Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems

Christian Kurtz
University of Hamburg,
Department of Informatics
christian.kurtz@uni-hamburg.de

Florian Wittner
Hans-Bredow-Institut
for Media Research, Hamburg
f.wittner@hans-bredow-institut.de

Martin Semmann
University of Hamburg,
Department of Informatics
martin.semmann@uni-hamburg.de

Wolfgang Schulz
Hans-Bredow-Institut
for Media Research, Hamburg
w.schulz@hans-bredow-institut.de

Tilo Böhmann
University of Hamburg,
Department of Informatics
tilo.boehmann@uni-hamburg.de

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.

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 [1]. Moreover, Facebook shared information with apps, although this was technically revised before and should prevent such privacy-critical transmission [2]. 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 [3]. 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" [4]. Furthermore, he also stated in the context of the Cambridge Analytica case that he "[…] wouldn't be in this situation" [4].

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 [5]. 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.

URI: https://hdl.handle.net/10125/59943
ISBN: 978-0-9981331-2-6

2. Theoretical framework

2.1 Information privacy in service ecosystems

In this article, we focus on the diffusion of personal data respectively personal information in hyper-connected services. In general, the ways in which services are delivered have changed essentially in many respects [6]. Service delivery has likewise shifted from single services towards ecosystems of services [6, 7] (Figure 1). We posit these service ecosystems comprise users, platforms, frontend services, and backend services.

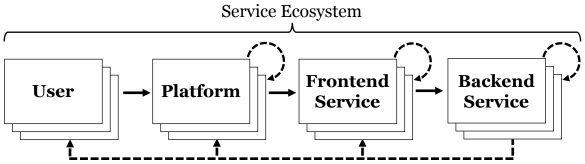

Figure 1. Adapted model of information privacy in service ecosystems [8]

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 [9, 10]. In this context, privacy risks and privacy concerns exist in the decision-making of users whether to share data [11, 12]. 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 [13].

Platforms facilitate multi-sided interactions of different actors [14, 15], typically between users and frontend services [16]. In this article, we define platforms as a set of digital resources that enable value-creating interactions between frontend services and users [15]. 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 [17]. Here, platforms act as intermediaries and can exert control over how data and service flows between platform participants [17, 18]. Examples for this are Apple's rules for developers [19].

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 [20]. The interactions of the actors result in the diffusion of personal data in hyper-connected services ecosystems [20]. 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 [21], where it remains to be seen to what extent the GDPR in form of data regulation can cover these challenges.

2.2 GDPR

In May 2018 the GDPR [22], 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 [23]. 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 [22, Art. 4 No. 7][1], 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 [22, Art. 4 No. 2]. These can include the collection, recording, organization, structuring, storage, adaptation, usage, disclosure, cf. In order to limit risks from acts of processing, the GDPR enjoins controllers with certain obligations that are meant to

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

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 [24]. 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 [25, 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" [26]. 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).

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" [27, 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?

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 [28]. 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 [3]. At the time that the case was formed, users had to manually opt-out of sharing their data with the apps used by friends [29]. 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 [30].

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 [31] 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 [32]. 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 [33]. 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.

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 [34]. 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 […]" [35, p. 2]. More precisely, RevealMobile focusses on mobile marketing by using such data to segment user groups for advertising [36].

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 [37]. During a testing period of 36 hours, the data was sent 16 times to the company RevealMobile [37]. 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 [38, 39]. On Apple's website (which corresponds to the iOS version of the case) [40] about location services in iOS, however, this is presented differently to the user. Thus, it is stated "Tap Don't Allow to prevent access" [40, 41]. 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 [42], the access to MAC addresses of network devices (such as WiFi routers) barred in iOS 11 [43]. 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" [25, 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 [26]. 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 [26]. 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.

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 [29]. 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

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 [22, Art. 6] and to inform their users about the ways they plan to use this data [22, Art. 13]. Concerning the legal basis, Facebook lists different kinds of potential bases on its website for different intended usage cases [44]. 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 [22, 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 [45].

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 [22, Art. 24].

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]" [22, 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 [46] 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 [43].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" [47].

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.

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.

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 [43], that "Facebook suspends 200 apps as part of investigation into data misuse" [48]. 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.

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.

7. References

[1] G. J. X. Dance, N. Confessore, and M. LaForgia, "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, 08.06.2018.
[2] The Guardian, "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, 10.06.2018.
[3] S. Frier,"FacebookSays There May Be More CambridgeAnalytica-SizedLeaks", https://www.bloomberg.com/news/articles/2018-04-26/facebook-says-there-may-be-more-cambridge-analytica-sized-leaks, 10.06.2018.
[4] J. C. Wong, "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, 10.05.2018.
[5] C. Kurtz, M. Semmann, and T. Böhmann, "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors" presented at the Americas Conference on Information Systems (AMCIS), New Orleans, 2018.
[6] T. Böhmann, J. M. Leimeister, and K. Möslein, "Service Systems Engineering" Business & Information Systems Engineering, vol. 6, 2014, pp. 73-79.
[7] S. L. Vargo and R. F. Lusch,"It's all B2B... and beyond: Toward a systems perspective of the market" Industrial marketing management, vol. 40, 2011, pp. 181-187.
[8] S. Conger, J. H. Pratt, and K. D. Loch, "Personal information privacy and emerging technologies" Information Systems Journal, vol. 23, 2013, pp. 401-417.
[9] E. F. Stone, D. G. Gardner, H. G. Gueutal, and S. Mcclure, "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations" Journal of Applied Psychology, vol. 68, 1983, pp. 459-468.
[10] S. Milberg, S. Burke, H. Smith, and E. Kallman, "Values, Personal Information Privacy, and Regulatory Approaches" Com. of the ACM, vol. 38, 1995, pp. 65-74.
[11] T. Dinev and P. Hart, "An extended privacy calculus model for E-commerce transactions" Information Systems Research, vol. 17, 2006 pp. 61-80.
[12] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model" Information Systems Research, vol. 15, 2004, pp. 336-355.

[13] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information" Science, vol. 347, 2015, pp. 509-514.
[14] T. Böhmann, J. M. Leimeister, and K. Möslein, "Service Systems Engineering: A field for future Information Systems Research" Business Information Systems Engineering, vol. 6, 2014, pp. 73-79.
[15] G. G. Parker, M. W. Van Alstyne, and S. P. Choudary, "Platform Revolution: How Networked Markets Are Transforming the Economyand How to Make Them Work for You", WW Norton & Company, 2016.
[16] A. Hagiu and J. Wright, "Multi-sided platforms" International Journal of Industrial Organization, vol. 43, 2015, pp. 162-174.
[17] P. Constantinides, O. Henfridsson, and G. G. Parker, "Introduction—Platforms and Infrastructures in the Digital Age" Information Systems Research, Vol. 29, No. 2, 2018.
[18] M. W. Van Alstyne, G. G. Parker, and S. P. Choudary, "Pipelines, platforms, and the new rules of strategy" Harvard business review, vol. 94, 2016, pp. 54-62.
[19] Apple, "Apple Developer Program License Agreement", https://download.developer.apple.com/Documentation/License_Agreements__Apple_Developer_Program/Apple_Developer_Program_License_Agreement_20180604.pdf, 10.06.2018.
[20] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, et al., "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem", Network and Distributed Systems Security Symposium 2018, 2018.
[21] C. Kurtz, M. Semmann, and W. Schulz, "Towards a Framework for Information Privacy in Complex Service Ecosystems" International Conference on Information Systems (ICIS), San Fransisco, 2018.
[22] General Data Protection Regulation, "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), 2016.
[23] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Metayer, R. Tirtea, "Privacy and Data Protection by Design-from policy to engineering" arXiv preprint:1501.03726, 2015.
[24] M. Martini, Art. 28. "Beck'sche Kompaktkommentare BDSG - DSGVO", 2018.
[25] European Commission, "Article 29 Data Protection Working Party", 2010.
[26] European Court of Justice, C-210/16: ULD Schleswig-Holstein vs. Wirtschaftsakademie Schleswig-Holstein GmbH, http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543, 08.06.2018.
[27] F. Belanger and H. Xu, "The role of information systems research in shaping the future of information privacy" Inf. Systems Journal, vol. 25, 2015, pp. 573-578.
[28] United States House of Representatives Committee on Energy and Commerce, "Testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook", 2018.
[29] P. McCausland and A. R. Schecter, "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, 20.05.2018.
[30] M. Rosenberg, N. Confessore, and C. Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions", https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html, 20.05.2018.
[31] A. Hartmans, "It's impossible to know exactly what data Cambridge Analytica scraped from Facebook - here's the kind of information apps could access", https://www.businessinsider.de/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3, 01.06.2018.
[32] J. Albright, "The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle", https://medium.com/tow-center/b69fe692d747, 01.06.2018.
[33] C. Kaşlı, "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, 30.05.2018.
[34] AccuWeather, "Privacy Statement", https://web.archive.org/web/20170831185056/ https:/www.accuweather.com/en/privacy, 03.06.2017.
[35] RevealMobile, "Using mobile location data and beacons to measure retail shopping behavior", 2016.
[36] RevealMobile, "RevealMobile Website", https://revealmobile.com, 15.08.2017.
[37] W. Strafach, "Advisory: AccuWeather iOS app sends location information to data monetization firm", https://hackernoon.com/83327c6a4870, 21.08.2017.
[38] S. J. Vaughan-Nichols, "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/, 19.11.2011.
[39] P. Sapiezynski, A. Stopczynski, R. Gatej, and S. Lehmann, "Tracking Human Mobility Using WiFi Signals" Plos One, vol. 10, 2015.
[40] Apple, "iOS 7: Understanding Location Services", https://support.apple.com/en-en/HT201357, 04.06.2017.
[41] Apple, "Turn Location Services and GPS on or off on your iPhone, iPad, or iPod touch", https://support.apple.com/en-au/ht207092, 04.06.2018.
[42] Apple "What's New in iOS - iOS 7.0", https://developer.apple.com/library/archive/releasenotes/General/WhatsNewIniOS/Articles/iOS7.html, 01.09.2017.
[43] J. Butts, "Apps Can't View MAC Addresses on iOS 11", https://www.macobserver.com/news/product-news/apps-cant-view-mac-addresses-on-ios-11/, 01.09.2017.
[44] Facebook, "Legal Bases", https://www.facebook.com/about/privacy/legal_bases, 09.06.2018.
[45] A. Hern, "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, 28.05.2018.
[46] A. Mosenia, X. Dai, P. Mittal, and N. Jha, "PinMe: Tracking a Smartphone User around the World" IEEE Transactions on Multi-Scale Computing Systems, 2017.
[47] AccuWeather, "Privacy Statement", https://www.accuweather.com/en/privacy, 03.06.2018.
[48] S. Levin, "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, 10.06.2018.