Exploring Archetypes of Value Co-Destructive Privacy Practices

Christian Kurtz
Universität Hamburg (Germany)
Christian.Kurtz@uni-hamburg.de

Pascal Vogel
Universität Hamburg (Germany)
Pascal.Vogel@uni-hamburg.de

Martin Semmann
Universität Hamburg (Germany)
Martin.Semmann@uni-hamburg.de

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.

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.

URI: https://hdl.handle.net/10125/79505
978-0-9981331-5-7

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.

2. Theoretical foundations

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.

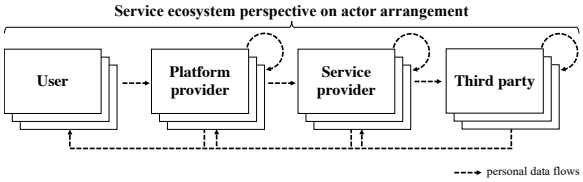

Figure 1. Simplified service ecosystem perspective (based on Kurtz et al. (2018) [24])

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.

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.

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. / Documents	1	2	3	4	5	6	7	∑
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**
∑	**7**	**7**	**6**	**12**	**6**	**7**	**12**	**57**

4. Multi-case analysis

In the following, we describe and analyze the identified cases that reported information privacy violations in different RIPs.

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].

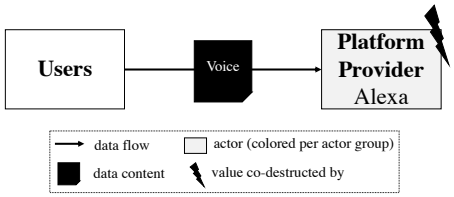

Figure 2. Case 1: VCD in the service system.

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.

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.

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.

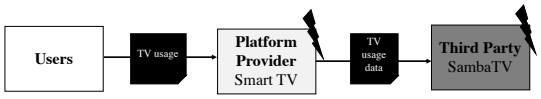

Figure 4. Case 3: VCD in the service system.

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.

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.

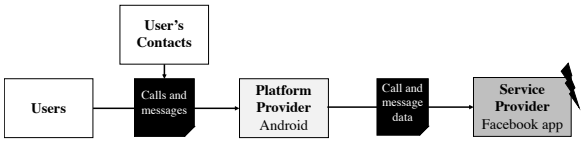

Figure 6. Case 4: VCD in the service system.

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.

4.5. Third-party in app track 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.

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.

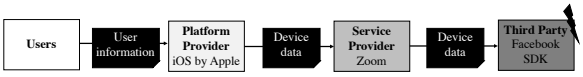

Figure 8. Case 6: VCD in the service system.

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.

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.

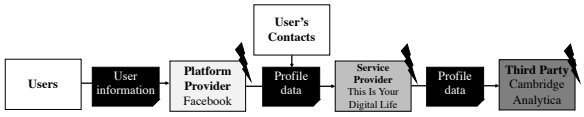

Figure 9. Case 7: VCD in the service system.

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.

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.

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			

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.

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].

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.

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.

8. Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality (project: Information Governance Technologies, LFF-FV 34).

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).