the GDPR for specific actor groups such as platform providers and thereby help them understand their requirements, strengthening the user privacy in the platform ecosystems. While current EU framework proposals such as the Digital Services Act (DSA) (Commission, 2020) specifically address and obligate platforms concerning the lawfulness or diversity of the content they show and aggregate, no such classification and taxonomy exist for platforms in the field of data protection. More recent data protection proposals such as the ePrivacy Regulation (Commission, 2017) have the potential to change that but are still far from a final draft. Solid knowledge of boundary resources and their scientific background can therefore help provide a suitable definition for data protection-relevant platform providers and act as a starting point for filling their obligations with life. Secondly, as a benefit of the abstractness of the GDPR provisions, platform providers are generally provided with considerable leeway to satisfy their obligations. Essentially, the goal is fixed, but the method is not.

On the micro-level, adding privacy as a tool of analysis to the factors regulating the composition of a platform's boundary resources involves certain trade-offs that present an advantage to the platform providers. The boundary resources can be composed to realize a favorable scope of obligations by understanding the means by which the specific scope of obligations represents a specific composition. In certain cases, this can alter the composition to such an extent that a platform provider sheds its classification as a data controller and, by extension, its liability for potential privacy violations. The realization of the relationship between the boundary resources and the obligation scope grants platform providers a considerable amount of influence.

On a second, more macro level, establishing "good standards" of boundary resource compositions can shape the global understanding of those obligations. Therefore, the platform providers are encouraged to consider and understand the GDPR and its compliance mechanisms. Instruments such as codes of conduct (Art. 40 of the GDPR) or certification schemes (Art. 42 of the GDPR) could be used by platform providers to ensure the composition of boundary resources into sophisticated, compliant platforms and influence other platforms in the process.

Overall, the crucial contribution of the boundary resources for privacy-oriented regulation on platforms and the converse effects they can have on regulations when applied and designed in a privacy-conscious way is apparent. The controllership of the GDPR is triggered through a platform provider's influence on its platform, which is evident in the platform's architecture.

16.7.3 Implications for Research

This study shows that a platform ecosystem design can have essential effects on users' privacy. Privacy regulations, such as the GDPR limit the flexibility of the platform providers in designing the boundary resources in platform ecosystems (Eaton et al., 2015). In this regard, providers must understand the regulations' goals and functioning and their obligations to produce a platform that meets these constraints beyond their own strategic goals.

We have not been able to source internal data from Facebook or Apple that address the uncertainties involved in processes of platform boundary design. In this context, studies with the support of platform providers can enable a deeper understanding. However, the methodological challenges of gaining access to empirical data in exploring platforms are known and difficult to solve (de Reuver et al., 2018). Moreover, the study relied on the two cases documenting the privacy violations over the exclusive platforms of Facebook and Apple's iOS and on the GDPR as a legal framework. Thereby, a similar analysis of other cases in other platform ecosystems and the consideration of other data-protection legislation can benefit research, practice, and regulation. Starting with cases that demonstrate the basic premise was the crucial first step that helped establish the relevant criteria and draw a first, albeit very wide, line of when they are met. Following up with cases involving smaller, less powerful platform providers will be the necessary next step toward approaching a more precise scope of those criteria.

In line with de Reuver et al. (2018), other studies should also consider the boundary resource concept as a unit of analysis for information privacy in the context of highly distributed arrangements (Eaton et al., 2015; Yoo, Henfridsson, & Lyytinen, 2010). As this study has been focused on two platforms with closed architectures, it is yet to be determined whether platforms with an open or hybrid architecture (Constantinides et al., 2018; de Reuver et al., 2018) can and should be classified as joint controllers as well. Considering the flexibility of many obligations and the nature of controllership as connected to specific processing activities, such a classification, combined with a smaller scope of obligations and a limitation to a specific set of processing activities by the service providers and third parties, would be feasible. Further research is required to understand the relationships in this regard.

16.8 Conclusion

In the platform ecosystems, the platform providers act as gatekeepers and intermediaries that define and set the rules for personal data flows through the platform. However, determining the means of data processing is constrained by accountability and obligations according to the GDPR. In the case of Facebook, media coverage and our assessment identify Facebook as the major party accountable for ensuring data protection. The other important factor is Apple's role as a joint controller within the scope of its iOS platform. In tuning its boundary resources via iOS 13, Apple has introduced fine-grained user configuration options regarding the usage of location data by apps (Apple, 2019b). In addition, this update includes API changes that prevent apps from approximating a user's location using other data without consent (Apple, 2019b). These refinements indicate the ability to enforce personal data access limitations by tuning existing boundary resources.

From a regulatory point of view, this type of analysis at the intersection of information systems research and law contributes to the debate about the protection of privacy in platform ecosystems under the regulatory scheme of the GDPR in three ways: Firstly, it helps those who apply the law to substantiate the definitions and the obligations under the regulation. Secondly, it supports the application of rules in specific cases. Lastly, it supports controllers in assessing the risks and the obligations.

Summing up, the results of this article demonstrate that platform providers play a significant role in the protection of personal data. The platform's architecture and the related boundary resources are objects for the regulation through and of platforms. They fulfill the functions of the interactions enabled by the platform providers on the platform and the possibility of regulation of platforms and personal data flows and, thus, the protection of personal liberty and rights in such socio-technical systems.

16.9 References

AccuWeather. (2017). Privacy Statement. Retrieved from https://web.archive.org/web/20170831185056/https:/www.accuweather.com/en/privacy

Albright, J. (2018). The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle.

Apple. (2017a). Apple Developer Program License Agreement. Retrieved from https://download.developer.apple.com/Documentation/License_Agreements__Apple_Developer_Program/Apple_Developer_Program_License_Agreement_20180604.pdf

Apple. (2017b). iOS 7: Understanding Location Services. Retrieved from https://support.apple.com/en-en/HT201357

Apple. (2017c). What's New in iOS - iOS 7.0. Retrieved from https://developer.apple.com/library/archive/releasenotes/General/WhatsNewIniOS/Articles/iOS7.html

Apple. (2018). Turn Location Services and GPS on or off on your iPhone, iPad, or iPod touch. Retrieved from https://support.apple.com/en-au/ht207092

Apple. (2019a). App Review. Retrieved from https://developer.apple.com/app-store/review/

Apple. (2019b). iOS 13 Preview. Retrieved from https://www.apple.com/ios/ios-13-preview/features/

Baldwin, C. Y., & Woodard, C. J. (2009). The architecture of platforms: A unified view. *Harvard Business School, 32*.

Opinion C-210/16 Rt.47 (2018).

Butts, J. (2017). Thanks to Misuse, Apps Can't View MAC Addresses on iOS 11. Retrieved from https://www.macobserver.com/news/product-news/apps-cant-view-mac-addresses-on-ios-11/

Cadwalladr, C., & Graham-Harrison, E. (2018). How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. *The Guardian, 18*.

Commission, E. (2017). Proposal for a Regulation of the European Parliament And of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

Commission, E. (2020). Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive. 2000/31/EC: European Commission Brussels, Belgium.

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*.

de la Torre, L. (2018). GDPR matchup: The California Consumer Privacy Act 2018. Retrieved from https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: a research agenda. *Journal of Information Technology, 33*(2), 124-135.

Eaton, B., Elaluf-Calderwood, S., Sorensen, C., & Yoo, Y. (2015). Distributed tuning of boundary resources: the case of Apple's iOS service system. *MIS Quarterly, 39*(1), 217-243.

ECJ. (2018). C-210/16: ULD *European Court of Justice 2018* (June 08).

European Commission. (2010). *Article 29 Data Protection Working Party* Retrieved from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

European Data Protection Supervisor, E. (2018). *EDPS record of processing activity*. Retrieved from https://edps.europa.eu/sites/default/files/publication/37_gdpr_mobile_app_en.pdf

Facebook. (2018). Facebook Response to National Association of Attorneys General. Retrieved from https://consumer.sd.gov/docs/facebookResponse_05-09-2018letter.pdf

Frenzel, E. (2018). DS-GVO Art. 5 Grundsätze Für Die Verarbeitung Personenbezogener Daten. *DSGVO BDSG*.

Frier, S. (2018). Facebook Says There May Be More Cambridge Analytica-Sized Leaks. *Bloomberg*.Retrieved from https://www.bloomberg.com/news/articles/2018-04-26/facebook-says-there-may-be-more-cambridge-analytica-sized-leaks

GDPR. (2016a). General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Directive 95/46). *59*, 1-88.

GDPR. (2016b). General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *59*, 1-88.

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: the boundary resources model. *Information Systems Journal, 23*(2), 173-192.

Gordon, S., & Ram, A. (2018). Information wars: How Europe became the world's data police. Retrieved from https://www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8

Hagiu, A., & Wright, J. (2015). Multi-sided platforms. *International Journal of Industrial Organization, 43*.

Hartmans, A. (2018). It's impossible to know exactly what data Cambridge Analytica scraped from Facebook. Retrieved from https://www.businessinsider.com.au/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2019). Digital platform ecosystems. *Electronic Markets*, 1-12.

Jirotka, M., & Stahl, B. C. (2020). The need for responsible technology. *Journal of Responsible Technology, 1*, 100002.

Kaplan, B., & Maxwell, J. A. (2005). Qualitative research methods for evaluating computer information systems *Evaluating the organizational impact of healthcare information systems* (pp. 30-55): Springer.

Karhu, K., Gustafsson, R., & Lyytinen, K. (2018). Exploiting and defending open digital platforms with boundary resources: Android's five platform forks. *Information Systems Research, 29*(2), 479-497.

Kogan, A. (2018, 16.04.2018). Written evidence submitted by Aleksandr Kogan. *Digital, Culture, Media and Sport Committee - UK Parliament.*Retrieved from https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Written-evidence-Aleksandr-Kogan.pdf

Martini, M. (2018). Art. 28. Beck'sche Kompaktkommentare BDSG - DSGVO.

McCausland, P., & Schecter, A. R. (2018). Cambridge Analytica harvested data from millions of unsuspecting Facebook users. Retrieved from https://www.nbcnews.com/news/us-news/cambridge-analytica-harvested-data-millions-unsuspecting-facebook-users-n857591

Paré, G. (2004). Investigating information systems with positivist case research. *Communications of the Association for Information Systems, 13*(1), 18.

Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You: WW Norton & Company.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 977-988.

RevealMobile. (2017). RevealMobile Website. Retrieved from https://revealmobile.com

Ribas, C. (2017). The Accuweather Situation Is Really An iOS Privacy Problem. Retrieved from https://medium.com/@carlosribas/the-accuweather-reveal-situation-is-really-an-ios-privacy-problem-78e85a6f8539

Rodrigues, R. (2020). Legal and human rights issues of AI: gaps, challenges and vulnerabilities. *Journal of Responsible Technology, 4*, 100005.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018a, 17.03.2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018b). How Trump Consultants Exploited the Facebook Data of Millions. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Schreieck, M., Wiesche, M., & Krcmar, H. (2016). *Design and Governance of Platform Ecosystems-Key Concepts and Issues for Future Research.* Paper presented at the Proceedings of the European Conference on Information Systems (ECIS).

Sherr, I. (2018). Facebook, Cambridge Analytica and data mining. Retrieved from https://cnet.co/2Vx3ITh

Strafach, W. (2017). AccuWeather iOS app sends location information to data monetization firm.

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research, 21*(4), 675-687.

Van Alstyne, M. W., Parker, G. G., & Choudary, S. P. (2016). Pipelines, platforms, and the new rules of strategy. *Harvard Business Review, 94*(4), 54-62.

Vedder, A., & Naudts, L. (2017). Accountability for the use of algorithms in a big data environment. *International Review of Law, Computers & Technology, 31*(2), 206-224.

WashingtonPost. (2019). Transcript of Mark Zuckerberg's Senate hearing. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing

Whittaker, Z. (2017). AccuWeather caught sending user location data, even when location sharing is off. Retrieved from https://www.zdnet.com/article/accuweather-caught-sending-geo-location-data-even-when-denied-access/

Yin, R. K. (2009). Case Study Research: Design and Methods SAGE.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. *Information Systems Research, 21*(4), 724-735.

Zuckerberg, M. (2018). Testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook. (Hearing before the United States House of Representatives Committee on Energy and Commerce).

17 Article No. 9 (Kurtz et al. 2022)

Kurtz, C., Vogel, P., and Semmann, M. Exploring Archetypes of Value Co-Destructive Privacy Practices. Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS), Hawaii (USA), 2022.

Abstract

Personal data is a critical resource to tailor digital services to the context of use and the preferences of individual users. Services have the characteristic that users and providers no longer interact in a dyadic relationship but rather in service systems co-creating value. Here, actors can provoke adverse effects that result from misaligned or destructive behavior. In service research, value co-destruction emerged as a perspective to study such undermined value co-creation. We use this lens in the case of information privacy as an example of a normative value. Building on a multi-case analysis of information privacy violations reported in the news, we elucidate seven archetypes of value co-destruction. These archetypes enable an understanding of underlying conceptions and mechanisms of actor arrangements that inhibit the holistic consideration of normative values such as information privacy in digital services.

17.1 Introduction

Processing data relating to an individual is often an essential resource for providing smart services that reflect the context of use (e.g., locations) and the individual user's preferences. However, today's digitized services have the characteristics that users and providers interact no longer in a dyadic relationship but in service systems with multiple actors. Such multi-actor service encounters make use of personal data in the service's value co-creation (VCC) process. VCC can be understood as a general concept encompassing various occurrences in which companies and customers generate value through interaction [1]. For the term *value,* diverse approaches and conceptualizations exist in the literature [2, 3]. Value can be the result of an exchange in a joint service process [4]. Here, value is subjective and relies on the perception of the beneficiary [5]. Given this understanding, value can be increased by joint endeavors but likewise be reduced [6].

Given the example of digital services, service providers can involve third parties which offer manifold possibilities to further improve the value for the customer by integrating their resources in the value co-creation process. Examples are application performance monitoring services to ensure that an app runs smoothly or the actor integration for advertisement enabling the offer of the services to the customer free of charge. Here, the growing number of connected actors can generate, communicate, share, and access personal data [7, 8]. A broader set of actors involved in the service's VCC process goes hand in hand with the potential for the exchange and misuse of personal data. This can inflict harm to the normative value of information privacy. To explore this issue, we make use of value co-destruction (VCD). This concept emerged as a lens to investigate a failed co-creation due to the misaligned or destructive behavior of involved actors [5, 6, 9]. Thus, VCD can be understood as the decline at least for one actor's well-being in interaction [6]. This work addresses the research question: *Which resource integration patterns lead to value co-destruction violating information privacy?*

We use a multi-case analysis to identify archetypes of resource integration patterns (RIP) that led to information privacy violations. This enables two contributions: first, it builds the basis for identifying patterns in service systems to find future ways to design and regulate privacy in services. Second, the current understandings of the concept of VCD can be extended by the consideration of a normative value. The decrease of well-being is the typical facet and result of value co-destruction. The violation of a normative value can have social consequences besides reducing well-being for an individual actor since the normative value can be classified as worth protecting for a society. Human norms –also referred to as institutions in service research [10]– enable and constrain action and make social life meaningful. Interrelated sets of institutions constitute an assemblage of institutional arrangements [10]. Mustak and

Plé [11] emphasized that actors might have divergent understandings of institutional arrangements [12, 13], and the consequences remain relatively unknown, as a typical assumption in service research is a shared understanding of institutions [11]. Thus, if different understandings regarding information privacy exist, this can, in consequence, promote VCD.

We start in the following section by introducing the theoretical foundations of VCC and VCD, service systems, and information privacy. Next, we describe our research approach. Afterward, we discuss the identified archetypes and elaborate on the findings of our study. We conclude with a summary of the results and an outlook.

17.2 Theoretical Foundations

17.2.1 VCC and VCD in Service Systems

Service encounters have shifted from the traditional dyadic interaction of an individual and a service provider towards service systems [14]. This shift triggered service research to change the perspectives and to consider service systems [15]. According to service logic, the joint resource integration and utilization in configurations of people, technologies, and other entities create value [16-18]. Here, different configurations may be apparent [19, 20]. VCC and VCD can be considered based on different levels of abstraction, from the service ecosystem, characterized as relatively self-contained and self-adjusting systems of resource-integrating parties [14, 21], to the processes of engaging individual actors [22]. In this regard, the perspective on service systems allows studying the resource integration among actors [23] in service ecosystems.

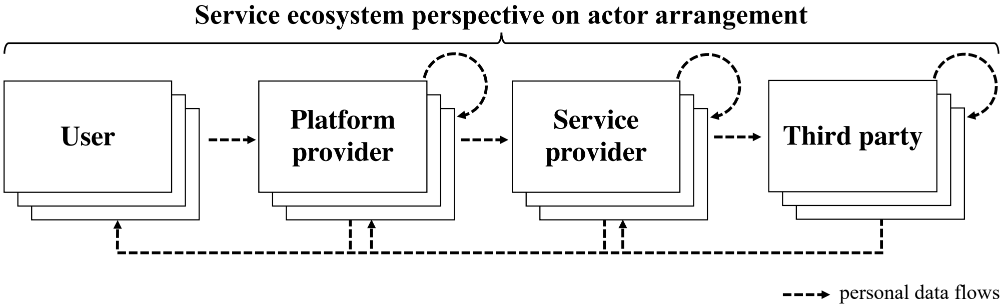


Figure 1. Simplified service ecosystem perspective (based on Kurtz et al. (2018) [24])

In service systems, individuals as users integrate resources, often in the form of personal data. A RIP can be defined as a "distinct combination of the changing set of actors with various dispositions, the multitude of engagement platforms and the engagement properties resulting from various activities"

[22]. Platforms can set the framework for multi-sided interactions between actors [15, 25]. Platform providers interpose themselves between individuals and service providers [19, 20]. Platforms can be defined as a set of digital resources that enable interactions between the actor groups of individuals and service providers [26]. Platforms provide resources such as an operating system or an app store that offer the possibility for value-creating interactions [25]. Here, service providers offer their services via the platform to users in the form of e. g. applications. Examples are Google Maps on the platform of iOS or Cundy Crush Saga on Facebook. Moreover, third parties are involved in service systems, typically not visible for a user in interaction. Especially, service providers involve (third) parties for reasons such as performance management, cloud infrastructure, analytics, or advertisement. A configuration of multiple actors in a service system leads to a broader set of actors that can access personal data compared to the traditional, dyadic interaction (Figure 1, very simply presented, technologies, rules, etc., not included in the figure).

In versatile services, actors and their actions are not necessarily visible or even understandable for users [27]. In addition, VCC implies an optimistic ideal that is unrealistic due to VCC failures [9, 28]. The accessibility of resources, the matching or mismatching of resources, and whether a resource can be turned into benefits through operations contribute to VCC or VCD. Thus, VCD can be caused in the interaction process of co-creating actors, resulting in at least one actor with a decline of value [5, 6, 18, 29, 30]. In VCD, one actor integrates and/ or applies the resources (of the other actor) in a way that is not expected or appropriate from the view of the other actor [18]. Such actions can be intended or unintended [6]. For example, in a situation of intended co-destruction, one actor misuses the available resources of the second actor and tries to gain more benefit. This misuse may result in customer loss, dissatisfaction, or a negative firm's image.

Lintula, Tuunanen and Salo [18] developed a framework on VCD ordered into three key categories ‘orientation', 'resources,' and ‘perceptions.' The category 'orientation' includes on the one side whether the VCD was intended in e. g. motivated by opportunism [30] or not intended [6]. On the other side, actors' goals in the co-creation process are addressed, which can be incongruent due to e. g. information asymmetry [31]. The ‘resource’ category is divided into four sections. Reduced well-being in VCD for one actor can be driven by a 'lack of resources' [6]. In the situation of 'misuse and non-integration of resources,' available resources are misused in the interaction process [6]. The third classification, 'loss of resources,' describes an actor's exceeded loss of resources [32]. These classifications may result in the ‘attempt to restore resources’ losses [32]. The category 'perception' considers inconsistencies in expectations regarding the interacting actors [33, 34]. The first classification, 'expectations,' refers to the actor's expectation regarding the interaction outcome. A VCD can be indicated in case an expectation is not met [33, 34]. Second, 'insufficient perceived value' refers to the circumstances that an expected value is not met based on a previous value experience [35]. Third, the 'incongruence of practices' in procedures, understandings, or engagements can result in VCD. Fourth, 'contradictions of value' specifies that the value for actors diverges. The interaction can create value for one actor and destruct value for another actor [6]. In addition, reasons for VCD from the provider's perspective have been investigated, which can be divided into the absence of information, an insufficient level of trust, mistakes, an inability to serve, an inability to change, the absence of clear expectations, customer misbehavior and blaming [36].

Companies are involved in VCD, both intentionally and unintentionally, which can lead to negative reporting or negative attitudes of customers towards the company. Especially in the case of non-intentional involvement, companies need to understand what is not happening in service systems according to their expectations and institutional arrangements to prevent such behaviors. Recently, new interdisciplinary studies considered VCD in service ecosystems. Examples are the investigation of actors' opportunistic behavior or business model challenges that lead to VCD in the business-to-business context [37], socially, environmentally, or economically undesirable effects in the sharing economy [38], or the imbalances within smart city ecosystems [39].

"Shared" institutional arrangements among actors have not to be the case [11]. Divergent interpretations of institutional arrangements can induce inferior value experiences or the actors [11, 12]. Such consequences can be observed in tourism ecosystems, in which tourists often have different values and norms than local residents [11, 13]. In the following, we want to lay down the foundations for investigating information privacy in digital service systems.

17.2.2 Information Privacy

Actors in service provision can make use of the quantitative changes in the amount of personal information that can be collected, the speed at which personal data can be exchanged, and the qualitative factor in types of information that can be acquired [7]. In this relation, the assumption that users in service systems have transparency and clarity to build an expectation needed for consent to privacy policies is questionable. The limited expectation of users about their data resource integration is often status quo, which intensifies with the growing number of actors that interact in a single service system [40]. Given the case of eBay, about 1,000 third parties are involved and may collect personal data [40]. Research points out that users perceive negative consequences when external actors assess their personal information and thus provoke information privacy protection [41].

In the last decades, two conceptualizations of information privacy were predominant in the literature [7]. First, the understanding of privacy as "restricted access" postulated that one has information privacy when a user can restrict the access of others to one's personal information. On the other hand, understanding information privacy as "control" postulated that one has privacy when one has control over information about oneself [7]. Due to shortcomings of both understandings in the face of upcoming practices on personal data led Nissenbaum [42] develop a new understanding of information privacy as contextual integrity. The main idea behind this approach is that, in order not to violate the information privacy of an individual, information flows must be appropriate. Thus, a data flow is appropriate because it represents a balance of diverse interests and societal and contextual ends and not because it favors the interests of an actor above all others [8]. Following this conceptualization, we investigate cases in which actors' institutional arrangements regarding information privacy have not been consistent and complementary and thus, led to VCD.

17.3 Methodology

In this article, we conduct a multi-case analysis [43] to explore the VCD of actors in service systems that lead to individuals' violation of information privacy. The methodology is deemed appropriate for investigating contemporary events and particularly suitable for research at an early, formative stage [44]. Based on the case analysis, we utilize archetype building to systematically classify VCD actors' arrangements that violate information privacy and further attempt to understand the change mechanisms (i.e., how they occur). Archetypes build a basis for the systematic description of RIPs in their structural arrangement [45]. Existing studies investigate patterns or sets of structures and explore organizational archetypes [45]. Thus, identifying archetypes set the basis for a subsequent theory-driven investigation of configurations and their inherent dynamics by opening new avenues [46].

According to Yin (2009) [44], the usage of news articles published in mass media or community newspapers can serve as sources of evidence. Thus, we draw on news articles as primary data to analyze cases, as these provide a rich basis of empirical evidence and enable studying complex phenomena. In detail, new articles report on the opinions or claims of affected individuals, researchers, businesses, regulators, and others [47]. In addition, we added further data in the form of technical investigations or posts. In this regard, the review of secondary sources, such as media articles or supplementing documents, is common to identify archetypes and changes among archetypes [45]. News articles enable empirical access to the phenomenon of information privacy violations. Often, actors and violations of information privacy are hidden [8]. News articles reporting information privacy violations make practices transparent and, thus, examinable.

To methodologically substantiate the case identification process, we adopt the taxonomy development process by Nickerson et al. (2013) [48]. This widely used approach enables a structured, iterative process for us to identify cases. In this regard, this process has already been considered purposeful in IS research in different ways for archetype building [49-51]. As an object of interest, our case meta-characteristic and case selection criteria report an information privacy violation and a resource integration of at least two actors. In the identification of cases, we proved whether a news article matched our meta characteristic. If this was the case, we screened the news article and identified the respective RIP in this case. If the actor-configuration of the RIP was not considered in our case database, an in-depth case analysis (cf. table 2) followed. When the actor-configuration of the RIP has already been considered, we did not include the news article. We proceeded, as the focus of this study was on the identification of diverse RIPs [45]. Our ending condition results from the permutations of potential RIPs of platform providers, service providers, and third parties that could co-destruct value in digital services [45, 48]. We carry out this process until no further permutation is found or the ending condition is reached when all actor permutations are covered.

Table 1. Cases reporting privacy violations.

Case No.	Description	Link
1	Amazon’s smart speaker Alexa makes unexpected recordings	nyti.ms/2IBbF93
2	Android makes location data accessible for Google apps	zd.net/35BfEuG
3	Smart TVs install tracking software ex-works	nyti.ms/36IhzNB
4	Facebook app accesses call and message data on Android	zd.net/3pExDby
5	Weather app and third-party track user locations	zd.net/2IIZSW5
6	Facebook SDK accessed device data by integration in Zoom	zd.net/32Tzz6u
7	Facebook and Cambridge Analytica data scandal	nyti.ms/3nxaUwf

We started to search for the keyword "privacy" on the mass media website of the New York Times and limited the publication year of the article to 2018. This broad keyword was used in order not to exclude articles that would have been the case for "privacy violation" or "information privacy." With a worldwide readership, the New York Times was identified as a data source due to its privacy project, an ongoing examination of privacy. The ending condition was not reached on the mass media website of the New York Times, and we considered the technology news platform zdnet.com to extended the data source from mass media to a technology-centered source. We again searched for the keyword “privacy” and considered our meta characteristic and articles published since 2017. In the following, we reached the ending condition. Table 1 gives a case overview, sorted by the closeness of an actor in interaction with a user in a service system.

After the case identification, we enriched the data material for each case by conducting backward searches. Table 2 gives an overview of the variety of documents and corresponding numbers per case. Here, the usage of diverse sources and material to the same case enables data triangulation and improves the validity of our findings [43]. In the further course, these documents that include various statements and opinions by practitioners or affected users helped characterize the different archetypes (see result section).

Table 2. Documents per Case.

Case No.	1	2	3	4	5	6	7	Σ
Documents								
News articles	5	5	1	6	2	5	10	34
Studies, reports, blogs, discussion boards, and further informing websites		1	2	1	2			6
Actor documents (incl. help websites, company blog articles, privacy policies, mails)	1		1	5	2	2	1	12
Videos and screenshots	1		1					2
Legal documents by commission offices or charges		1	1				1	3
Σ	7	7	6	12	6	7	12	57

17.4 Multi-Case Analysis

In the following, we describe and analyze the identified cases that reported information privacy violations in different RIPs.

17.4.1 Amazon's Alexa Makes Unexpected Recordings

In the first case, the news report indicated that the smart speaker of the platform provider Amazon recorded a customer in daily life [52] (cf. Figure 2). Amazon declared that the device's virtual assistant, called Alexa, mistakenly heard a series of requests and commands to send the recording as a voice message. According to the customer, the smart speaker did not request permission to send the data. The case documents indicate that the case is not the only case for information-privacy violating smart assistants and other criticized practices [52].

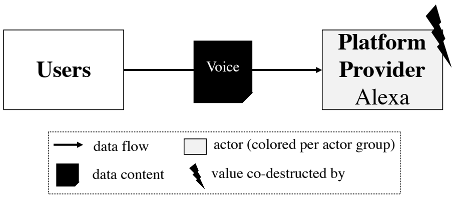


Figure 2. Case 1: VCD in the service system.

As a result of the VCD process in this case, which also applies to all following cases, the user has a negative value outcome by violating information privacy. According to Amazon's statement, the value was not increased for the company since the VCD was not intended. However, the case pointed out that a platform can have a crucial role due to the technical data interface design to the user. Such a role has a notable sensitivity for information privacy since a platform provider takes an influential role that enables predefine mechanisms and, thus, to be able to react to value co-destructive behaviors in service systems.

17.4.2 Android Makes Location Data Accessible for Google Apps

Google's both, as platform provider of Android and as the service provider of apps such as Google Chrome, collected individual's location data [53] (cf. Figure 3). In detail, even if the user rejected to share location data on the mobile device platform, Android enabled Google applications to access and send individual’s location data to Google servers [53]. A referenced study compared an Android phone with the web browser Google Chrome active in the background and an iPhone with Safari but not Chrome [54]. After 24 hours, the report states that the Android device sent 900 data samples to Google's servers, 340 times consisting of location data [54].

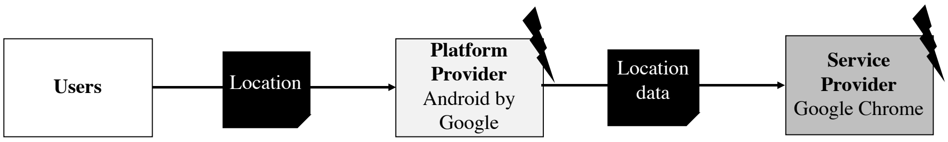


Figure 3. Case 2: VCD in the service system.

This case demonstrated an intended VCD by Google. By accessing location data via apps, the company can infer diverse information about an individual–where the individual works, sleeps or goes shopping. These data increase the accuracy of Google's advertisement, and thus, while violating information privacy, this process increases the value for Google. A particularity, in this case, is that Google is involved in two different actor groups: Google makes use of its role as a platform provider of Android and as a service provider of Chrome.

17.4.3 Smart TVs Install Tracking Software

The third-party software Samba TV is integrated into smart TVs to recognize and track any show viewed, any advertisement that appeared, or any game played on a TV [55] (cf. Figure 4). When an individual sets up such a smart TV, a screen appears to enable Samba Interactive TV service. The service is recommended in these statements by its recognition of onscreen content. On this basis, targeted ads are possible.

The company Samba TV offers organizations the ability to customize their targeting on the media outlets people watch, such as ads based on an individual's conservative or liberal direction [55]. One of Samba TV executives stated that at the end of 2016, more than 90 percent of people opted in using the service [55]. The director of the consumer privacy and technology policy group and a former policy director of the Federal Trade Commission stated that "[i]t’s still not intuitive that the box maker or the software embedded by the box maker is going to be doing this” and desires that “companies do a better job of making that clear and explaining the value proposition to consumers” [55]. Due to these information privacy violations, two senators encouraged the respective federal regulation to investigate the case. The senators claim that companies are tracking viewing behavior presumable without the knowledge of individuals.

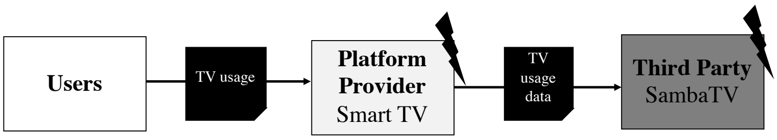


Figure 4. Case 3: VCD in the service system.

In this case, smart TV providers intendedly involved the third-party software Samba TV. This led to an increased value for both actors but value destruction for the user. Compared to the following case in which a service provider integrates a third party, a special virulence is evident. Here, the platform provider can control the direct data access to the user. If an actor co-destructs value at this point (of a platform) in the service system, this can lead to major impacts for all other RIPs in which a platform is apparent. This issue leads to a set of information privacy violations, where the platform is an intermediary between user and service provider. In detail, the case describes that personal viewing data is collected across the service system, of any show viewed, any game played, or any app used.

17.4.4 Facebook Accesses Call and Message Data

The Facebook app installed on the device platform Android enabled Facebook access to the user's phone calls and text message metadata [56] (cf. Figure 6). On Android, Facebook easily pulled down the data by using the platform's API (application programming interface) [56]. Facebook stated that “When [the user] sign[s] up for Messenger or Facebook Lite on Android, or log[s] into Messenger on an Android device, [the user is] given the option to continuously upload [the] contacts as well as [the] call and text history” [56]. However, the reporter notes that a differentiation should be considered between contacts and calling and texting metadata [56]. If a user has granted permission to access contacts on Android during an app installation once, specifically before version 4.1, this permission gave an app continuous access to call and message logs by default.

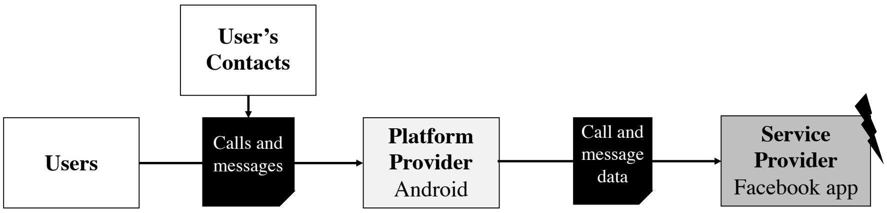


Figure 6. Case 4: VCD in the service system.

Compared to the previous case, the platform provider does not destruct the value by an information privacy-critical action. Instead, in the service system, value is co-destructed by the unexpected practice of Facebook to collect the data accessible on the device platform. As also the second case demonstrated, personal data collection increases the value, in this case for Facebook, due to the enhancement of targeted advertisement. This goes with the violation of information privacy and the criticism of the accessibility of data from android devices.

17.4.5 Third-Party in App Tracks User Locations

The app's service provider, AccuWeather, implemented the third party RevealMobile [57] (cf. Figure 7). On iOS, this third party accessed the user's currently connected Wi-Fi router name, the BSSID (Basic Service Set Identification which is the MAC address of the connected wireless access point), and the Bluetooth status [58]. An IT security consultant tested this transmission in which data was sent 16 times in 36 hours to the backend service [58]. The organization used these data to identify the user's location by enriching the data with public databases about wireless access points and their precise locations. In the next step, these location data were used to create audience data for mobile marketing. This procedure seems critical for users who previously deactivated the settings of the application's access to their location [58]. Apple declines any misuse of network data and bypasses user settings, e.g., to track user's Wi-Fi network data to determine the location if the location access has been disabled.

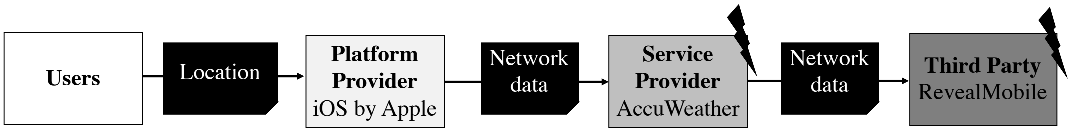


Figure 7. Case 5: VCD in the service system.

In this case, the joint VCD of a service provider a third party leads to a violation of information privacy for the user. The location settings have been bypassed by the access to network data. The case shows that although measures were taken by the platform provider through agreements that prohibit the usage of such network data, this directive was not technically enforced, and data access was possible. As in the other cases, the values for the value co-destructive actors of service provider and third-party increase while the privacy-violating action in the co-destructive process has a negative impact on the user and the bypassed platform restrictions.

17.4.6 Facebook SDK Accessed Device Data by Integration in Zoom

A privacy violation occurred in the context of the iOS app of the videoconferencing tool Zoom [59] (cf. Figure 8). In detail, the app integrated the SDK of Facebook that enabled users to log in with their Facebook account [59]. However, Facebook accessed data included the operating system type and version, IP address, the iOS Advertiser ID, the device model and carrier, screen size, processor cores, and disk space [59]. Zoom-founder Eric Yuan criticized that Facebook's SDK collected device fingerprinting information that is unnecessary for Facebook [60]. This lead to the removal of Facebook's SDK in the Zoom app.

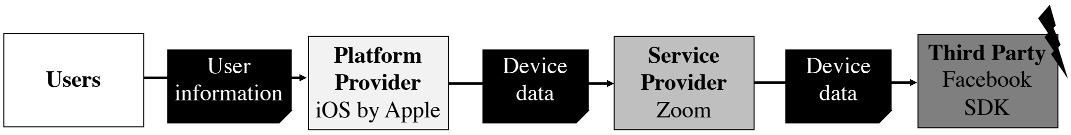


Figure 8. Case 6: VCD in the service system.

In this case, the third-party plugin by Facebook intentionally accessed personal data by using the involvement in a service provider's app. In comparison to the fourth case, Facebook co-destruct value not in the role as a service provider but instead as a third-party. However, in contrast to the previous case, the service provider did not intentionally integrate the third party to increase the value for both actors. Instead, the integration of the Facebook plugin by Zoom was originally intended to create value for the customer.

17.4.7 Cambridge Analytica Data Scandal

The developer, Aleksandr Kogan, built the personality quiz app This Is Your Digital Life (TIYDL) on the Facebook platform (cf. Figure 5). However, the terms conflicted with Facebook's platform policy for developers. Despite this conflict, the application passed Facebook's app review process. When installing and using the application, users had to accept the requested data access by the app along with the app's terms of service. By accepting these conditions, users allowed the app to access their data and the data of their Facebook friends [61]. This access was possible due to the far-reaching design of the data access defined by the platform provider Facebook. Whereas the users consciously using the app were asked to accept the app's terms, and by this act consent to its processing, the user's friends were not asked directly and had no chance to refuse. Instead, Facebook implemented the option of letting the app access the personal data as an option within the profile settings of the users' friends and kept it activated by default [61]. Many users' friends did not do that, resulting in Facebook allowing the app to access the friend's user data. Here, the data access implementation led to unveiling the data of 87 million Facebook users to TIYDL, where 270,000 of those had actively used the app. After that, TIYDL did not comply with the platform provider's policy to share accessed data via the platform. The app provider shared the data with Cambridge Analytica, which used it to target users on Facebook for individualized advertisement.

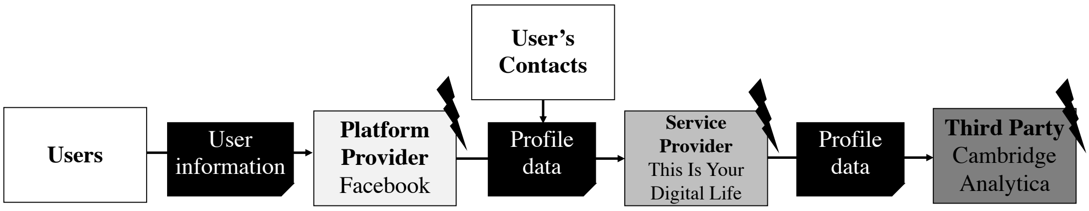

User's Contacts
Users
User information
Platform Provider Facebook
Profile data
Service Provider This Is Your Digital Life
Profile data
Third Party Cambridge Analytica

Figure 9. Case 7: VCD in the service system.

In this case, we have a service system in that all three actor groups of platform, service provider, and third party have been involved in the VCD. In comparison to the other cases with a platform provider involvement in the co-destruction, the platform provider Facebook did not provide a device platform in this case. This limits the extent of the potential data interface to the user compared to the previous cases. However, the same problems were apparent where the data access by a platform provider was designed to the detriment of the user's information privacy. While value was co-destructed for the user, Facebook increased its value by extensive data access towards app providers, attracting them to get on the platform. This was reflected in the data access that an app provider could access both the app user's data and the data of the app user's friends. This was supported by the fact that this data access was activated by default in Facebook's user settings. TIYDL increased the value by sharing the data with Cambridge Analytica. The company Cambridge Analytica misused personal data to infer analytical insights for political advertisement and thus, increased its value through the influence on the presidential election. Further, Facebook increased its value by receiving money from Cambridge Analytica to display users' targeted ads.

17.5 Results

Our case analysis provides insights about VCD in service systems. VCC implies an optimistic ideal for RIPs. Diverse value co-destructive RIPs emerge relating to a service system. Reasons are that at least one actor violates information privacy by integrating –intended or unintended– of user's data in the value co-destructive process that was not expected or appropriate from a user's perspective. Here, not only the loss of resources is a consequence of VCD [9, 18, 62], but also a violation of human values that are classified as societal important and to be protected. In sum, seven archetypes of RIPs that violate user's information privacy become visible in our study (Table 3).

In the archetypes I – III and VII, a platform provider is involved in a VCD that implies privacy violations. The positioning of a platform in a service system involves designing the main data access to the user. If a platform provider offers a device platform, this is further strengthened by the fact that the technical device interface to data access is designed. No actor group can act as a corrective in these archetypes. Since the platform provider has no incentive (except through criticism in media) to prevent VCD (although the reverse is true for platforms preventing service providers in VCD), intervention in the service system through regulation for information privacy protection is most plausible. This fact is also shown by the data where regulators were actively involved in reporting the case compared to the other cases.

In the archetypes, IV-VI, the service providers and third parties use the data access made possible via the platform. Actors related to the two groups of service providers or third parties increase the value by reducing the value of the user and thus the overall value proposition. After the report in the news, the cases referenced that platform providers took measures to prevent these VCDs. One reason for this is that the VCD processes of service providers or third parties can result in platforms in a bad image. Moreover, the archetypes indicate that besides the user, the other actors may also be affected by the VCD. Value was co-destructed for the actor groups of platform and service providers.

17.6 Discussion

The identified archetypes in this work create the basis for further investigation of information privacy in service systems and ecosystems. As Mustak and Plé (2020) [11] already indicated, in a service ecosystem, actors' interactions may result in VCD because the actors' goals are not always complementary or try to maximize self-interest with consequences for the other actors [63].

Table 3. Seven archetypes of VCD in service systems.

No	Description	VCD by			VCD for			
		Platform provider	Service provider	Third party	User	Platform provider	Service provider	Third party
I	The platform provider is the only actor in the VCD process with a negative value outcome for an individual in the form of an information privacy violation. In the case that a device platform is apparent, the provider can exploit the device data interface.	x			x			
II	The platform provider co-destructs value together with a service provider. The role of the platform provider in the design of data access can be a crucial.	x	x		x			

III	The platform provider interacts with a third party not visible for a user in interaction. A user can not replace a third party. In this archetype, the third party acts as a platform extension.	x		x	x		x	
IV	This archetype characterizes that a service provider makes use of the data access provided via the platform. A user has an option to replace a service with another.		x		x			
V	The value for a user is co-destructed by a service provider in combination with a third party. Third-party integration in a service can be opaque for a user. However, with the knowledge about VCD, the user can replace a service with another.		x	x	x	x		
VI	In this archetype, the third party takes advantage of the integration by a service provider. Value is co-destructed by the third parties' data collection, often opaque towards the service and platform provider and the user.			x	x	x	x	
VII	This archetype involves all actor groups in the VCD process that a user faces in a digital service. No counterbalancing actor group exists in this archetype that could serve as a corrective.	x	x	x	x			

The archetypes indicate that the actors that access personal data do not necessarily remain with these data in the service system. An example is demonstrated in the sixth archetype. Facebook accesses personal data in the individual's service system dedicated to the usage of Zoom. Facebook does not remain in the service system with the accessed personal data and uses the data in providing targeted advertisements in the social network. This personal data diffusion across service systems results in the need for further research in service ecosystems. Nissenbaum [8] already called for investigating hidden practices and the overwhelming scale of the shadow data universe. The consideration of a service ecosystem perspective might be fruitful. In addition, our approach can be transferred to RIPs that are harmful to other normative values. Normative values like fairness likewise can be important. Therefore, the lens of VCD should be further considered for the investigation of normative values, or in other words, (divergent) institutions. Here, studies may benefit from adopting an institutional perspective [13].

Our work also has limitations. First, the case context considers the user rather with a passive attitude. It could be argued that the cases and archetypes do not demonstrate VCD for all individuals and the related awareness. Nevertheless, we consider information privacy as a normative value [7]. Second, in data collection, we build on cases reported in the news. At this point, the reporter or publisher decides on reporting a case that involves a VCD.We minimized this by the consideration of two sources. Third, the article focuses on actors and respective actor groups. Future studies can investigate more detailed characteristics of the archetypes, considering an ecosystem perspective.

The need to consider such a perspective also applies for practitioners to evaluate the collaboration with other actors [3]. The RIPs can give indications to prevent being negatively affected in a service system.

One example is the assessment of RIPs on a platform by the platform provider. A second example is the examination of the behavior of third parties by service providers.

17.7 Conclusion

Actors interact, collaborate, and integrate resources for VCC. Destructive behavior during the process of VCC limits the resulting perceived value. We investigated cases with privacy violations as one facet of RIPs and identified seven archetypes of VCD in service systems. It is not the actor configuration by its design that is co-destructive, but the RIP.

In a digital society, personal data processing is deeply rooted in everyday life. A data flow is appropriate not because it favors the interests of individual subjects (or, conversely, of organizations) above all others, but because it represents a balance of diverse interests as well as societal and contextual ends [8]. This study points out archetypes where the balancing act is out of equilibrium. Our approach can be applied in further research on other normative values like equality to understand how normative values are affected by actions within a service system and ecosystem. It would be worthwhile studying which actor is misbehaving. I.e., misbehavior of a platform could reduce the perception of value more significantly than a third party that is potentially not perceived as an integral actor in the system. Additionally, maximizing the value for all involved actors in a service (eco)system should be the goal and to minimize the destruction of value.

17.8 Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality (project: Information Governance Technologies, LFF-FV 34).

17.9 References

[1] Vargo, S.L., Maglio, P.P., and Akaka, M.A. On value and value co-creation: A service systems and service logic perspective. *European management journal*, 26, 3 (2008).

[2] Ng, I.C., and Smith, L.A. An integrative framework of value. *Special issue–Toward a better understanding of the role of value in markets and marketing*: Emerald Group Publishing Limited, 2012, pp. 207-243.

[3] Vargo, S.L., Akaka, M.A., and Vaughan, C.M. Conceptualizing Value: A Service-ecosystem View. *Journal of Creating Value* (2017).

[4] Spohrer, J.C., and Maglio, P.P. Toward a science of service systems. *Handbook of service science*: Springer, 2010, pp. 157-194.

[5] Plé, L. Why Do We Need Research on Value Co-destruction? , 3, 2 (2017), 162-169.

[6] Plé, L., and Chumpitaz Cáceres, R. Not always co-creation: introducing interactional co-destruction of value in service-dominant logic. 24, 6 (2010), 430-437.

[7] Tavani, H.T. Informational privacy: Concepts, theories, and controversies. *The handbook of information and computer ethics* (2008), 131-164.

[8] Nissenbaum. Contextual integrity up and down the data food chain. *Theoretical inquiries in law*, 2019, pp. 221-256.

[9] Lintula, J., Tuunanen, T., Salo, M., and Myers, M.D. When Value Co-Creation Turns to Co-Destruction: Users™ Experiences of Augmented Reality Mobile Games.(2018).

[10] Vargo, S.L., and Lusch, R.F. Institutions and axioms: an extension and update of service-dominant logic. *Journal of the Academy of Marketing Science*, 44, 1 (2016), 5-23.

[11] Mustak, M., and Plé, L. A critical analysis of service ecosystems research: rethinking its premises to move forward. *Journal of Services Marketing* (2020).

[12] Kleinaltenkamp, M. Institutions and institutionalization. *The Sage Handbook of Service-Dominant Logic, Sage, London* (2018), 265-283.

[13] Plé, L., and Demangeot, C. Social contagion of online and offline deviant behaviors and its value outcomes: The case of tourism ecosystems. *Journal of Business Research*, 117 (2020), 886-896.

[14] Vargo, S.L., and Akaka, M.A. Value cocreation and service systems (re) formation: A service ecosystems view. *Service Science*, 4, 3 (2012), 207-217.

[15] Böhmann, T., Leimeister, J.M., and Möslein, K. Service Systems Engineering: A field for future Information Systems Research. *BISE*, 6, 2 (2014).

[16] Vargo, S.L., and Lusch, R.F. Evolving to a new dominant logic for marketing. 68, 1 (2004), 1-17.

[17] Vargo, S.L., Maglio, P.P., and Akaka, M.A. On value and value co-creation: A service systems and service logic perspective. 26, 3 (2008), 145-152.

[18] Lintula, J., Tuunanen, T., and Salo, M. Conceptualizing the value co-destruction process for service systems: literature review and synthesis. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[19] Riedl, C., Boehmann, T., Leimeister, J.M., and Krcmar, H. A framework for analysing service ecosystem capabilities to innovate. *17th European Conference on Information Systems* (2009).

[20] Van Alstyne, M.W., Parker, G.G., and Choudary, S.P. Pipelines, platforms, and the new rules of strategy. *Harvard Business Review*, 94, 4 (2016), 54-62.

[21] Maglio, P.P., Vargo, S.L., Caswell, N., and Spohrer, J. The service system is the basic abstraction of service science. *Information Systems and E-Business Management*, 7, 4 (2009), 395-406.

[22] Storbacka, K., Brodie, R.J., Böhmann, T., Maglio, P.P., and Nenonen, S. Actor engagement as a microfoundation for value co-creation. *Journal of Business Research*, 69, 8 (2016), 3008-3017.

[23] Vargo, S.L., and Lusch, R.F. From repeat patronage to value co-creation in service ecosystems: a transcending conceptualization of relationship. *Journal of Business Market Management*, 4, 4 (2010), 169-179.

[24] Kurtz, C., Semmann, M., and Schulz, W. Towards a Framework for Information Privacy in Complex Service Ecosystems. *International Conference on Information Systems (ICIS)*, San Fransisco, 2018.

[25] Parker, G.G., Van Alstyne, M.W., and Choudary, S.P. Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You. WW Norton & Company, 2016.

[26] Constantinides, P., Henfridsson, O., and Parker, G.G. Introduction—Platforms and Infrastructures in the Digital Age. INFORMS, 2018.

[27] Sampson, S.E. Visualizing Service Operations. *Journal of Service Research*, 15, 2 (2012), 182-198.

[28] Prahalad, C.K., and Ramaswamy, V. Co-creation experiences: The next practice in value creation. 18, 3 (2004), 5-14.

[29] Vartiainen, T., and Tuunanen, T. Value co-creation and co-destruction in an is artifact: Contradictions of geocaching. *System Sciences (HICSS), 2016 49th Hawaii International Conference on System Sciences.*

[30] Worthington, S., and Durkin, M. Co-destruction of value in context: Cases from retail banking. 12, 3 (2012).

[31] Ertimur, B., and Venkatesh, A. Opportunism in co-production: Implications for value co-creation. 18, 4 (2010).

[32] Smith, A.M. The value co-destruction process: a customer resource perspective. 47, 11/12 (2013).

[33] Kashif, M., and Zarkada, A. Value co-destruction between customers and frontline employees: A social system perspective. 33, 6 (2015), 672-691.

[34] Oliver, R.L. Co-producers and co-participants in the satisfaction process.(2006), 118-127.

[35] Stieler, M., Weismann, F., and Germelmann, C.C. Co-destruction of value by spectators: the case of silent protests. 14, 1 (2014), 72-86.

[36] Järvi, H., Kähkönen, A.-K., and Torvinen, H.J.S.J.o.M. When value co-creation fails: Reasons that lead to value co-destruction. 34, 1 (2018), 63-77.

[37] Pathak, B., Ashok, M., and Tan, Y.L. Value co-destruction: Exploring the role of actors' opportunism in the B2B context. *International journal of information management*, 52 (2020), 102093.

[38] Buhalis, D., Andreu, L., and Gnoth, J. The dark side of the sharing economy: Balancing value co-creation and value co-destruction. *Psychology & Marketing*, 37 (2020).

[39] Pellicano, M., Calabrese, M., Loia, F., and Maione, G. Value co-creation practices in smart city ecosystem. *Journal of Service Science and Management*, 12, 1 (2018), 34-57.

[40] Kurtz, C., Wittner, F., Vogel, P., Semmann, M., and Böhmann, T. Design Goals for Consent at Scale in Digital Service Ecosystems. *Proceedings of the European Conference on Information Systems*, 2020.

[41] Karwatzki, S., Trenz, M., Tuunainen, V.K., and Veit, D. Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, 26, 6 (2017), 688-715.

[42] Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79 (2004), 119.

[43] Yin, R.K. Case Study Research: Design and Methods SAGE, 2009.

[44] Benbasat, I., Goldstein, D.K., and Mead, M. The case research strategy in studies of information systems.(1987), 369-386.

[45] Schilling, R., Haki, K., and Aier, S. Introducing archetype theory to information systems research: a literature review and call for future research. AIS, 2017.

[46] Guillemette, M.G., and Paré, G. Toward a new theory of the contribution of the IT function in organizations. *MIS Quarterly* (2012), 529-551.

[47] Bowen, G.A. Document analysis as a qualitative research method. *Qualitative research journal*, 9, 2 (2009).

[48] Nickerson, R.C., Varshney, U., and Muntermann, J. A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, 22, 3 (2013), 336-359.

[49] Möller, F., Bauhaus, H., Hoffmann, C., Niess, C., and Otto, B. Archetypes of digital business models in logistics start-ups.(2019).

[50] Weking, J., Stocker, M., Kowalkiewicz, M., Bohm, M., and Krcmar, H. Archetypes for industry 4.0 business model innovations. *Proceedings of the 24th Americas Conference on Information System*, 2018.

[51] Vogel, P., Grotherr, C., Kurtz, C., and Böhmann, T. Conceptualizing Design Parameters of Online Neighborhood Social Networks. *WI* (2020).

[52] Chokshi, N. Is Alexa Listening? : New York Times (2018). https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html

[53] Tung, L. Want Google to track you less?(2018). https://www.zdnet.com/article/want-google-to-track-you-less-get-an-iphone-ditch-the-android/

[54] Schmidt, D. Google data collection. *Digital Content Next [Online]* (2018).

[55] Maheshwari, S. How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight.(2018). https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html

[56] Vaughan-Nichols, S.J. Facebook was tracking your text message and phone call data. Now what? : ZDNet (2018). https://www.zdnet.com/article/facebook-was-tracking-your-text-message-and-phone-call-data-now-what/

[57] Whittaker, Z. AccuWeather caught sending user location data, even when location sharing is off. ZDNet (2017). https://www.zdnet.com/article/accuweather-caught-sending-geo-location-data-even-when-denied-access/

[58] Strafach, W. AccuWeather iOS app sends location information to data monetization firm. Hackernoon (2017).

[59] Tung, L. Zoom to iPhone users: We're no longer sending your data to Facebook.(2020).

[60] Yuan, E. Zoom's Use of Facebook's SDK in iOS Client. Zoom Blog (2020). https://blog.zoom.us/zoom-use-of-facebook-sdk-in-ios-client/

[61] Facebook. Facebook Response to National Association of Attorneys General.(2018). https://consumer.sd.gov/docs/facebookResponse_05-09-2018letter.pdf

[62] Li, M., and Tuunanen, T. Actors' Dynamic Value Co-creation and Co-destruction Behavior in Service Systems: A Structured Literature Review. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[63] Mele, C., Nenonen, S., Pels, J., Storbacka, K., Nariswari, A., and Kaartemo, V. Shaping service ecosystems: exploring the dark side of agency. *Journal of Service Management*, 29, 4 (2018).

18 References

Aaen, J., Nielsen, J.A., and Carugati, A. 2021. "The dark side of data ecosystems: A longitudinal study of the DAMD project," *European Journal of Information Systems*, pp. 1-25.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), pp. 509-514.

Ananny, M., and Crawford, K. 2018. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability," *new media & society* (20:3), pp. 973-989.

Barros, A., and Dumas, M. 2006. "The rise of web service ecosystems," *IT professional* (8:5), pp. 31-37.

Barth, A., Datta, A., Mitchell, J.C., and Nissenbaum, H. 2006. "Privacy and contextual integrity: Framework and applications," *2006 IEEE Symposium on Security and Privacy (S&P'06)*: IEEE, pp. 15-198.

Baskerville, R., and Pries-Heje, J. 2010. "Explanatory design theory," *Business & Information Systems Engineering* (2:5), pp. 271-282.

Bélanger, F., and Xu, H. 2015. "The role of information systems research in shaping the future of information privacy," *Information Systems Journal* (25:6), pp. 573-578.

Benbasat, I., Goldstein, D.K., and Mead, M. 1987. "The case research strategy in studies of information systems," *MIS Quarterly*, pp. 369-386.

Benson, V., Saridakis, G., and Tennakoon, H. 2015. "Information disclosure of social media users: does control over personal information, user awareness and security notices matter?," *Information Technology & People* (28:3), pp. 426-441.

Bichler, M., Frank, U., Avison, D., Malaurent, J., Fettke, P., Hovorka, D., Krämer, J., Schnurr, D., Müller, B., and Suhl, L. 2016. "Theories in business and information systems engineering," *Business & Information Systems Engineering* (58:4), pp. 291-319.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., and Shadbolt, N. 2018. "Third Party Tracking in the Mobile Ecosystem," *10th ACM Conference on Web Science.*

Brey, P. 2010. "Values in technology and disclosive computer ethics," *The Cambridge handbook of information and computer ethics*, pp. 41-58.

Buhalis, D., Andreu, L., and Gnoth, J. 2020. "The dark side of the sharing economy: Balancing value co-creation and value co-destruction," *Psychology & Marketing* (37.

Burmeister, F., Kurtz, C., Drews, P., and Schirmer, I. 2021. "Unraveling Privacy Concerns in Complex Data Ecosystems with Architectural Thinking," *Proceedings of the 42nd International Conference on Information Systems (ICIS), Austin (USA).*

Callegati, F., Campi, A., Melis, A., Prandini, M., and Zevenbergen, B. 2015. "Privacy-preserving design of data processing systems in the public transport context," *Pacific Asia Journal of the Association for Information Systems* (7:4).

Christensen, L.T., and Cheney, G. 2015. "Peering into transparency: Challenging ideals, proxies, and organizational practices," *Communication Theory* (25:1), pp. 70-90.

Conger, S., Pratt, J.H., and Loch, K.D. 2013. "Personal information privacy and emerging technologies," *Information Systems Journal* (23:5), pp. 401-417.

Constantinides, P., Henfridsson, O., and Parker, G.G. 2018. "Introduction—Platforms and Infrastructures in the Digital Age," *Information Systems Research*, pp. 381-400.

de la Torre, L. 2018. "GDPR matchup: The California Consumer Privacy Act 2018." Retrieved June 05, 2019, from https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/

de Reuver, M., Sørensen, C., and Basole, R.C. 2018. "The digital platform: a research agenda," *Journal of Information Technology* (33:2), pp. 124-135.

Dinev, T., McConnell, A.R., and Smith, H.J. 2015. "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box," *Information Systems Research* (26:4), pp. 639-655.

Dinev, T., Xu, H., Smith, J.H., and Hart, P. 2013. "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems* (22:3), May, pp. 295-316.

Drews, P., and Schirmer, I. 2014. "From enterprise architecture to business ecosystem architecture: Stages and challenges for extending architectures beyond organizational boundaries," *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*: IEEE, pp. 13-22.

Eaton, B., Elaluf-Calderwood, S., Sorensen, C., and Yoo, Y. 2015. "Distributed tuning of boundary resources: the case of Apple's iOS service system," *MIS Quarterly* (39:1), pp. 217-243.

Eisenhardt, K.M., and Graebner, M.E. 2007. "Theory building from cases: Opportunities and challenges," *Academy of Management Journal* (50:1), Feb, pp. 25-32.

Ethics Commission. 2019. "Report of the Data Ethics Commission of the German Federal Government."

Fischer, C., Winter, R., and Wortmann, F. 2010. "Design theory," *Business & Information Systems Engineering* (2:6), pp. 387-390.

Florini, A. 2007. *The right to know: transparency for an open world*. Columbia University Press.

Friedman, B., and Hendry, D.G. 2019. *Value sensitive design: Shaping technology with moral imagination*. MIT Press.

Friedman, B., Kahn, P.H., and Borning, A. 2008. "Value sensitive design and information systems," *The handbook of information and computer ethics*, pp. 69-101.

Gawer, A., and Cusumano, M.A. 2015. "Platform Leaders," *MIT Sloan Management Review*, pp. 68-75.

GDPR. 2016. "General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Directive 95/46)," pp. 1-88.

Gebken, L., Drews, P., and Schirmer, I. 2021a. "Stakeholder and Value Orientation in Digital Social Innovation: Designing a Digital Donation Concept to Support Homeless Neighbors," *Proceedings of the 54th Hawaii International Conference on System Sciences*, Hawaii (USA).

Gebken, L., Kurtz, C., Drews, P., Schirmer, I., and Böhmann, T. 2021b. "Human-Value-Oriented Digital Social Innovation: A Multilevel Design Framework," *Proceedings of the 42nd International Conference on Information Systems (ICIS)*, Texas (USA).

Gelhaar, J., Groß, T., and Otto, B. 2021. "A Taxonomy for Data Ecosystems," *Proceedings of the 54th Hawaii International Conference on System Sciences*, Hawaii (USA).

Ghazawneh, A., and Henfridsson, O. 2013. "Balancing platform control and external contribution in third-party development: the boundary resources model," *Information Systems Journal* (23:2), pp. 173-192.

Gopal, R., Hidaji, H., Patterson, R., Rolland, E., and Zhdanov, D. 2018. "How much to share with third parties? User privacy concerns and website dilemmas," *MIS Quarterly* (42:1), pp. 143-164.

Greenaway, K.E., and Chan, Y.E. 2013. "Designing a Customer Information Privacy Program Aligned with Organizational Priorities," *MIS Quarterly Executive* (12:3).

Gregor, S., and Jones, D. 2007. "The anatomy of a design theory," *Journal of the Association for Information Systems* (8:5).

Guillemette, M.G., and Paré, G. 2012. "Toward a new theory of the contribution of the IT function in organizations," *MIS Quarterly*, pp. 529-551.

Hagiu, A., and Wright, J. 2015. "Multi-sided platforms," *International Journal of Industrial Organization* (43:1), pp. 162-174.

Hein, A., Schreieck, M., Riasanow, T., Setzke, D.S., Wiesche, M., Böhm, M., and Krcmar, H. 2019. "Digital platform ecosystems," *Electronic Markets*, pp. 1-12.

Hevner, A.R., March, S.T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *Management Information Systems Quarterly* (28:1), pp. 75-105.

Hong, W.Y., and Thong, J.Y.L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.

Horlach, B., Schirmer, I., and Drews, P. 2019. "Agile Portfolio Management: Design Goals and Principles," *Proceedings of the European Conference on Information Systems, Stockholm-Uppsala, Sweden (ECIS 2019).*

Jacobs, M., Kurtz, C., Simon, J., and Böhmann, T. 2021. "Value-sensitive design and power in socio-technical ecosystems," *Internet Policy Review.*

Jia, Y.J., Chen, Q.A., Wang, S., Rahmati, A., Fernandes, E., Mao, Z.M., Prakash, A., and Unviersity, S. 2017. "ContexloT: Towards Providing Contextual Integrity to Appified IoT Platforms," *NDSS.*

Johannesson, P., and Perjons, E. 2014. "Research strategies and methods," in *An Introduction to Design Science*. Springer, pp. 39-73.

Kallemeyn, D., and Chipidza, W. 2021. "Towards a Forward-Looking Conceptualization of Privacy," *Proceedings of the International Conference on Information Systems (ICIS)*, Texas (USA).

Karhu, K., Gustafsson, R., and Lyytinen, K. 2018. "Exploiting and defending open digital platforms with boundary resources: Android’s five platform forks," *Information Systems Research* (29:2), pp. 479-497.

Karwatzki, S., Trenz, M., Tuunainen, V.K., and Veit, D. 2017. "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence," *European Journal of Information Systems* (26:6), pp. 688-715.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal* (25:6), pp. 607-635.

Kleinaltenkamp, M. 2018. "Institutions and institutionalization," *The Sage Handbook of Service-Dominant Logic, Sage, London*, pp. 265-283.

Kuechler, B., and Vaishnavi, V. 2008. "On theory development in design science research: anatomy of a research project," *European Journal of Information Systems* (17:5), pp. 489-504.

Kühl, N., Martin, D., Wolff, C., and Volkamer, M. 2020. ""Healthy surveillance": Designing a concept for privacy-preserving mask recognition AI in the age of pandemics," in: *Proceedings of the Hawaii International Conference on System Sciences*. Hawaii (USA).

Kumaraguru, P., and Cranor, L.F. 2005. *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University.

Kurtz, C., Burmeister, F., Wittner, F., Semmann, M., and Schirmer, I. 2022 (under review). "Multi-Role Actors and Rebounding Effects in Data Ecosystems - Exposing Limitations of the GDPR," in: *43rd International Conference on Information Systems (ICIS)*. Copenhagen (Denmark).

Kurtz, C., Semmann, M., and Böhmann, T. 2018a. "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors," in: *Proceedings of the 24th Americas' Conference on Information Systems (ACMIS)*. New Orleans (USA).

Kurtz, C., Semmann, M., and Schulz, W. 2018b. "Towards a Framework for Information Privacy in Complex Service Ecosystems," in: *Proceedings of the 39th International Conference on Information Systems (ICIS)*. San Fransisco (USA).

Kurtz, C., Vogel, P., and Semmann, M. 2022. "Exploring Archetypes of Value Co-Destructive Privacy Practices," *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*, Hawaii (USA).

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. 2019. "The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems," in: *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Hawaii (USA).

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., and Böhmann, T. 2021. "Accountability of Platform Providers for Unlawful Personal Data Processing in their Ecosystems – A Socio-Techno-Legal Analysis of Facebook and Apple's iOS according to GDPR," *Journal of Responsible Technology*.

Kurtz, C., Wittner, F., Vogel, P., Semmann, M., and Böhmann, T. 2020. "Design Goals for Consent at Scale in Digital Service Ecosystems," *Proceedings of the 28th European Conference on Information Systems (ECIS)*, AIS Virtual Conference.

Legner, C., and Löhe, J. 2012. "Improving the realization of IT demands: A design theory for end-to-end demand management," *Proceedings of the International Conference on Information Systems (ICIS)*, Florida (USA).

Lindner, M. 2014. "Dissertation: Privatheit im Informationszeitalter. Ethische Grundlagen von Privatheit und Anwendungsfragen in der Informationstechnologie." Universitätsbibliothek Tübingen.

Lintula, J., Tuunanen, T., and Salo, M. 2017. "Conceptualizing the value co-destruction process for service systems: literature review and synthesis," *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii (USA).

Lintula, J., Tuunanen, T., Salo, M., and Myers, M.D. 2018. "When Value Co-Creation Turns to Co-Destruction: Users™ Experiences of Augmented Reality Mobile Games," *Proceedings of the International Conference on Information Systems (ICIS)*, San Francisco (USA).

Manikas, K. 2016. "Revisiting software ecosystems research: A longitudinal literature study," *Journal of systems and software* (117:1), pp. 84-103.

March, S.T., and Smith, G.F. 1995. "Design and Natural-Science Research on Information Technology," *Decision Support Systems* (15:4), pp. 251-266.

Mele, C., Nenonen, S., Pels, J., Storbacka, K., Nariswari, A., and Kaartemo, V. 2018. "Shaping service ecosystems: exploring the dark side of agency," *Journal of Service Management* (29:4).

Möller, F., Bauhaus, H., Hoffmann, C., Niess, C., and Otto, B. 2019. "Archetypes of digital business models in logistics start-ups," *Proceedings of the European Conference on Information Systems (ECIS)*, Stockholm (Sweden).

Moor, J.H. 2006. "Using genetic information while protecting the privacy of the soul," *Ethics, Computing, and Genomics, Jones and Bartlett, Sudbury, MA* (1(4), pp. 109-119.

Moore, J. 1996. "The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems. Leadership." New York: Harper Business.

Mueller, M., and Heger, O. 2018. "Health at Any Cost? Investigating Ethical Dimensions and Potential Conflicts of an Ambulatory Therapeutic Assistance System through Value Sensitive Design," in: *Proceedings of the International Conference on Information Systems (ICIS)*. San Fransisco (USA).

Mustak, M., and Plé, L. 2020. "A critical analysis of service ecosystems research: rethinking its premises to move forward," *Journal of Services Marketing* (34:3), pp. 399-413.

Myers, M.D. 2019. *Qualitative research in business and management*. SAGE.

Nickerson, R.C., Varshney, U., and Muntermann, J. 2013. "A method for taxonomy development and its application in information systems," *European Journal of Information Systems (EJIS)* (22:3), pp. 336-359.

Nischak, F., Hanelt, A., and Kolbe, L.M. 2017. "Unraveling the interaction of information systems and ecosystems-A comprehensive classification of literature," *Proceedings of the International Conference on Information Systems (ICIS)*, Seoul (South Korea).

Nissenbaum. 2004. "Privacy as contextual integrity," *Washington Law Review* (79:1), pp. 119-158.

Nissenbaum. 2011. "A Contextual Approach to Privacy Online," *Daedalus* (140:4), pp. 32-48.

Nissenbaum. 2019. "Contextual integrity up and down the data food chain," in: *Theoretical inquiries in law*. pp. 221-256.

Norberg, P.A., Horne, D.R., and Horne, D.A. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs* (41:1), Sum, pp. 100-126.

Oliveira, M.I.S., Lima, G.d.F.B., and Lóscio, B.F. 2019. "Investigations into Data Ecosystems: a systematic mapping study," *Knowledge and Information Systems* (61:2), pp. 589-630.

Oliveira, M.I.S., Oliveira, L.E.R., Batista, M.G.R., and Lóscio, B.F. 2018. "Towards a meta-model for data ecosystems," *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pp. 1-10.

Parker, G., Alstyne, M.V., and Jiang, X. 2017. "Platform ecosystems: how developers invert the firm," *MIS Quarterly* (41:1), pp. 255-266.

Parker, G.G., Van Alstyne, M.W., and Choudary, S.P. 2016. *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*. WW Norton & Company.

Pathak, B., Ashok, M., and Tan, Y.L. 2020. "Value co-destruction: Exploring the role of actors' opportunism in the B2B context," *International journal of information management* (52:1).

Peffers, K., Tuunanen, T., Rothenberger, M.A., and Chatterjee, S. 2007. "A design science research methodology for Information Systems Research," *Journal of Management Information Systems* (24:3), pp. 45-77.

Pellicano, M., Calabrese, M., Loia, F., and Maione, G. 2018. "Value co-creation practices in smart city ecosystem," *Journal of Service Science and Management* (12:1), pp. 34-57.

Peters, C., Maglio, P., Badinelli, R., Harmon, R.R., Maull, R., Spohrer, J.C., Tuunanen, T., Vargo, S.L., Welser, J.J., Demirkan, H., Griffith, T.L., and Moghaddam, Y. 2016. "Emerging Digital Frontiers for Service Innovation," *Communications of the Association for Information Systems* (39:1), pp. 136-149.

Plé, L. 2017. "Why Do We Need Research on Value Co-destruction?," *Journal of Creating Value* (3:2), pp. 162-169.

Plé, L., and Chumpitaz Cáceres, R. 2010. "Not always co-creation: introducing interactional co-destruction of value in service-dominant logic," *Journal of Services Marketing* (24:6), pp. 430-437.

Plé, L., and Demangeot, C. 2020. "Social contagion of online and offline deviant behaviors and its value outcomes: The case of tourism ecosystems," *Journal of Business Research* (117, pp. 886-896.

Prahalad, C.K., and Ramaswamy, V. 2004. "Co-creation experiences: The next practice in value creation," *Journal of Interactive marketing* (18:3), pp. 5-14.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., and Gill, P. 2018. "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem," *Network and Distributed Systems Security (NDSS) Symposium 2018*, California (USA).

Regan, P.M. 1995. *Legislating privacy: Technology, social values, and public policy*. University of North Carolina Press.

Riedl, C., Boehmann, T., Leimeister, J.M., and Krcmar, H. 2009a. "A framework for analysing service ecosystem capabilities to innovate," *Proceedings of the European Conference on Information Systems (ECIS)*, Verona (Italy).

Riedl, C., Boehmann, T., Leimeister, J.M., and Krcmar, H. 2009b. "A framework for analysing service ecosystem capabilities to innovate," *17th European Conference on Information Systems.*

Sampson, S.E. 2012. "Visualizing Service Operations," *Journal of Service Research* (15:2), pp. 182-198.

Schilling, R., Haki, K., and Aier, S. 2017. "Introducing archetype theory to information systems research: a literature review and call for future research," *International Conference on Wirtschaftsinformatik*, St. Gallen (Switzerland).

Schreieck, M., Wiesche, M., and Krcmar, H. 2016. "Design and Governance of Platform Ecosystems-Key Concepts and Issues for Future Research," *Proceedings of the European Conference on Information Systems (ECIS)*, Istanbul (Turkey).

Seawright, J., and Gerring, J. 2008. "Case selection techniques in case study research - A menu of qualitative and quantitative options," *Political Research Quarterly* (61:2), pp. 294-308.

Simon, J. 2016. "Values in design," in *Handbuch Medien-und Informationsethik*. Springer, pp. 357-364.

Simon, J. 2017. "Value-Sensitive Design and Responsible Research and Innovation," *The Ethics of Technology: Methods and Approaches*, pp. 219-236.

Sjöström, J., Ågerfalk, P., and Hevner, A.R. 2022. "The Design of a System for Online Psychosocial Care: Balancing Privacy and Accountability in Sensitive Online Healthcare Environments," *Journal of the Association for Information Systems* (23:1), pp. 237-263.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

Smith, H.J., Milburg, S.J., and Burke, S.J. 1996. "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly* (20:2), pp. 167-196.

Solove, D.J. 2002. "Conceptualizing privacy," *California Law Review* (90:1), pp. 1087-1156.

Spiekermann, S., and Novotny, A. 2015. "A vision for global privacy bridges: Technical and legal measures for international data markets," *Computer Law & Security Review* (31:2), pp. 181-200.

Steinbart, P., Keith, M., and Babb, J. 2017. "Measuring Privacy Concern and the Right to Be Forgotten," *Proceedings of the Hawaii International Conference on System Sciences*, Hawaii (USA).

Tavani, H.T. 2008. "Informational privacy: Concepts, theories, and controversies," in *The handbook of information and computer ethics*. Wiley, pp. 131-164.

Thiebes, S., Lyytinen, K., and Sunyaev, A. 2017. "Sharing is About Caring? Motivating and Discouraging Factors in Sharing Individual Genomic Data," *Proceedings of the Internation Conference on Information Systems (ICIS)*, Seoul (South Korea).

Thompson, J.B. 2013. *Political scandal: Power and visability in the media age*. John Wiley & Sons.

Tiwana, A., Konsynski, B., and Bush, A.A. 2010. "Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics," *Information Systems Research* (21:4), pp. 675-687.

Tiwana, A., Konsynski, B., and Venkatraman, N. 2013. "Information technology and organizational governance: The IT governance cube," *Journal of Management Information Systems* (30:3), pp. 7-12.

Van Alstyne, M.W., Parker, G.G., and Choudary, S.P. 2016. "Pipelines, platforms, and the new rules of strategy," *Harvard Business Review* (94:4), pp. 54-62.

Vargo, S., and Lusch, R. 2011. "Service-dominant logic: Looking ahead," *Presentation at the Naples Forum on Service*, pp. 14-17.

Vargo, S.L., and Akaka, M.A. 2012. "Value cocreation and service systems (re) formation: A service ecosystems view," *Service Science* (4:3), pp. 207-217.

Vargo, S.L., Akaka, M.A., and Vaughan, C.M. 2017. "Conceptualizing Value: A Service-ecosystem View," *Journal of Creating Value* (3:2).

Vargo, S.L., and Lusch, R.F. 2004. "Evolving to a new dominant logic for marketing," *Journal of Marketing* (68:1), pp. 1-17.

Vargo, S.L., and Lusch, R.F. 2010. "From repeat patronage to value co-creation in service ecosystems: a transcending conceptualization of relationship," *Journal of Business Market Management* (4:4), pp. 169-179.

Vargo, S.L., and Lusch, R.F. 2016. "Institutions and axioms: an extension and update of service-dominant logic," *Journal of the Academy of Marketing Science* (44:1), pp. 5-23.

Vargo, S.L., Maglio, P.P., and Akaka, M.A. 2008a. "On value and value co-creation: A service systems and service logic perspective," (26:3), pp. 145-152.

Vargo, S.L., Maglio, P.P., and Akaka, M.A. 2008b. "On value and value co-creation: A service systems and service logic perspective," *European management journal* (26:3), pp. 145-152.

Vargo, S.L., Wieland, H., and Akaka, M.A. 2015. "Innovation through institutionalization: A service ecosystems perspective," *Industrial marketing management* (44:1), pp. 63-72.

Vartiainen, T., and Tuunanen, T. 2016. "Value co-creation and co-destruction in an is artifact: Contradictions of geocaching," *Proceedings of the Hawaii International Conference on System Sciences*, Hawaii (USA), pp. 1266-1275.

Vial, G. 2019. "Understanding digital transformation: A review and a research agenda," *The Journal of Strategic Information Systems* (28:2), pp. 118-144.

Vogel, P., Grotherr, C., Kurtz, C., and Böhmann, T. 2020. "Conceptualizing Design Parameters of Online Neighborhood Social Networks," *Proceedings of the 15th International Conference on Wirtschaftsinformatik*, Potsdam (Germany).

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. 2009. "Reconstructing the giant: On the importance of rigour in documenting the literature search process," *Proceedings of the European Conference in Information Systems*, Verona (Italy), pp. 2206-2217.

Walls, J.G., Widmeyer, G.R., and El Sawy, O.A. 1992. "Building an information system design theory for vigilant EIS," *Information Systems Research* (3:1), pp. 36-59.

Webster, J., and Watson, R.T. 2002. "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly* (26:2), pp. Xiii-Xxiii.

Weking, J., Stocker, M., Kowalkiewicz, M., Bohm, M., and Krcmar, H. 2018. "Archetypes for industry 4.0 business model innovations," *Proceedings of the Americas Conference on Information Systems (AMCIS)*, New Orleans (USA), pp. 1-10.

Westin, A.F. 1967. "Privacy and freedom, atheneum," *New York* (7:1).

Westin, A.F. 1991. "Harris-Equifax consumer privacy survey 1991," *Atlanta, GA: Equifax Inc.*

Winkler, T., and Spiekermann, S. 2018. "Twenty years of value sensitive design: a review of methodological practices in VSD projects," *Ethics and information technology*, pp. 1-5.

Worthington, S., and Durkin, M. 2012. "Co-destruction of value in context: Cases from retail banking," *The Marketing Review* (12:3), pp. 291-307.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2008. "Examining the formation of individual's privacy concerns: Toward an integrative view," *Proceedings of the International Conference on Information Systems*, Paris (France).

Yin, R.K. 2009. "Case study research: Design and methods (applied social research methods)."

Zuboff, S. 2015. "Big other: surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology* (30:1), pp. 75-89.

Zuboff, S. 2019. *The Age of Surveillance Capitalism*. Profile Books.

Appendix A: Article No. 10 (Kurtz et al. 2022 (under review))

Kurtz, C., Burmeister, F., Wittner, F., Semmann, M., and Schirmer, I. Multi-Role Actors and Rebounding Effects in Data Ecosystems – Exploring Big Tech's Privacy Scandals and GDPR Limitations. International Conference on Information Systems (ICIS), Copenhagen (Denmark), 2022 – under review.

Abstract

Big Tech companies' ecosystems build on the commodification of personal data with consequences for individuals' information privacy. The sustained data collection in data ecosystems bases often on secrecy. This opacity creates problems for regulators in assessing privacy-violating practices, and regulation fails to materialize. Given the challenge of data access to privacy-violating practices in data ecosystems, we analyzed 21 privacy scandals reported in the media. The scandals include Facebook and Google, which maximized personal data accumulation and utilization practices. Our results show that the companies take various roles across service contexts. These diverse roles enable to decouple personal data from the original service context and build the basis for rebounding effects in other service contexts. Using the GDPR in a legal assessment, we indicate that for regulation of Big Tech companies' practices, the actors' spheres of influence and the totality of their data processing operations are crucial.

18.1 Introduction

Billions of people use information technologies extensively, and personal data arise almost everywhere (Mikalef et al. 2019). The growing number of information systems (IS) connected in networks creates unprecedented opportunities to create and share data in all spheres of life (Zuboff 2015). Big Tech companies and related services are central parts of these evolutions. The companies often called “platforms" have contributed to diverse and useful developments. For this, the companies created expansive data ecosystems around individuals. The companies’ capabilities build around commodifying a huge amount of personal data with consequences for individuals’ information privacy (Zuboff 2019). So far, little is known in detail about Big Tech privacy-violating practices, as they established secrecy around the companies’ ecosystems (Zuboff 2019). The lack of individuals’ understanding concerning their privacy is also highlighted in a survey: 59% of respondents understand very little about companies’ data collection, 79% are concerned about the ways how their personal data are used, and 84% declared to have no control over the data that companies collect about them (Center 2019). Still, a large part of privacy research in the IS field focuses on the concept of information privacy as one’s ability to control personal data about oneself to study the dyadic relationship between an individual and a company (Bélanger and Xu 2015; Kallemeyn and Chipidza 2021). Existing data ecosystems in which individuals and companies create and collect personal data are less taken into account. IS research on information privacy in data ecosystems is missing, and thus, the empirical facts and constructs that enable research to proceed are outstanding.

This manuscript moves beyond the traditional perspective on privacy in the IS field. It adopts a systemic perspective to get insights about the triangle of privacy, Big Tech companies, and data ecosystems. In this regard, systemic means a broader perspective shifting from the focus on the interaction between an individual and a company towards the personal data creation, collection, and use in data ecosystems with different companies involved. Given the problem of secrecy established by Big Tech companies, we use privacy scandals reported in media. By considering various scandals with the involvement of Google and Facebook, we aim to create a better understanding of their practices in data ecosystems to unearth the Big Tech companies’ ecosystems. Hence, we address the following research question:

RQ1: What are the roles of Big Tech companies in data ecosystems, and how are these roles violating individuals’ information privacy?

Still, many people pin hopes on the regulation of personal data processing also regarding proliferating practices in data ecosystems. In this context, the EU’s General Data Protection Regulation (GDPR) introduced several new substantives and also applies to companies outside the European Union (EU) when processing the personal data of EU citizens. In addition, the regulation served as a blueprint for data protection regulations throughout the world, such as the California Consumer Privacy Act (de la Torre 2018). The question still leaves open whether this regulation can be a springboard to privacy-invasive practices of Big Tech companies in data ecosystems. Thus, we address also a second research question:

RQ2: Is the GDPR able to regulate privacy-violating practices of Big Tech companies in data ecosystems?

We introduce the literature and background of data ecosystems, information privacy, and the GDPR. We continue by specifying our research approach to study privacy in data ecosystems. Our results show that Big Tech companies in data ecosystems masquerade as platform providers, service providers, and third parties to gain access to individuals' personal data. These roles create the basis for rebounding effects on individuals in other service contexts. Given these results, we examine whether the GDPR would be applicable to regulate related data processing. As part of our discussion, we elaborate on the results before we draw a conclusion.

18.2 Literature and Background

18.2.1 Data Ecosystems

Along with other types of ecosystems that conceptualize networks of value co-creation, such as business ecosystems (Moore 1996), platform ecosystems (Tiwana et al. 2010), service ecosystems (Lusch and Vargo 2014), or software ecosystems (Manikas 2016), data ecosystems are gaining increasing attention in IS research (Aaen et al. 2021). We consider a data ecosystem perspective and not a platform ecosystem perspective on Big Tech companies. A platform ecosystem perspective might be too narrow to holistically grasp the data practices of Big Tech companies that may also appear outside their platform ecosystems.

Research on data ecosystems is still in its infancy and perceived as “new and undertheori[z]ed” (Aaen et al. 2021, p. 3). For example, recent literature analyses of ecosystems in IS research lack to consider data ecosystems (Benedict 2018; Faber et al. 2019). According to Oliveira et al. (2019), data ecosystems can be defined as "a loose set of interacting actors that directly or indirectly consume, produce, or provide data and other related resources (e.g., software, services, and infrastructure). Each actor performs one or more roles and is connected to other actors through relationships, in such a way that actors by collaborating and competing with each other promote data ecosystems" (p. 604). While many studies on data ecosystems refer to open data communities, e.g., in the public sector (Ponte 2015; Zuiderwijk et al. 2014), there is a lack of research applying the data ecosystem perspective to study practices that violate information privacy (BLINDED). For example, modeling approaches in the context of data ecosystems do not focus on personal-data sharing and its effects on privacy (Demchenko et al. 2014; Oliveira et al. 2018).

18.2.2 Information Privacy

IS studies typically consider the information privacy understanding of one's ability to control personal data about oneself (Bélanger and Xu 2015; Kallemeyn and Chipidza 2021). The research addresses individual actions and motivations by using this conceptualization (Acquisti et al. 2015; Dinev et al. 2015; Kallemeyn and Chipidza 2021; Kehr et al. 2015). For example, studies address individuals' intentions to disclose data (and the information privacy concerns that relate to that intention) (Gopal et al. 2018; Steinbart et al. 2017); or the privacy paradox, which is a gap between the intention to disclose personal data and the disclosure behavior (Acquisti et al. 2015; Norberg et al. 2007). In this regard, dyadic interactions between an individual and a company have been investigated in depth (Acquisti et al. 2015; Kallemeyn and Chipidza 2021). This aspect is also true for studies on individuals' privacy in the cases of Facebook and Google (Cabinakova et al. 2016; Choi and Land 2016; Lankton and Tripp 2013; Ozdemir et al. 2017; Proudfoot et al. 2018; Teubner and Flath 2019; Xu et al. 2012).

Existing studies also consider privacy concerns regarding individual beliefs about companies' personal data usage (Smith et al. 1996). Literature divides privacy concerns into categories that include the secondary usage of data, improper access to data, collection of data, control over data, or data errors (Hong and Thong 2013; Smith et al. 1996). In detail, secondary usage specifies personal data processed by companies for a specific purpose but also used for other secondary purposes without an individual's permission to do so (Smith et al. 1996). Improper access encompasses the concerns where personal data are accessible to a company that is not authorized to use or process them (Smith et al. 1996). The violation of information privacy and unauthorized access to personal data can cause adverse consequences for individuals (Karwatzki et al. 2017). Karwatzki et al. (2017) highlight that consequences provoked by companies may be psychological, freedom-related, or resource-related (Karwatzki et al. 2017). Psychological consequences refer to mental discomfort regarding unknown consequences, surveillance, or loss of control (Karwatzki et al. 2017). Freedom-related consequences specify the individuals' loss of freedom of opinion and behavior. Related consequences can be divided into three parts: manipulations of behavior to influence an individual's decision, manipulations of behavior, and restrictions on behavior (Karwatzki et al. 2017). Resource-related consequences are dividable into loss of time, material losses, and direct and indirect financial losses (Karwatzki et al. 2017). While studies about concerns and consequences consider dyadic relationships between individuals and companies, privacy research at the group level remains scarce (Kallemeyn and Chipidza 2021). A few articles modeled personal data processing in multi-party constellations (Benson et al. 2015; Conger et al. 2013; Karwatzki et al. 2017). However, "[n]o known research focuses on the data themselves, i.e., their existence, movement and life cycle once released by the individual." (Conger et al. 2013, p. 412f.)

Summing up, we consider two research streams. The existing literature on information privacy covers individuals' concerns and adverse consequences of companies' personal data access and usage. However, only limited knowledge exists besides the dyadic relationship between the individual and the company. The concept of a data ecosystem addresses data creation, collection, and sharing in a complex multi-actor constellation but has little been considered regarding information privacy (BLINDED).

18.2.3 Personal Data Protection by the GDPR

In terms of protecting individuals' personal data, the new body of EU regulation known as the GDPR has made significant inroads (Andrew and Baker 2019). Personal data refers to "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR 2016, Art. 4 No. 1).

The GDPR is the central framework for data protection in Europe (GDPR 2016). The regulation aims to protect personal data and privacy for one of the largest consumer markets worldwide (GDPR 2016, Art. 1 (1)). The GDPR also binds companies outside the jurisdiction of the EU when they process the personal data of the EU citizens (GDPR 2016, Art. 3 (2)) and serves as a blueprint for privacy regulation throughout the world, such as the California Consumer Privacy Act 2018 (de la Torre 2018). The GDPR has the explicit aim of regulating the modern data processing environment and attempts to enforce data protection by offering a binary system of two opposing groups: a *controller* (entity processing the personal data) and a *data subject* (person to whom these data relate; namely, the users in this study). Data controllership, the role within the GDPR that attributes accountability and responsibility for the lawfulness of a data processing operation to a company, is always defined concerning any operation or set of (identical) operations performed on personal data (GDPR 2016, Art. 4 No. 2). In addition, two or more actors can be *joint controllers* for an act of processing in which they jointly determine its purposes and means (GDPR, Art. 26). Moreover, a processor is an actor that processes data on behalf of the controller, according to Art. 4 No. 8. Under the GDPR, regulators can invoke substantial penalties of up to 4% of the annual worldwide revenues of companies for violating the data protection clauses (GDPR

2016, Art. 83 No. 5). The regulation is formulated in an abstract way to fill the regulation with life over time. This characteristic enables a regulation to be applicable to novel practices. At the same time, this abstractness creates doubts regarding data processing, for which judgments create clarity concerning the legality.

18.3 Research Approach

We conduct a multiple case analysis (Yin 2009) as the foundation of our research strategy (see Figure 1). In detail, we examined privacy scandals (in the remainder of this article termed as cases) related to Google and Facebook as major representatives of Big Tech companies.

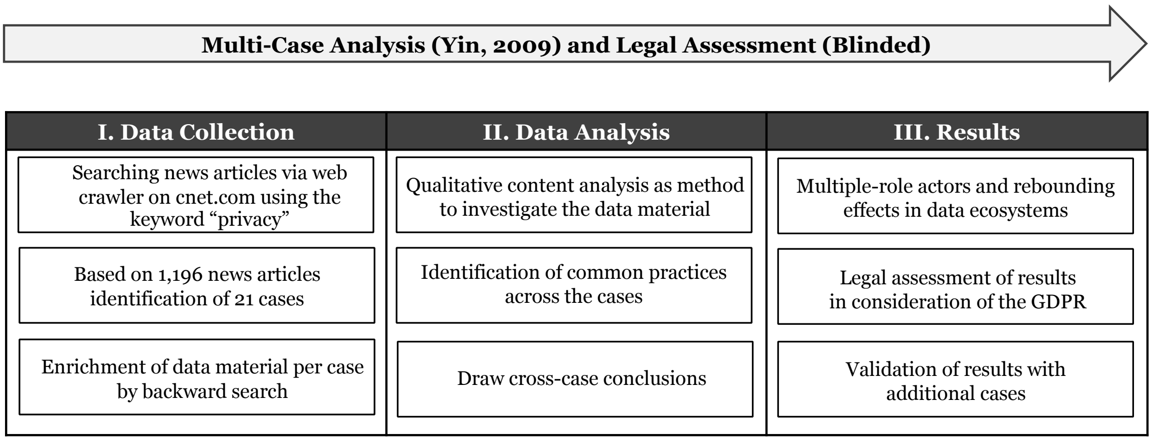
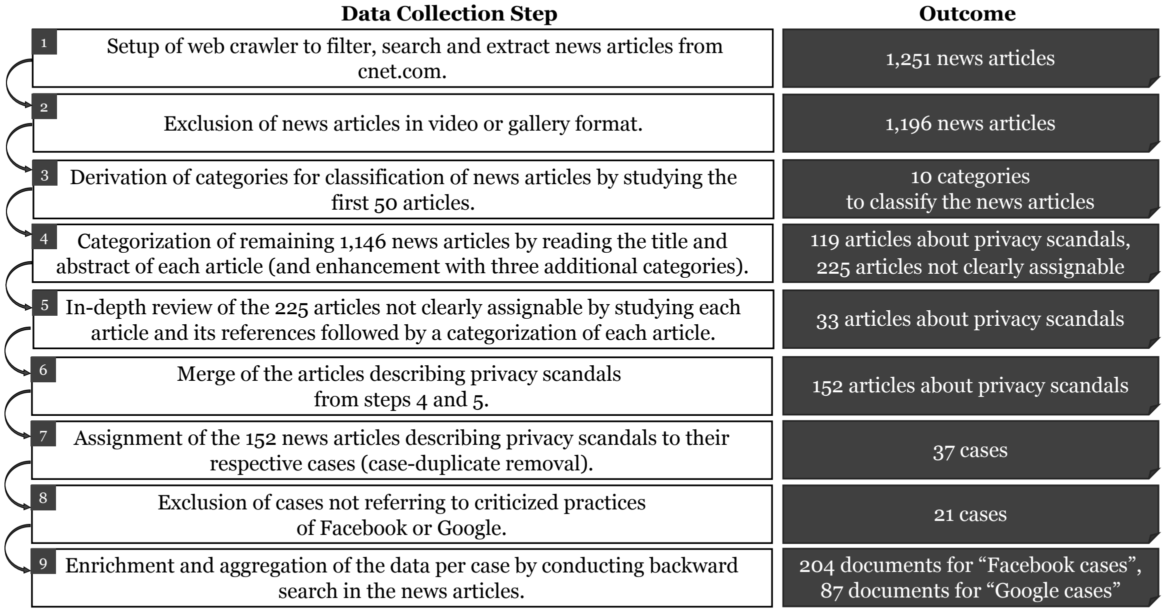

Multi-Case Analysis (Yin, 2009) and Legal Assessment (Blinded)
I. Data Collection
Searching news articles via web crawler on cnet.com using the keyword "privacy"
Based on 1,196 news articles identification of 21 cases
Enrichment of data material per case by backward search
II. Data Analysis
Qualitative content analysis as method to investigate the data material
Identification of common practices across the cases
Draw cross-case conclusions
III. Results
Multiple-role actors and rebounding effects in data ecosystems
Legal assessment of results in consideration of the GDPR
Validation of results with additional cases

Figure 1. Research approach

In the first step, we identified cases by searching news articles and enriching the data material per case (Yin 2009). In the second step, we applied qualitative content analysis (Kohlbacher 2006; Mayring 2004) to interpret the cases and examine the data material per case. Mayring describes content analysis as the proper approach for "the systematic examination of communicative material (originally from the mass media in particular)" (Mayring 2004, p. 266). In the third step, based on the cross-case conclusions, we identified multiple roles of actors across service contexts that build the basis for rebounding effects. Here, created illustrations of the privacy scandals supported to understand the cases. We further validated our results with additional cases. Finally, we analyzed the GDPR's applicability to the regulation of data processing related to these roles and rebounding effects in a legal assessment (BLINDED).

18.3.1 Data Collection

Our selection of multiple cases is based on theoretical replication logic, according to which different cases are predicted to provide heterogeneous characteristics (Benbasat et al. 1987; Yin 2009). Figure 2 shows the steps of our data collection process. We used cnet.com as our initial data source, as it is the technology-news website with the highest traffic rank worldwide (SimilarWeb 2019). News articles on this website are interlinked to other sources such as websites or documents such as scientific studies or technical reports. We also considered the other sources to increase the variety of data within the data material (see Table 3) and the robustness of our analysis.



	Data Collection Step	Outcome
1	Setup of web crawler to filter, search and extract news articles from cnet.com.	1,251 news articles
2	Exclusion of news articles in video or gallery format.	1,196 news articles
3	Derivation of categories for classification of news articles by studying the first 50 articles.	10 categories to classify the news articles
4	Categorization of remaining 1,146 news articles by reading the title and abstract of each article (and enhancement with three additional categories).	119 articles about privacy scandals, 225 articles not clearly assignable
5	In-depth review of the 225 articles not clearly assignable by studying each article and its references followed by a categorization of each article.	33 articles about privacy scandals
6	Merge of the articles describing privacy scandals from steps 4 and 5.	152 articles about privacy scandals
7	Assignment of the 152 news articles describing privacy scandals to their respective cases (case-duplicate removal).	37 cases
8	Exclusion of cases not referring to criticized practices of Facebook or Google.	21 cases
9	Enrichment and aggregation of the data per case by conducting backward search in the news articles.	204 documents for "Facebook cases", 87 documents for "Google cases"

Figure 2. Data collection process

As the first step of data collection, we set up a web crawler to search news articles on cnet.com using the keyword "privacy," as we wanted to identify the roles of Big Tech companies and practices in data ecosystems exposed in privacy scandals. For this, we use the definition of scandal by Thompson (2013). Articles complaining about privacy scandals include data collection or data use practices with the characteristics that their occurrence (1) involves an element of opacity and (2) a transgression related to privacy (3) that offends individuals. In addition, (4) reporters publicly denounce the practices from which follows that (5) the disclosure of the practices may damage the reputation of the party responsible. We sorted the articles by descending date and considered a 13-month time period for an initial list of 1,251 news articles. These articles mention the word "privacy" in the title, abstract, or text. The articles were extracted by the web crawler and integrated into a case-study database (Yin 2009). We excluded news articles in video or gallery format in the second step, resulting in 1,196 news articles. In the third step, two researchers studied the first 50 news articles and derived 10 categories for classification (see Table 1).

Table 1. Categorization of news articles

Category	Example	Σ
Company viewpoint: the position of a company regarding an issue or another company.	cnet.co/34LSkdu	38
Court judgment: court judgments, such as decisions on changes of law or fines.	cnet.co/2HWaVKA	23
Crime: criminal activities, including spying by government institutions and technologies used by the police or FBI to investigate criminal cases.	cnet.co/2TIZAAi	28
Data breach: data breaches, including data loss through IT infrastructure incidents, unconscious data leakage, and data theft by hackers.	cnet.co/2TGw7Hl	47
Event: events, such as conferences or trade fairs for IT products.	cnet.co/3oW0Xdw	49
Government debate: the concerns and discussions of government actors, e.g., federal institutions, future legislative changes, or the behavior of specific companies	cnet.co/3mFPiO2	118
How-to: hints in the use and personalization of technologies, such as apps.	cnet.co/3kY7Log	104
Innovation: new products and technologies launched on the market.	cnet.co/2GgCDl3	105
Public debate: subjective views and statements on specific issues	cnet.co/2I9g56E	28
Privacy scandal: criticized personal-data practice involving kinds of transgressions that become known to others and is serious about eliciting a public response.	cnet.co/2IdRcXn	152
Product update: new features or updates of products, such as apps, and hardware	cnet.co/2TgwyRV	142
Security incident: security issues and vulnerabilities of software and hardware	cnet.co/3jMnHsz	78
Technology information: technology characteristics and strategy changes in companies	cnet.co/384gFx1	284

Σ 1,196

In the fourth step, all news articles were assigned to the categories based on their title and abstract. Some articles could not be assigned to one of the 10 categories. Therefore, three categories were added: company viewpoint, court judgment, and public debate. In this way, 119 news articles referred to privacy scandals, and 225 were marked as unclear or ambiguous, requiring further in-depth review. In the fifth step, the two researchers classified the 225 articles marked as unclear for categorization by studying their content and references in detail, resulting in 33 additional articles about privacy scandals. In the sixth step, the researchers merged the news articles from steps 4 and 5. Since many of the resulting 152 news articles reported on the same cases, the researchers assigned the articles to their respective cases in the seventh step. The researchers excluded all cases not referring to privacy scandals related to Facebook or Google in the next step. This procedure resulted in 21 identified cases (see Table 2).

Table 2. Overview of privacy scandals with the involvement of Facebook and Google

No.	Facebook	Google	Case description	Exemplary link
1	X		Facebook receives data (e.g., heart rates) from popular apps.	cnet.co/3mPi1jq
2	X		VPN service Onavo Protect shared user data with Facebook.	cnet.co/3oVcrhl
3	X		Facebook gathers personal data from Pregnancy+ and other apps.	cnet.co/2SZlxZv
4	X		Facebook, This Is Your Digital Life and Cambridge Analytica.	cnet.co/2Vx3Ith
5	X		Cambri. Analytica gathered Facebook data via a “sex compass” quiz.	cnet.co/2HxGucc
6	X		Facebook uses “like” buttons to collect data on individuals.	cnet.co/2qEPbqB
7	X		Facebook app CubeYou collected data through personality quizzes.	cnet.co/2IHLOcV
8	X		Facebook tracks users and ex-employees who are potential threats.	cnet.co/3kTY5Lu
9	X		Facebook paid teens to access their browsing history and phone.	cnet.co/3kIayC8
10	X		Facebook sued over the collection of mobile call and text data.	cnet.co/3oHJ4is
11	X		Australian sports event offers Wi-Fi and shares data with Facebook.	cnet.co/3egZA43
12	X		Facebook shared admitted user data access to dozens of companies.	cnet.co/2Mimd2v

13	X	X	Up to 17,000 apps tracked individuals via their advertising IDs.	cnet.co/2Bx97Sf
14	X	X	Thousands of apps on Android are tracking children.	cnet.co/2IHKLK1
15	X	X	Facebook and Google use “dark patterns” to trick people.	cnet.co/3emckql
16		X	YouTube collects data on child viewers younger than 13.	cnet.co/2NqbjTB
17		X	Google tracked individuals’ locations without consent.	cnet.co/2GxsMVr
18		X	Android infers data through passive means.	cnet.co/2wkmNxv
19		X	Google accused of secretly collecting data via its Nest Secure hub.	cnet.co/2TFdwvj
20		X	Google monitors people via Screenwise Meter in exchange for gifts.	cnet.co/2JarzH5
21		X	Google had deal with Mastercard to receive data about retail sales.	cnet.co/3oEM8vJ

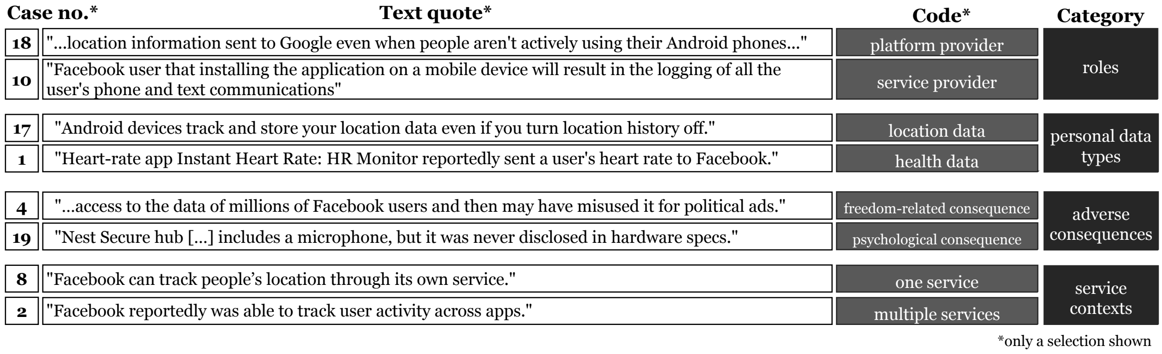
In the final step, the data material for each case was enriched by a backward search using the links in the news articles. This procedure enabled the collection of further documents from diverse sources (e.g., further news articles, studies, court decisions) and increased the validity of our study (Table 3). In addition, we ensured that the scandals were verified by other sources and not biased by a (media) source.

Table 3. Data material

	News Articles	Government Press Releases	Privacy Policies	Party Websites	Court Decisions	Studies	Technical Documents	Blogs	Σ
Facebook	174	10	3	6	1	2	4	4	204
Google	61	6	2	6	0	3	5	4	87

18.3.2 Data Analysis

The subsequent data analysis aimed to understand the roles of Big Tech companies (in our study Facebook and Google) in data ecosystems. Guided by Saldaña’s codes-to-theory process and advice that a rigorous analysis of qualitative data requires multiple coding iterations (2015), we conducted two coding cycles (see Figure 3). In the first coding cycle, we combined induction and deduction to code the plain text (Elo and Kyngäs 2008; Mayring 2004). Induction allowed us an open coding of all case-specific characteristics relevant to our research. For example, we labeled the several types of personal data mentioned throughout the cases. If a described practice was limited to one service context, the practice was coded as a single service. We considered for the service context the value proposition and the promise of value that a service delivers to an individual (Chandler and Lusch 2015). If the article text or related documents in the case database gave indications of practices that could not be assigned to the value proposition and thus to more than one service context, we coded the practice as multiple services. Deduction guided us with a priori codes to look for in the data material. For example, platform providers interpose their platform between individuals and service providers and enable interaction (Riedl et al. 2009; Van Alstyne et al. 2016). In addition, companies providing services to users involve other (third) parties for reasons such as performance management or advertisement (Binns et al. 2018). These insights about the roles in digital interaction guided us in data analysis. In addition, the different types of adverse consequences resulting from companies' access to users' personal data (Karwatzki et al. 2017) helped us achieve consistent codes.



Case no.*	Text quote*	Code*	Category
18	"...location information sent to Google even when people aren't actively using their Android phones..."	platform provider	roles
10	"Facebook user that installing the application on a mobile device will result in the logging of all the user's phone and text communications"	service provider	
17	"Android devices track and store your location data even if you turn location history off."	location data	personal data types
1	"Heart-rate app Instant Heart Rate: HR Monitor reportedly sent a user's heart rate to Facebook."	health data	
4	"...access to the data of millions of Facebook users and then may have misused it for political ads."	freedom-related consequence	adverse consequences
19	"Nest Secure hub [...] includes a microphone, but it was never disclosed in hardware specs."	psychological consequence	
8	"Facebook can track people's location through its own service."	one service	service contexts
2	"Facebook reportedly was able to track user activity across apps."	multiple services	

*only a selection shown

Figure 3. Extract of the Coding Scheme

We combined the codes in the second coding cycle by constantly comparing and grouping them into broader categories (Saldaña 2015). For example, codes such as "platform" and "service provider" were grouped into the category "roles." The coding cycles were executed separately by two researchers to enhance the reliability of the analysis and ensure that codes were at an appropriate level of abstraction without information loss. The researchers conducted inter-coder agreement tests to reduce the coding bias and reach a consensus by comparing the assigned codes and recoding the data (Saldaña 2015).

18.4 Results

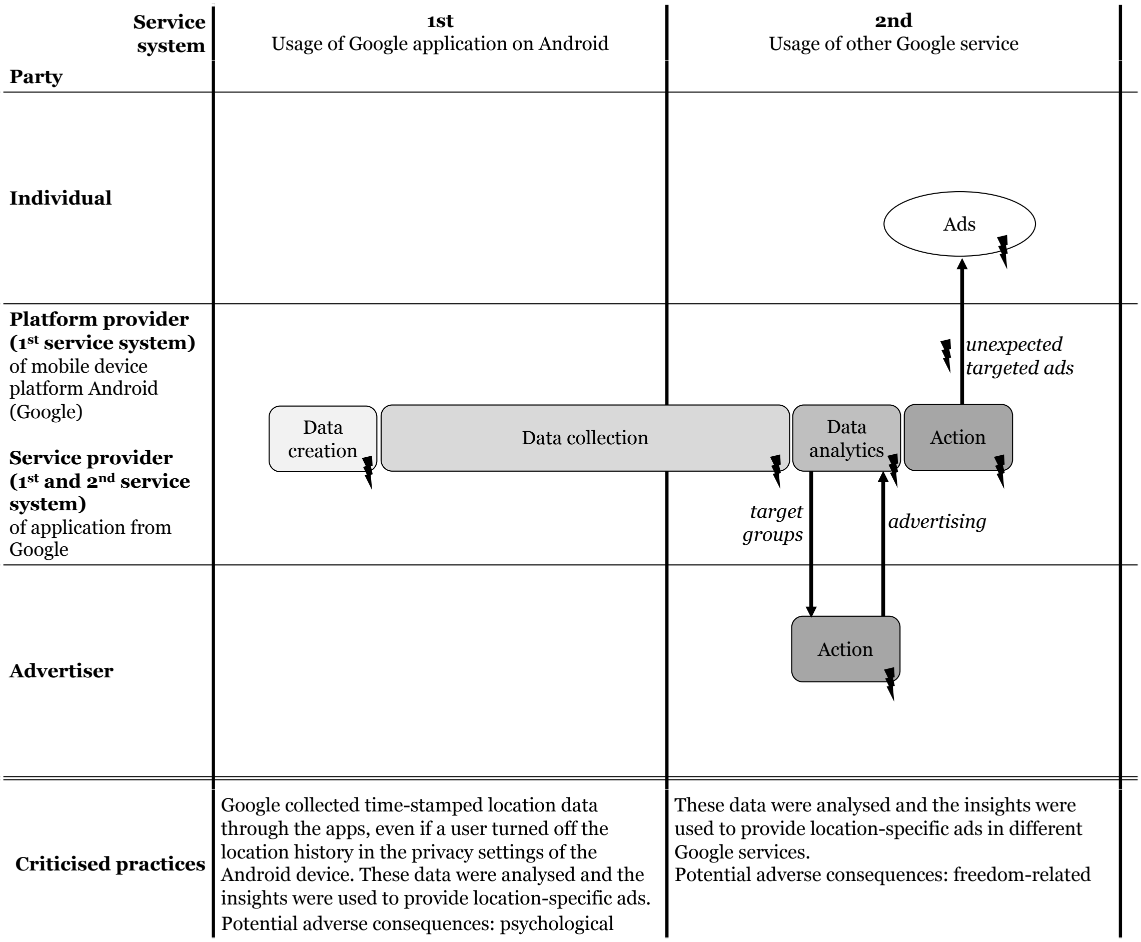
Our results show that Google and Facebook have established proliferating roles as opposed to an individual that enable access to personal data in data ecosystems. These companies assume the roles of platform provider, service provider, or third party to collect personal data (see Table 1).

Table 4. Case classification according to the data collecting role of Facebook and Google

	Company	
Role	Facebook	Google
Platform Provider	3 cases (nos. 4, 5, and 7)	2 cases (nos. 17 and 18)
Service Provider	6 cases (nos. 2, 8, 9, 10, and 15)	6 cases (nos. 15, 16, 18, 19, 20 and 21)
Third-Party	7 cases (nos. 1, 3, 6, 11, 12, 13 and 14)	2 cases (nos. 13 and 14)

18.4.1 The Role of Big Tech Companies as Platform Providers

The investigated cases show that Facebook collected users' personal data as a platform provider while a user interacts with an app accessible via the platform. The issue is shown in Google's practice in its role in providing the mobile device platform Android as visualized in Figure 4 (case no. 18). In detail, Google's Android sent location information to Google servers even when people are not actively using their Android phones. Moreover, Google's Android tracked location data even if an individual turned location history off in the device privacy settings.


Service system
Party
1st
Usage of Google application on Android
2nd
Usage of other Google service
Individual
Platform provider (1st service system) of mobile device platform Android (Google)
Service provider (1st and 2nd service system) of application from Google
Advertiser
Ads
unexpected targeted ads
Data creation
Data collection
Data analytics
Action
target groups
advertising
Action
Criticised practices

Google collected time-stamped location data through the apps, even if a user turned off the location history in the privacy settings of the Android device. These data were analysed and the insights were used to provide location-specific ads. Potential adverse consequences: psychological

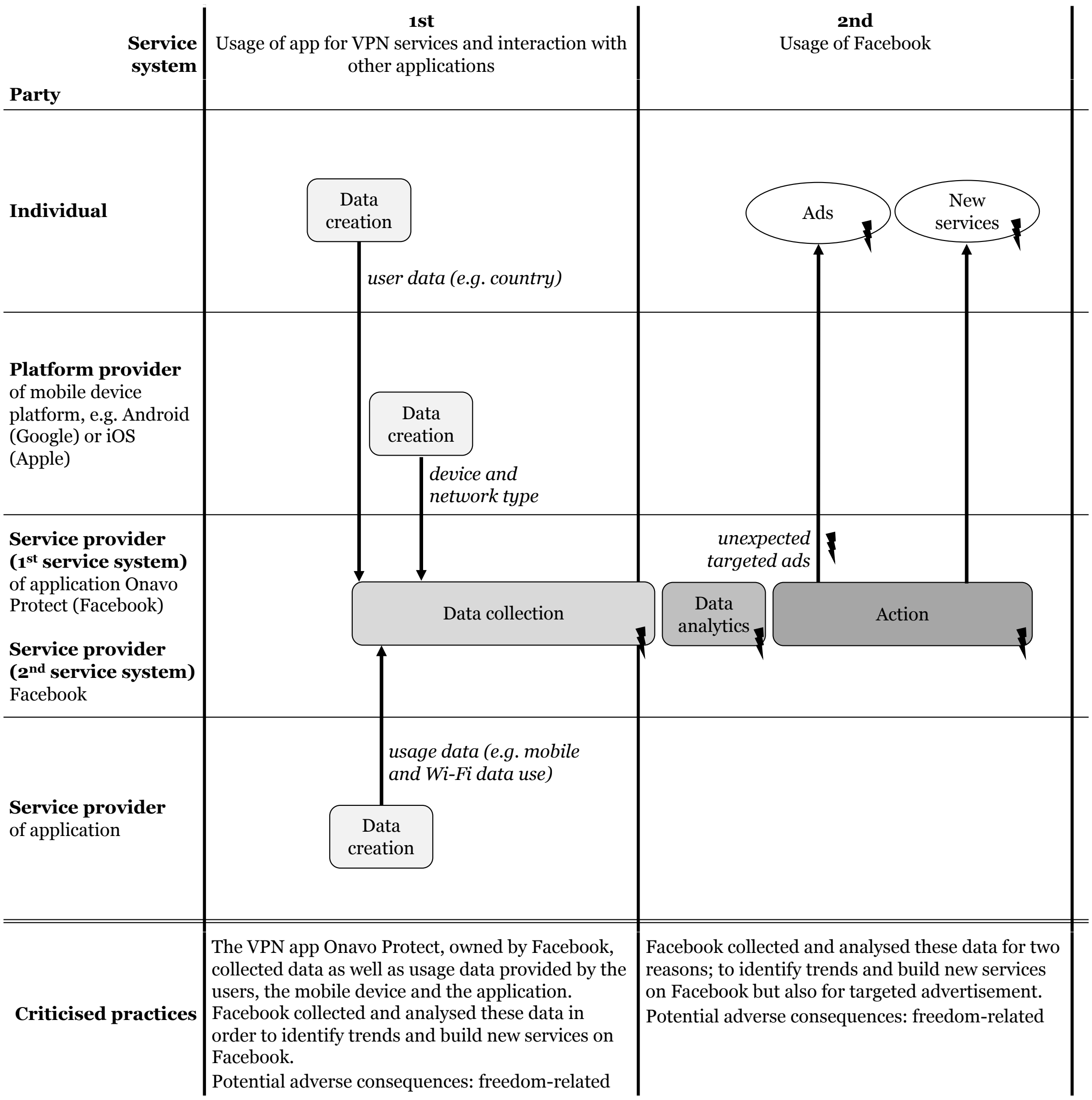
These data were analysed and the insights were used to provide location-specific ads in different Google services. Potential adverse consequences: freedom-related

Figure 4. Illustration of case no. 18

In the Cambridge Analytica scandal (case no. 4), a personality quiz app was accessible on the Facebook platform. The app was available on the platform's app store and was used by 270,000 users. Similarly, case nos. 5 and 7 indicate that Facebook, in its role as a platform provider, may access the data created by individuals using apps on the platform. The results show that the role of platform provider provides and related platforms are a suitable interface between individuals and digital services to accumulate personal data. The role of the platform provider enables access to data created when individuals use services via the platform. However, the case analysis revealed that at least two other roles are essential for sustaining personal data collection.

18.4.2 The Role of Big Tech companies as Service Providers

The second central role for personal data accumulation is the service provider role. In case no. 2, Facebook provides the virtual private network (VPN) service "Onavo" (Figure 5). The app should offer VPN functions such that users may send and receive data via a private network on their phones. However, the app (and thus, Facebook) used the granted permissions to access and track data on users' online activity via the mobile device across apps. In this case, these collection practices were not clear to individuals and resulted in public criticism.


Service system
Party
1st
Usage of app for VPN services and interaction with other applications
2nd
Usage of Facebook
Individual
Data creation
user data (e.g. country)
Ads
New services
Platform provider of mobile device platform, e.g. Android (Google) or iOS (Apple)
Data creation
device and network type
Service provider (1st service system) of application Onavo Protect (Facebook)
Service provider (2nd service system) Facebook
unexpected targeted ads
Data collection
Data analytics
Action
usage data (e.g. mobile and Wi-Fi data use)
Service provider of application
Data creation
Criticised practices

The VPN app Onavo Protect, owned by Facebook, collected data as well as usage data provided by the users, the mobile device and the application. Facebook collected and analysed these data in order to identify trends and build new services on Facebook.
Potential adverse consequences: freedom-related

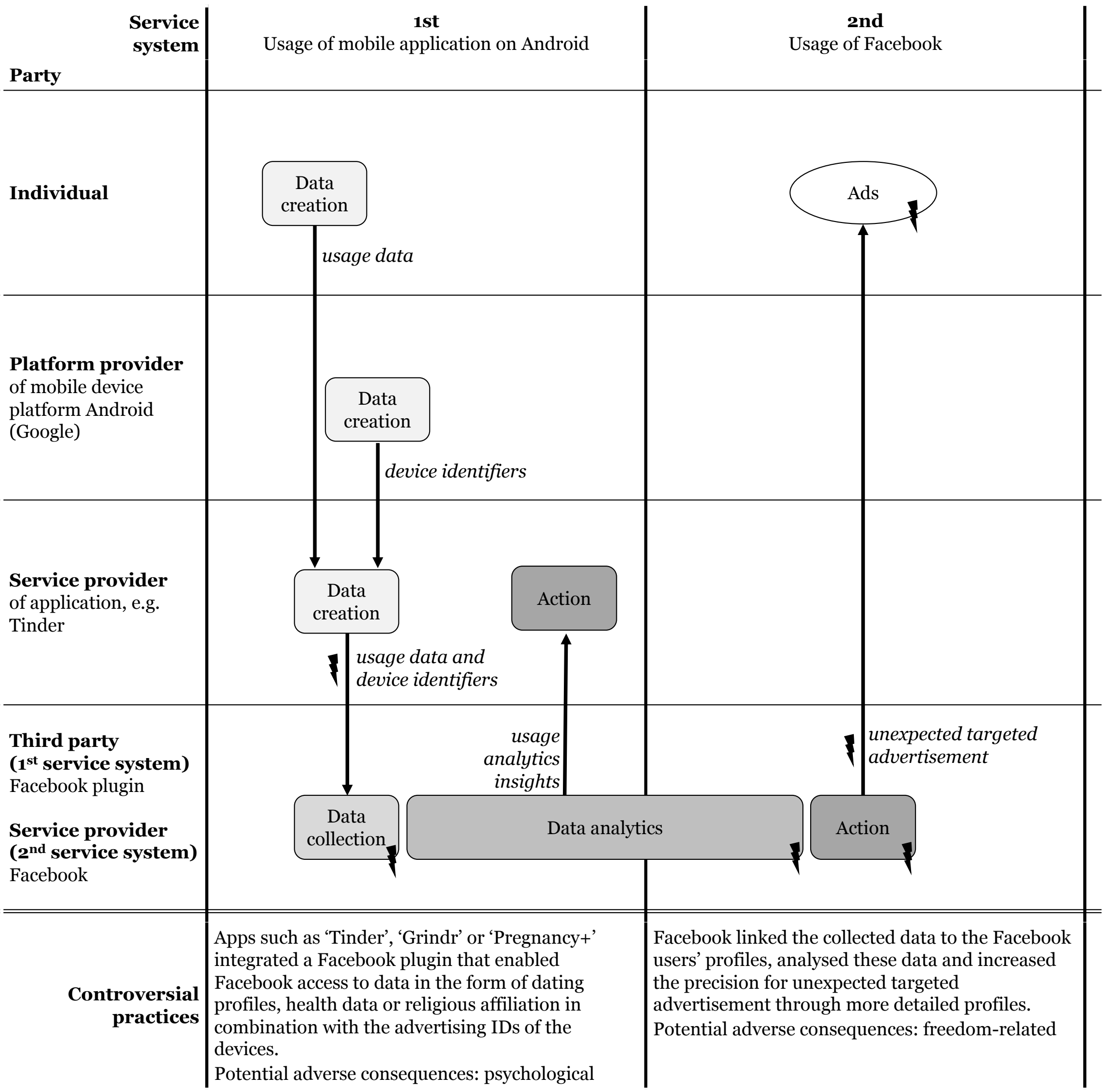
Facebook collected and analysed these data for two reasons; to identify trends and build new services on Facebook but also for targeted advertisement.
Potential adverse consequences: freedom-related

Figure 5. Illustration of case no. 2

Regarding the Facebook app, the personal data collection data is supported by an interface design that can result in users providing more data to Facebook than intended (case no. 15). Additionally, Facebook used this app to scrape metadata on calls and texts, such as the recipients of text messages and the time and duration of phone calls (case no. 10), and to collect device data which may include GPS location data, to promote safety and security online and offline (case no. 8). The cases show that Facebook is active in diverse service contexts but does not limit itself and the related data usage to the respective service context. As David Baser, a product management director of Facebook, wrote in a blog post: "When [a user] visit[s] a site or app that uses our services, we receive information even if [the user is] logged out or do[es]n't have a Facebook account" (Baser 2018) (case no. 6). Facebook also provides the app "Facebook Research," as part of which the company paid users, including teenagers, money to access their browsing history and phone (case no. 9). Like Facebook, Google assumes the accumulating role as a provider of services, e.g., YouTube (case no. 16) and the web browser Chrome (case no. 17). Google provided the Screenwise Meter app to collect personal data in exchange for gifts (case no. 20). In another case, Google collected user data when a user was logged into a Google account (case no. 21). In detail, when a user browsed across websites and the user clicked on an ad but did not purchase at that time, Google used data provided by Mastercard and tracked whether the individual purchased the product at a physical store within 30 days. This procedure enabled reporting of the sale to the advertiser who ran the ad online on Google. Here, the combination of two roles – as a service provider and as a third party to display ads on websites – has been central for Google. This duality of two roles for data accumulation and utilization is also apparent in case no. 18. Google as the platform provider of Android and in the role as the service provider of apps such as Google Chrome, collected location data.

18.4.3 The Role of Big Tech Companies as Third Parties

Various services and applications integrate Google and Facebook in the role of a third party. Case nos. 13 and 14 show that Google and Facebook are embedded into thousands of apps. Other cases refer to the issue that Facebook had integrations into a heart rate app (case no. 1), the app Pregnancy+ that processes sensitive health data (case no. 3) as visualized in Figure 6, or in an Australian sports event service (case no. 11). In addition, providers integrated the "like" button on various websites that enabled Facebook as a third party to accumulate behavioral surplus across the web (case no. 6). From a technical perspective, diverse software development kits or APIs are embedded into code. Examples include Facebook login, Facebook analytics, or Facebook ads. In case no. 12, Facebook admitted unusual access to user data to over 60 hardware and software companies. Facebook clarified that the related companies should build Facebook integrations into various services. Here, Facebook gave these companies access to user data for fostering an embedment as a third-party component in the next step.


Service system
Party
1st
Usage of mobile application on Android
2nd
Usage of Facebook
Individual
Data creation
usage data
Ads
Platform provider of mobile device platform Android (Google)
Data creation
device identifiers
Service provider of application, e.g. Tinder
Data creation
Action
usage data and device identifiers
Third party (1st service system) Facebook plugin
Service provider (2nd service system) Facebook
usage analytics insights
unexpected targeted advertisement
Data collection
Data analytics
Action
Controversial practices

Apps such as 'Tinder', 'Grindr' or 'Pregnancy+' integrated a Facebook plugin that enabled Facebook access to data in the form of dating profiles, health data or religious affiliation in combination with the advertising IDs of the devices.
Potential adverse consequences: psychological

Facebook linked the collected data to the Facebook users' profiles, analysed these data and increased the precision for unexpected targeted advertisement through more detailed profiles.
Potential adverse consequences: freedom-related

Figure 6. Illustration of case no. 3

18.4.4 Rebounding Effects across Service Contexts

As the results show, Google and Facebook accomplished the existence in diverse service contexts around users to collect personal data. Both companies use the roles of platform providers, service providers, and third parties. Both occupy practices under different names such as "Onavo VPN" or "Screenwise Meter." The Big Tech companies typically link the personal data practices to a single privacy policy. Here, the data accumulation by using various sources – no matter on which role basis and from which service context – is summarized under one umbrella and for a diverse set of purposes for which individuals provide consent. Following this, the companies create rebounding effects in the vastness of data ecosystems that are likely to be unanticipated by individuals. We define rebounding effects as information privacy violations for individuals in data ecosystems based on opaque data accumulation from one or multiple service contexts. These effects consist of processed data flowing from actors in data ecosystems to individuals, leading to adverse consequences. Rebounding effects build on users' lack of transparency in opaque data collection across service contexts. Big Tech companies particularly create rebounding effects because of their various roles in numerous services contexts built around commodifying a huge amount of personal data. In this regard, individuals no longer have control over their data and related practices in data ecosystems. Access to personal data may perpetuate adverse consequences (Karwatzki et al. 2017). Too little information is available in the cases to make detailed statements regarding the existence and depth of such consequences.

Given the business model of Google and Facebook, the rebounding effect is typically shown in the form of targeted advertisements. In case no. 17, Google used these location data to target geography-specific ads in other service contexts. In the data collecting role of providing the service YouTube (case no. 16), the data such as location or device information of users younger than 13 years of age were used for targeted ads (case no. 16). Concerning Facebook's app "Onavo Protect," Facebook’s internal-market researchers analyzed the collected data of different service contexts and utilized them by modifying their services (case no. 2). In addition, the rebounding effects base on personal data collection were also central in the Facebook and Cambridge Analytica scandal (case nos. 4 and 5). Initially, Facebook acted as a platform provider where the quiz app 'This Is Your Digital Life' was used by individuals. This app created various personal data and collected further data accessible via the Facebook platform. Later, Cambridge Analytica used these data for creating psychological profiles. Following, Facebook provided detailed opportunities for targeted ads and psychological profiles that Cambridge Analytica used. Facebook, in turn, displayed the targeted political advertising to the user, for example, in the related timeline in the role as a service provider.

In addition, in diverse cases exist uncertainty about the rebounding effects. In the case about the Nest Secure hub case, the web-connected home security system included a microphone that Google never disclosed in hardware specs (case no. 19). Members of the US Senate Commerce Committee demanded more information and stated that "Google's failure to disclose a microphone within its Nest Secure product raises serious questions about its commitment to consumer transparency and disclosure […] As consumer technology becomes ever more advanced, it is essential that consumers know the capabilities of the devices they are bringing into their homes so they can make informed choices" (Nieva 2019). Another example is the revelation that a dormant Android phone running the service Chrome in the background sent location information to Google 340 times during a 24-hour period (case no. 18).

Summing up, companies make use of the three roles in their extensive data ecosystems for personal data accumulation. Unanticipated rebounding effects that followed resulted in other service contexts in the vastness of data ecosystems.

18.4.5 Legal assessment regarding the applicability of the GDPR

Our results show Big Tech companies' practices in data ecosystems that accumulate and use personal data for rebounding effects in other service contexts. In the following, we assess our results from a legal perspective by questioning the applicability of the GDPR to regulate Big Tech companies' practices.

The set of roles defined by the GDPR and formulated in an abstractive manner may give the impression that every company in its related role and actions is sufficiently regulated. However, the dangers stemming from the processing of personal data can vary greatly. Not all of them are related to the individual processing act itself and its environments, such as the personnel or the technical architecture surrounding it. As the practices indicate, a distinctive danger can arise from the totality of different processing acts and the quantity of processed data. Given the ideal of the GDPR, all data processing operations would be dissected and legally analyzed independently. First, the legal basis of each single data processing operation would be in question. Within the GDPR's framework for lawful data processing, consent is one of six legal bases, albeit arguably the most important and widely used (GDPR, 2016, Art. 6 (1)). Typically, Google and Facebook link all their personal data operations as platform providers, service providers, and third parties to a single privacy policy. This policy includes the description of various data processing operations for various purposes and raises the question of valid consent. Consent is valid when it is freely given, unambiguously voiced for a specific purpose or set of purposes, and based on an informed decision (GDPR, 2016, Art. 6 (1)). Processing can be lawful without a user's consent when necessary for the performance of a contract or when its purpose serves the company's legitimate interests and the user's interests do not outweigh those interests. Here, the lawfulness of decoupling personal data from the service context and the re-usage in another service context with rebounding effects would have to be answered. In this relation, there is potential for a regulatory vacuum for two distinct reasons.

Firstly, under the GDPR, an entity processing different types of personal data through various stages and situations is a controller in each of these instances and for each processing operation. However, not all dangers related to the processing of personal data stem from such an individual processing operation: as indicated, the whole danger can be more than the sum of its (data processing) parts. It can be enhanced by combining all the processing operations or the variety of contexts from which the affected data stem. The GDPR tries to consider this heterogeneity of sources of danger by bestowing upon data controllers' obligations that also aim at the processing environment. For example, certain organizational and technical measures must be taken to ensure that the controller complies with all specific data protection and data security provisions of the GDPR and can demonstrate this compliance at any given point, as Art. 24 declares. These obligations concretize Art. 5 (2), which establishes the principle of accountability as one of the cornerstones of lawful processing. Measures to be taken by a controller depend on the scope, context, purpose, severity, probability of the occurrence of risks to the rights of data subjects, and the need to be "suitable" and "appropriate." Essentially, there is no general method of defining measures that every controller can take without considering the context and its specifics. Still, not every type of risk and danger might be covered by these obligations since, at the end of the day, they are still rooted in the concept of accountability for specific processing acts.

Secondly, not every critical participation act is necessarily covered by the GDPR. Big Tech companies such as Google or Facebook may tend to influence other data controllers in ways that shape and evolve the accumulation and proliferation of personal data. They define data processing circumstances as a platform provider or as a third party due to their market power. Some development, however, has been noticeable here as well. Starting in 2018 and in several court cases since, the European Court of Justice (ECJ) has opened the door for a more extensive application of the role of joint controllership. This concept, found in Art. 4 No. 7 and Art. 26 GDPR, attempts to avoid such a vacuum by allocating responsibility to all the groups that are sufficiently involved in such cases of distributed actions and influencing data processing acts. The primary goal is to provide sufficient clarity to allow and ensure effective application and compliance in practice (European Commission 2010). In theory, this can give a regulatory handle to apply on actors that apply modern, nontraditional influence on data processing acts carried out by other data controllers. In practice, though, it is still a barely sketched out the first draft with many undefined variables (e.g., what are the obligations? How far do they reach?).

These discussed points show that despite modernization efforts on the legislative and judiciary level, a legal vacuum remains for Big Tech companies and their proliferated architectures with a trifold role involvement within diverse service contexts that do not fit the single individual role model pursued by the GDPR. An isolated view on a single processing operation and the related juridical role according to the GDPR contrasts with the identified repeating practices, which are targeted on the countless number of data processing operations in diverse roles across service contexts. For the GDPR to cover these modern phenomena, a new actor perspective and interpretation are needed to cope with companies' accumulation and utilization practices related to Big Tech companies. Regulators can consider these results in three ways. First, in trials, by the interpretation of the GDPR. Judgments by the European Court of Justice (ECJ) already show the legal potential of joint controllership and the related obligations.

Second, a constant reevaluation, development, and improvement of the GDPR and its obligations and roles. The GDPR itself endorses such endeavors, as seen in its provisions regarding regular evaluations (GDPR 2016, Art. 97 No. 1). Such a legalistic approach would be preferable as it allows for fewer unclarities and more specificity than the judicial interpretation of current norms. The third way would be to apply other regulatory frameworks outside of data protection that follow a similar goal and bring their own regulatory toolbox. Antitrust law is one field that offers a valuable basis.

18.4.6 Validation based on Recent Cases

We reflect on our results by validating whether Google and Facebook still make use of their roles across service contexts and whether the GDPR was capable of addressing Big Tech companies' practices. To validate our results via recent cases, we defined a second investigative time frame from January 2020 to March 2021. Here, we identified other cases for which we provide some examples (Table 5).

Table 5. Examples of recent Cases with the involvement of Facebook and Google

No	Facebook	Google	Case Description	Link
22	X		Facebook's SDK integration into Zoom accesses diverse data	cnet.co/3ujew9c
23	X		Instagram may have used iPhone cameras to spy on users	cnet.co/3t98Ehe
24		X	Google still tracks users in private web browser modes	cnet.co/3ecjI92

In the context of the iOS app of the videoconferencing tool Zoom, personal data were accumulated by Facebook in its role as a third party due to its integration of 'Login with Facebook' into the app (case no. 22). The Zoom app transmitted data to Facebook whenever a user opened the app, including what phone or device was used, phone carrier, location, and unique advertising identifier. Zoom stated that they take its users' privacy extremely seriously. The idea behind the 'Login with Facebook' implementation by the SDK was to provide users with another convenient way to access the service. However, the company was made aware that the Facebook SDK was accumulating unnecessary device data via the app leading to the removal of the third-party component.

Case no. 23 refers to the issue that Facebook, in the service-providing role of Instagram, may have used iPhone cameras to spy on users. As an improvement, Apple's iOS 14 reports at the top of the screen when an application uses the device's camera or microphone. In this case, users did not actively use the camera in the app—a lawsuit in the US District Court in San Francisco accused of Instagram accessing users' smartphone cameras. In detail, the service is accused of monitoring users without permission. The service may have been able to monitor users' most intimate moments, including those in the privacy of their own homes while the app is open. However, Facebook stated that the issue appears to be related to a bug, and the app would not use the camera, even though Apple's iOS 14 software indicated it did.

In a third example, Google's data collection is criticized. In detail, while users browsed in private mode, the company collected data through their third-party role in the form of Google Analytics, Google Ad Manager, or further website plugins. Google noted earlier that when users open a new private tab in Google Chrome, they are informed that websites (and involved third parties) might collect information about their browsing activity during the browsing session despite using the private mode.

To summarize, the given examples of recent cases substantiate our results. Both Facebook and Google still make use of their multiple roles. They accumulate personal data across service contexts so that rebound effects can follow. In this regard, the GDPR did not regulate Big Tech companies accumulating practices and, thus, did not achieve to protect individuals' privacy in data ecosystems.

18.5 Discussion

In this study, we were able to gain insights into the data ecosystems of Big Tech companies. Big Tech companies proliferate in the digital interaction of an individual as a platform provider, service provider, and third party (see Figure 7). Involvement in a digital interaction leads to access to personal data. This proliferation opens the door for decoupling personal data from the original service context, enabling the company to enter spaces where transparency is limited. It is immensely difficult to assess the following utilization practices. Thus, regulation fails to materialize. Consequently, the accumulated data are decoupled from the original service context and are diffused into other service contexts for rebounding effects on the individual concerned.

We contribute to research on both information privacy and data ecosystems. Information on modeling the movement and lifecycle of personal data once released by an individual is scarce (Conger et al. 2013; Spiekermann and Novotny 2015). We highlight that a single company may take multiple roles across different service contexts. Here, besides data that flow away from the individuals, also data flow back to an individual with rebounding effects. In such ecosystems, the control over what happens with personal data is no longer in the decision sphere of individuals. As Zuboff (2019) highlighted, the control over personal data is redistributed. Thus, the conceptualization of one's control of personal data of privacy studies in the IS field is too limited to deepen the understanding regarding information privacy in data ecosystems, as concerns and adverse consequences appear not only in a single digital interaction but also across interactions service contexts. This aspect is particularly privacy virulent for Big Tech companies due to their diverse appearance in different contexts. At the same time, new questions arise about the concepts of concern in privacy research (Karwatzki et al. 2017; Smith et al. 1996). The clear differentiation of what falls under improper access or secondary usage is hardly determinable in data ecosystems as, for example, users agree to privacy policies with variously specified personal data practices.

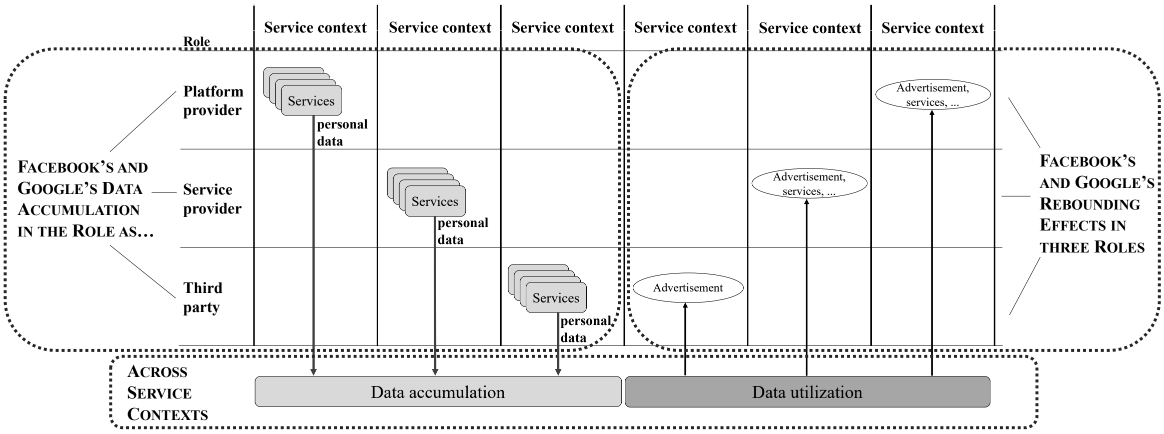


Figure 7. Multi-role actors and rebounding effects in data ecosystems

In addition, this study contributes to the existing research on data ecosystems. Big Tech companies are often referred to in common parlance or studied solely as platforms (Constantinides et al. 2018), which does not reflect the extent of their roles in data ecosystems as demonstrated. This study offers insights into the respective data ecosystems of Google and Facebook. Our results show that many connections into service contexts have a high data ecosystem-connecting mechanism for accumulating personal data across service contexts. Oliveira et al. (2019) already stated that actors could perform one or multiple roles in data ecosystems. However, limited knowledge exists regarding the roles relevant to information privacy. This study extends this knowledge by specifying the three roles Big Tech companies take in data ecosystems to accumulate personal data and which effects result. In addition, we extend the view on data ecosystems as existing studies address less the negative sides of data ecosystems (Oliveira et al. 2019). In addition, Big Tech companies provide integrations in their roles as third parties (such as 'share' or 'like' buttons, advertisements, or application performance management) that service providers can use. Service providers have to accept the conditions imposed by Big Tech companies or omit Big Tech third-party integrations, which may be problematic given that alternatives rarely exist (e.g., for sharing buttons) or, if they do, they may be less efficient (e.g., regarding application performance or advertisement). Thus, Big Tech companies act as influential actors in data ecosystems that can support or inhibit values that affect their interests in data ecosystems.

This work also indicates a prudent way forward for the GDPR, in combination with other regulatory fields, to move out in front of Big Tech companies in data ecosystems. A regulation that limits itself on fine-granular assessment of a single data processing operation cannot cope with Big Tech companies' data ecosystems. In detail, a specific regulatory role that reclassifies companies masquerading as a platform provider, service provider, and third-party is tailored to their spheres of influence and considers the totality of their data processing activities by stressing service context changes might be a prudent way forward and an opportunity to incorporate some of our research findings to the legal realm. This consideration requires a change of perspective from individual data processing operations to considering actors and scaled practices in multiple services. Ideally, a newfound role would also need to be considered in a way that recognizes and utilizes the potential of applying other regulatory frameworks outside of data protection that follow a similar goal and brings their own regulatory toolbox to the table. A decision by an antitrust law authority factored in data protection law to come to the decision that the obligatory sharing of user data in the Facebook group (now: Meta Platforms) between Facebook, WhatsApp, Oculus Masquerade, and Instagram when using any of these services was unlawful because the group's dominant position did not leave users any free choice and nullified their consent (German Federal Cartel Office 2019).

Our research is not without limitations. First, our first data source in the form of new articles may be pre-filtered by journalists. Due to this reason, we used diverse other sources in the form of court decisions, privacy policies, blogs, studies, party websites, government press releases, or technical documents to increase the validity of our results. Second, our focus was on privacy scandals with the involvement of Google or Facebook as major representatives of Big tech companies. Future studies could consider other Big Tech companies and smaller data aggregators to deepen the understanding abound rebounding effects in data ecosystems. Third, the rebounding effects are not traceable in all cases as Google and Facebook try to keep their practices opaque. At this point, to get a deeper understanding of the inner workings of data ecosystems, novel research methods that solve problems of data access about ecosystems may be fruitful. Fourth, we could not study the whole data ecosystems of Big Tech companies. We rather focused on parts of the data ecosystems based on the analysis of privacy scandals and relevant to information privacy. In this regard, it is unclear how to determine data ecosystems' boundaries. Future research is required to work out this conceptual gap. Fifth, this study builds on investigating privacy scandals involving multiple individuals. However, research shows that individuals' privacy awareness differs (Kumaraguru and Cranor 2005). On an individual level, not every investigated personal data practice or rebounding effect may be necessarily perceived as a privacy violation by each individual. Future research can address which practices in data ecosystems are less considered privacy critical.

18.6 Conclusion

This study spotlighted Google and Facebook as major representatives of Big Tech companies and their roles regarding information privacy in data ecosystems. We unveil the masquerade and show that the companies operate in more roles than just as platform providers to enable interaction between users and service providers. Google and Facebook also provide their services and aim that other service providers inject their third-party integrations into a plethora of services. These connections between the accumulation and the rebounding effects are difficult to reveal due to the secrecy established of the inner workings of their data ecosystems. With this study, we support a substantial basis for the debate among researchers, regulators, and practitioners and point out potential regulatory approaches to data ecosystems in consideration of the GDPR. The GDPR – combined with other regulatory frameworks – can be a springboard to regulate the practices considering a new actor perspective.

Our systemic perspective on data ecosystems reveals for the future that researchers may require an additional privacy conceptualization since not individuals but companies in data ecosystems control the decisions regarding personal data processing operations, also highlighted by Zuboff (2019). Future studies could consider getting more details by trying to model complex data ecosystems. In addition, rebounding effects are a new privacy phenomenon to be studied in the future. Quantitative studies could consider this described phenomenon and investigate the individuals' awareness and concerns. In addition, IS research should consider that companies take multiple roles leading to privacy violations. Here, research could address how service providers that involve other parties can create privacy-sensitive ecosystems. When service providers embed third parties, they may be unaware of data accumulation practices by the third party. Here, design science research that creates solutions to support software developers' decision-making regarding a careful embedding of third-party plugins in digital services could be valuable.

18.7 References

Aaen, J., Nielsen, J.A., and Carugati, A. 2021. "The dark side of data ecosystems: A longitudinal study of the DAMD project," *European Journal of Information Systems*, pp. 1-25.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), Jan 30, pp. 509-514.

Andrew, J., and Baker, M. 2019. "The general data protection regulation in the age of surveillance capitalism," *Journal of Business Ethics*, pp. 1-14.

Baser, D. 2018. "Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?" Retrieved 10.03., 2021, from https://about.fb.com/news/2018/04/data-off-facebook/

Bélanger, F., and Xu, H. 2015. "The role of information systems research in shaping the future of information privacy," *Information Systems Journal* (25:6), pp. 573-578.

Benbasat, I., Goldstein, D.K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3).

Benedict, M. 2018. "Modelling ecosystems in information systems–a typology approach," *Proceedings of the Multikonferenz Wirtschaftsinformatik*, pp. 453-464.

Benson, V., Saridakis, G., and Tennakoon, H. 2015. "Information disclosure of social media users: does control over personal information, user awareness and security notices matter?," *Information Technology & People* (28:3), pp. 426-441.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., and Shadbolt, N. 2018. "Third Party Tracking in the Mobile Ecosystem," *10th ACM Conference on Web Science*.

Cabinakova, J., Zimmermann, C., and Mueller, G. 2016. "An empirical analysis of privacy dashboard acceptance: the google case."

Center, P.R. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information."

Chandler, J.D., and Lusch, R.F. 2015. "Service Systems: A Broadened Framework and Research Agenda on Value Propositions, Engagement, and Service Experience," *Journal of Service Research*Feb.

Choi, B.C., and Land, L. 2016. "The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage," *Information & Management* (53:7), pp. 868-877.

Conger, S., Pratt, J.H., and Loch, K.D. 2013. "Personal information privacy and emerging technologies," *Information Systems Journal* (23:5), Sep, pp. 401-417.

Constantinides, P., Henfridsson, O., and Parker, G.G. 2018. "Introduction—Platforms and Infrastructures in the Digital Age," *Information Systems Research*, pp. 381-400.

de la Torre, L. 2018. "GDPR matchup: The California Consumer Privacy Act 2018." Retrieved June 05, 2019, from https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/

Demchenko, Y., De Laat, C., and Membrey, P. 2014. "Defining architecture components of the Big Data Ecosystem," *2014 International conference on collaboration technologies and systems (CTS)*: IEEE, pp. 104-112.

Dinev, T., McConnell, A.R., and Smith, H.J. 2015. "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box," *Information Systems Research* (26:4), pp. 639-655.

Elo, S., and Kyngäs, H. 2008. "The qualitative content analysis process," *Journal of advanced nursing* (62:1), pp. 107-115.

European Commission. 2010. "Article 29 Data Protection Working Party " in: *WP 169: Opinion 1/2010 on the concepts of "controller" and "processor"*. .

Faber, A., Riemhofer, M., Rehm, S.-V., and Bondel, G. 2019. "A systematic mapping study on business ecosystem types," in: *Americas Conference on Information Systems*.

GDPR. 2016. "General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Directive 95/46)," (59, pp. 1-88.

German Federal Cartel Office. 2019. "Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing."

Gopal, R., Hidaji, H., Patterson, R., Rolland, E., and Zhdanov, D. 2018. "How much to share with third parties? User privacy concerns and website dilemmas," *MIS Quarterly* (42:1), pp. 143-164.

Hong, W.Y., and Thong, J.Y.L. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), Mar, pp. 275-298.

Kallemeyn, D., and Chipidza, W. 2021. "Towards a Forward-Looking Conceptualization of Privacy," *Proceedings of the International Conference on Information Systems (ICIS)*, Texas (USA).

Karwatzki, S., Trenz, M., Tuunainen, V.K., and Veit, D. 2017. "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence," *European Journal of Information Systems* (26:6), pp. 688-715.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal* (25:6), Nov, pp. 607-635.

Kohlbacher, F. 2006. "The use of qualitative content analysis in case study research," *Forum: Qualitative Social Research*, pp. 1-30.

Kumaraguru, P., and Cranor, L.F. 2005. *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University.

Lankton, N.K., and Tripp, J.F. 2013. "A quantitative and qualitative study of Facebook privacy using the antecedent-privacy concern-outcome macro model."

Lusch, R.F., and Vargo, S.L. 2014. *Service-dominant logic: Premises, perspectives, possibilities*. Cambridge University Press.

Manikas, K. 2016. "Revisiting software ecosystems research: A longitudinal literature study," *Journal of systems and software* (117, pp. 84-103.

Mayring, P. 2004. "Qualitative content analysis," *A companion to qualitative research*, pp. 159-176.

Mikalef, P., Popovič, A., Lundström, J.E., and Conboy, K. 2019. "Call for Papers: Special Issue on the Dark Side of Analytics and Artificial Intelligence," *European Journal of Information Systems*.

Moore, J. 1996. "The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems. Leadership." New York: Harper Business.

Nieva, R. 2019. "Senate demands Google CEO answer for hidden Nest microphone." Retrieved 15.02., 2021, from https://www.cnet.com/news/senate-demands-google-ceo-answer-for-hidden-nest-microphone/

Norberg, P.A., Horne, D.R., and Horne, D.A. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs* (41:1), Sum, pp. 100-126.

Oliveira, M.I.S., Lima, G.d.F.B., and Lóscio, B.F. 2019. "Investigations into Data Ecosystems: a systematic mapping study," *Knowledge and Information Systems* (61:2), pp. 589-630.

Oliveira, M.I.S., Oliveira, L.E.R., Batista, M.G.R., and Lóscio, B.F. 2018. "Towards a meta-model for data ecosystems," *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pp. 1-10.

Ozdemir, Z.D., Smith, H.J., and Benamati, J.H. 2017. "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study," *European Journal of Information Systems* (26:6), Nov, pp. 642-660.

Ponte, D. 2015. "Enabling an open data ecosystem," in: *European Conference on Information Systems.*

Proudfoot, J.G., Wilson, D., Valacich, J.S., and Byrd, M.D. 2018. "Saving face on Facebook: Privacy concerns, social benefits, and impression management," *Behaviour & Information Technology* (37:1), pp. 16-37.

Riedl, C., Boehmann, T., Leimeister, J.M., and Krcmar, H. 2009. "A framework for analysing service ecosystem capabilities to innovate," *Proceedings of the European Conference on Information Systems (ECIS)*, Verona (Italy).

Saldaña, J. 2015. The coding manual for qualitative researchers. SAGE.

SimilarWeb. 2019. "Top sites ranking for News And Media." Retrieved 25.02.2020, from https://www.similarweb.com/top-websites/category/news-and-media/technology-news

Smith, H.J., Milburg, S.J., and Burke, S.J. 1996. "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly* (20:2), pp. 167-196.

Spiekermann, S., and Novotny, A. 2015. "A vision for global privacy bridges: Technical and legal measures for international data markets," *Computer Law & Security Review* (31:2), pp. 181-200.

Steinbart, P., Keith, M., and Babb, J. 2017. "Measuring Privacy Concern and the Right to Be Forgotten," *Proceedings of the Hawaii International Conference on System Sciences*, Hawaii (USA).

Teubner, T., and Flath, C.M. 2019. "Privacy in the Sharing Economy," *Journal of the Association for Information Systems* (20:3), pp. 213-242.

Thompson, J.B. 2013. Political scandal: Power and visability in the media age. John Wiley & Sons.

Tiwana, A., Konsynski, B., and Bush, A.A. 2010. "Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics," *Information Systems Research* (21:4), pp. 675-687.

Van Alstyne, M.W., Parker, G.G., and Choudary, S.P. 2016. "Pipelines, platforms, and the new rules of strategy," *Harvard Business Review* (94:4), pp. 54-62.

Xu, C.M., Benbasat, I., and Cavusoglu, H. 2012. "Trusting those who trust you: A study on trust and privacy on Facebook."

Yin, R.K. 2009. Case Study Research: Design and Methods SAGE.

Zuboff, S. 2015. "Big other: surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology* (30:1), pp. 75-89.

Zuboff, S. 2019. The Age of Surveillance Capitalism. Profile Books.

Zuiderwijk, A., Janssen, M., and Davis, C. 2014. "Innovation with open data: Essential elements of open data ecosystems," *Information polity* (19:1, 2), pp. 17-33.

Appendix B: Eidesstattliche Versicherung

Hiermit erkläre ich,

Christian Kurtz, geboren am 09. Mai 1991 in Paderborn,

an Eides statt, dass ich die vorliegende Dissertationsschrift mit dem Titel

„Exploration of Information Privacy in Digital Ecosystems“

selbst verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel genutzt habe.

______________________________ ______________________________

Ort, Datum Unterschrift