10 The Privacy Disconnect

Joris van Hoboken[1]

Introduction

In the last decade, a flurry of regulatory, legislative and judicial activity has taken place responding to concerns over commercial and government interferences with data privacy.[2] Europe stands out in this regard. In May 2018, the highly anticipated new General Data Protection Regulation (GDPR) came into force.[3] The European legislature is debating revision to the regulatory framework for electronic communications privacy (European Commission Proposal for ePrivacy Regulation 2017a).[4] New frameworks for cross-border access to digital evidence are being discussed.[5] Privacy regulators are stepping up enforcement in relation to Internet companies and adopting a growing stream of regulatory guidance.[6] National courts as well as the Court of Justice of the European Union (CJEU) and the European Court of Human Rights have been asked to rule, as a consequence of citizen and privacy activist initiatives, on the legality of government surveillance measures and the legality of international data flows in view of the fundamental right to privacy and the protection of personal data.[7] The CJEU has been particularly impactful, by invalidating the Data Retention Directive (CJEU 2014a), imposing a right to be forgotten on search engines (CJEU 2014b), and invalidating the Safe Harbour agreement for data flows between the EU and the United States in a sweeping ruling on the need to guarantee data privacy in the context of personal data flowing outside of the EU. The UN General Assembly adopted several resolutions on the right to privacy in the digital age and has also appointed a UN Special Rapporteur on the Right to Privacy.

From these developments alone, one would be tempted to draw the conclusion that, at least in Europe, we are living in a golden age of privacy. Finally, the conditions are being set for the right to privacy and the protection of personal data to be valued and enforced. Research and practice appear to be following suit. Privacy has become an increasingly active field of study in law, economics, social science, computer science, and engineering.[8] Nongovernmental privacy organizations are understaffed but growing; professional organizations of privacy practitioners such as the International Association of Privacy Professionals (IAPP) have seen membership soar and conferences and educational programs fill up with professionals seeking to make a new living.[9]

This contribution's starting point is that the amount of energy, resources, and good intentions going into privacy alone is a bad measure for evaluating whether fundamental challenges to data privacy are being addressed in practice. Clearly, when the European Commission proposes new rules for electronic communications privacy with the headline that they "will increase the protection of people's private life and open up new opportunities for business" (European Commission 2017a), close scrutiny of whether the specifics of the proposals back up this claim is warranted.[10] However, the problem with the protection of data privacy may run deeper than can be uncovered by a close reading of specific legislative acts and their particular legal consequences. Ultimately, the question is whether the current legal and policy frameworks for data privacy provide robust underpinnings for the legitimacy of pervasive processing of personal data in our societies. It is through this divide between the demands for such legitimacy and what current privacy governance offers in practice, a divide I will call "the Privacy Disconnect," that developments in the realm of privacy may be running into a wall.

With the aim to sketch some of the contours of a Privacy Disconnect, this chapter will review some of the major challenges related to the establishment of legitimacy for the pervasive processing of personal data. First, I will discuss the consolidation in the Internet service industry and its transformation into a data-driven environment, where the continuous capture and analysis of data in individualized networked relationships between services, third parties, and users has become an inseparable ingredient for the production of digital functionality and the accumulation of data-driven power (Gürses and Van Hoboken 2018). This transformation challenges

established core principles of data privacy, such as transparency and purpose limitation, in ways that are not easily addressed without radical reform. The way in which the environment is currently shaped along the principle of modularity also challenges the attribution of responsibility for observing data privacy laws and principles, without which the project of protecting and enforcing privacy is perhaps most fundamentally challenged.

Second, the discussion turns to the continuing erosion of restrictions on data collection and the recent debates about a refocus on regulating use instead. Historically, a debate has existed in privacy scholarship on whether privacy law, policy, and engineering should concern itself centrally with limiting the collection and flow of personal information (data minimization) or whether it is enough to put entities processing personal data under an obligation to act fairly, transparently, and lawfully, observing the right of individuals to exercise relative control over the collection and use of their personal data (De Hert and Gutwirth 2006; Gürses and Diaz 2013; Warren and Brandeis 1890; Westin 1967). More recently, a somewhat more radical position has emerged, arguing that regulation should turn away from regulating collection altogether and regulate the use of personal data instead.[11] This proposition may be understandable in the face of ever more pervasive data collection practices, the value that can be extracted from data through advances in data analytics and machine learning, and the limited success of data minimization standards. However, relevant legal frameworks, in Europe, but also in the United States, would require a rather unfeasible overhaul to facilitate this shift in practice. At a theoretical level, the argument for use regulation, as an alternative to the current broader focus of data privacy, is weak.[12] In addition, considering the repeated news about large-scale data breaches, most recently Equifax, Uber, and the use of Facebook by Cambridge Analytica,[13] the argument that people should no longer be concerned about the mere collection of their data rings hollow.

Third, the chapter will discuss the continued reliance on the concept of informed consent for providing legitimacy to data privacy interferences and the related emphasis on giving individuals control over their personal data. This is striking considering the theoretical issues with consent as central to privacy as well as the mountain of evidence that in current-day settings, meaningful consent and control are not practically possible in the first place. The European Union's legislature doubled down on the importance of consent and individual control over personal data in the GDPR.

Consent is the one legitimate ground for the processing of personal data, out of six, that is enshrined in the fundamental right to the protection of personal data in the Charter of Fundamental Rights.[14] Data subject rights to gain access to and erasure of personal data are strengthened, and a new right to data portability has been added to the legal mix.[15] It is possible that allowing people to reap some of the benefits of the economic value in personal data with a right to data portability could strengthen the legitimacy of pervasive personal data processing in certain regards.[16] However, there are reasons to doubt this will work in practice and whether this will further privacy or other values entirely, potentially with significant unintended distributive effects across industries and populations.

Finally, we will turn to the international level, specifically the tension between the different regulatory approaches to data privacy in the United States and Europe and the role of the human rights framework at the international level. In the commercial sphere, the comprehensive and rights-based approach to data privacy regulation in Europe stands in clear contrast to the sectoral and market-oriented approach to privacy law in the United States.[17] In addition, the fact that the dominant firms of the data-driven economy are US-based companies has turned the enforcement of European privacy law into a trans-Atlantic battle of the regions, in which a lot more than privacy is at stake. The latter is also true in the area of lawful access by government agencies. The frameworks for lawful access have been under pressure because of the Snowden revelations and generally need a rigorous internationally coordinated update in view of globally operating cloud service providers that see themselves confronted with growing pressure to provide access to data at home and abroad. While a series of efforts to bridge some of the divides between Europe and the United States on privacy remains ongoing and some strengthening of data privacy in the human rights context can be observed, the political realities seem to have become more challenging over the last years.

The chapter will conclude with some observations of the way in which the multiplicity of concerns and values that has informed privacy frameworks, debates, and practices can lead to a situation in which significant resources are spent on protecting certain aspects of data privacy while other aspects remain unaddressed. In my conclusion I call for data privacy regulation and discourse to move beyond a concern with the organizational handling of people's "personal data" and become more centrally concerned

with the value of the fair accumulation and exercise of data-driven power and the material and political conditions for this value to thrive.

Consolidation in a Networked Internet Service Industry

Over the last decade, we have witnessed a remarkable concentration of power in the hands of a handful of dominant technology companies, which are together providing the services and platforms that are giving shape to the digital environment. Personal information, including data from and about individualized interactions between users and Internet-based services, has become a key ingredient in the production of digital functionality in this environment in ways that challenge existing approaches to data privacy rights.

While some of the underlying developments in the Internet services industry are discussed in more detail and more eloquently elsewhere in this book, it is worth taking note of some of the basics. Of the top ten global companies in terms of market capitalization, the first seven are technology companies, that is, Apple, Alphabet, Amazon, Alibaba, Facebook, Microsoft, and Tencent.[18] The valuations of these companies are so staggering that they raise macroeconomic concerns beyond the specifics of the digital economy itself (Wolf 2017). The monetary assets controlled by these major companies amount to more than four trillion USD, and a general sense has emerged that there is a widespread problem of monopoly and supernormal profits (ibid.).

One of the most important ways in which these companies have become as dominant as they are is through acquisitions, including of potential future competitors. Facebook, for instance has bought Instagram, WhatsApp, and more than fifty other companies since 2005; Google has bought YouTube, Nest Labs, and Motorola and more than 200 other companies since 1999; and Microsoft recently bought Skype, Nokia, and LinkedIn.[19] The role of user data assets in these acquisitions raises important issues at the interface of data privacy and competition law.[20] It is undeniable that in many regards, the dominant tech companies are in competition with one another. Facebook and Alphabet, for instance, are in competition over digital advertising revenues in a market that is now seen as an effective duopoly, earning more than half of all digital advertising revenues worldwide.[21] In the cloud computing market, Amazon is firmly in the lead but has competition from

Alphabet, Microsoft, IBM, and a variety of strong niche players.[22] Without exception, however, leading technology companies have moved toward and built a technology and services environment in which service offerings and innovation have become dependent on the continuous capture of data about users, their behavior, and their interactions (Gürses and Van Hoboken 2018; Zuboff 2015).

Considering the reliance of the tech industry on the processing of data in individualized relationships with users, data privacy concerns abound. At a high level, a question that has to be tackled is how macrolevel concerns about the accumulation and exercise of data-driven power can be better incorporated into discussions of data privacy, which have a tendency to focus on microlevel, decontextualized, and individualized relations with users. Still, existing data privacy laws do offer ample opportunities for regulatory scrutiny. In Europe, in particular, consumer-facing major tech companies are facing regular enforcement actions with respect to their data-related practices.[23] Besides the enforcement of the so-called right to be forgotten since the *Google Spain* ruling,[24] Google has faced considerable pushback related to the consolidation of its privacy policies across its wide portfolio of different consumer-facing services.[25] Such combination of data from different sources easily breaks with the principle of purpose limitation enshrined in European data protection law, raising the question of lawfulness and often requiring a renegotiation of consent. Facebook, too, has been hit with a variety of enforcement actions, including litigation by privacy activist Max Schrems in relation to data flows to the United States and lawful access for intelligence purposes, as well as enforcement with respect to the pervasive tracking of Internet users, the breaking of its promises with respect to the use of WhatsApp user data, and the lack of proper oversight over the collection of data from the platform by Facebook apps.[26] Microsoft is being investigated over its privacy policy with respect to the Windows 10 operating system,[27] which signals a clear and final break with the age of shrink-wrapped software.

Gone are the days in which users bought software and technology products after which they would enjoy these in their relative private sphere, removed from direct interaction with software and technology producers. In the age of the cloud and the emerging Internet of Things, access to technology and software amounts to entering into continuous data-driven

relationships that require significant individualized data flows to function properly (Gürses and Van Hoboken 2018).

There is one aspect of the Internet services environment that is worth highlighting here, considering the resulting complications for the attribution of responsibility for privacy rights and values. This is the deployment of the concept of modularity in the cloud environment (ibid.). The term "modularity" is used to describe the degree to which a given (complex) system can be broken apart into subunits (modules), which can be coupled in various ways. As a design or architectural principle, modularity refers to the "building of a complex product or process from smaller subsystems that can be designed independently yet function together as a whole" (Baldwin and Clark 2003). Modularity can operate within the boundaries of tech companies, leading to the internal decomposition of software into so-called microservices. These components talk to each other through service interfaces and can get loosely coupled in integrated service offerings to users. Separate service components can grow into successful industry-wide offerings, as in the case of the cloud, which was developed internally by Amazon and Google before being offered as a service to others.

The principle of modularity can be seen in action outside the boundaries of technology companies, too. The integration of services into other services and organizational offerings is most simply illustrated by the so-called mash-up, which was pioneered by services such as HousingMaps.[28] It is also well illustrated by the start-up mantra of doing one thing really well. The range of basic service components that is available for integration into the offering of companies and organizations has grown significantly over the last decade.[29] All of these services tend to have direct privacy implications for users. Typical service components for publishers, retailers, and other organizations include[30] user analytics,[31] advertisement,[32] authentication,[33] captcha,[34] performance and (cyber)security,[35] maps and location,[36] search,[37] sales and customer relation management,[38] data as a service,[39] payment,[40] event organizing and ticketing,[41] stockage,[42] shipping,[43] reviews,[44] sharing and social functionality,[45] commenting,[46] and embedded media.[47] Notably, the amount of attention that has been paid to the privacy-invasive practices of online advertising may have distracted privacy researchers and regulators from looking at the integration of a variety of other service components (Englehardt 2017).

The strength and attraction of these third-party services is strongly linked to the fact that they can be built in such a way that they can be offered across organizational offerings and domains, at so-called "internet scale." The unbundling of service components leads to a situation in which users, when interacting with one organization, let us say a newspaper app or website or the IT infrastructure of one's employer, are pulled into a whole set of additional service relationships (Gürses and Van Hoboken 2018). Each of those relationships has its own (dynamic) privacy implications for users. The resulting network of relationships between different services and users raises the question of who the proper addressee is for privacy norms in such an environment. Privacy law and practice are struggling to provide an answer. Should the organization that decides to integrate a particular third-party service simply be held responsible for that service's compliance with data privacy laws? The CJEU is set to rule on these issues, which boil down to the interpretation of the concept of "controller" and the possibility of contributory liability of platforms for data privacy violations in the coming years.[48] Without answering this question precisely and effectively, data privacy law and policy can hardly be hoped to be achieving their more substantive aims.

Furthermore, even though the Internet industry may have become organized according to this principle of modularity, this does not appear to be the case in the way that users are offered a chance to negotiate and give shape to the value of data privacy that is affected by different service components. When using available software and services online, users are defaulted into bundles of relationships with first- and third-party service providers, which are collecting their information in ways that leave little room for real choice or escape.[49]

Erosion of Restrictions on Personal Data Collection

As mentioned in the introduction, one of the key debates has been whether data privacy centrally involves a restriction on the collection of personal data (data minimization) or whether data privacy should merely guarantee that the collection and use of personal data take place in ways that observe the fairness, transparency, and lawfulness of personal data-processing operations. In the first view, privacy involves the respect of a private sphere, the possibility of keeping information about oneself confidential and the respect of the so-called right to be let alone. In the second view, data privacy

can still be possible once data has been collected by others for further use if it is put under appropriate conditions that guarantee the respect for data protection principles.

It will come as no surprise that many have concluded that data minimization principles have failed entirely.[50] The growing commercial and government appetite for personal data has created a situation in which it is hard to imagine any social, economic, or administrative relationship that does not involve the collection of one's personal data. The data-driven nature of service offerings discussed in the previous section plays a role in this regard as well. In addition to developments in the commercial realm, governments have increasingly pushed for legal frameworks that ensure the general availability of personal data for administrative and law-enforcement purposes—for instance, through interagency data-sharing arrangements, data-retention obligations on telecommunications companies, license-plate-scanning programs, and fraud detection.

Where does this state of affairs lead us in terms of the connection between privacy regulations and the collection of personal data?[51] Answering this question, some have put forward the argument that privacy regulation should turn its focus toward the use of data instead of its mere collection.[52] The main argument for this shift tends to be pragmatic, namely, that the collection of personal data has become the normal state of affairs. As a result, focusing the regulation of personal data-driven processes by limiting the collection of data (data minimization) is considered to be no longer feasible and desirable. It is not feasible since the current environment can only function properly when data collection is left relatively unrestrained. It is not desirable considering the societal value involved in big data, which would be unduly restrained by the regulation of data collection practices. Thus, the argument goes, privacy regulation should focus (more) on issues arising from the actual use of personal data.

The arguments for "use regulation" tend to involve two specific elements. First, the existing mechanisms for establishing the *legitimacy* of personal data collection and further use need to move away from a negotiation from the moment of the collection, in terms of specified, legitimate purposes, toward a focus on data use and management practices. Second, a use-based approach would provide the *flexible reuse of data across contexts*, which is argued to be required to extract the optimal value from data analytics. Cate et al. (2014) argue as follows:

> The evolution of data collection and data use necessitates an evolving system of information privacy protection. A revised approach should shift responsibility away from individuals and toward data collectors and data users, who should be held accountable for how they manage data rather than whether they obtain individual consent. In addition, a revised approach should focus more on data use than on data collection because the context in which personal information will be used and the value it will hold are often unclear at the time of collection.[53]

Variations of the argument can be found in the technical literature on privacy engineering, too. Weitzner et al. (2008), for instance, argue for a refocusing of privacy engineering practices away from the implementation of data minimization strategies, which have been developed in the community working on privacy-enhancing technologies, toward information accountability architectures.

The resulting debate about regulatory flexibility for big data analytics may be one of the core data privacy debates of our time. Privacy scholar Helen Nissenbaum, known for her work on providing a theory of privacy in terms of contextual norms, has characterized the argument as "big data exceptionalism" (Nissenbaum 2017). For the purposes of this chapter, the problem with the argument for use regulation is that it proposes to redefine the legal and political question as regards the legitimacy of pervasive personal data processing in a way that is instable, both from a legal point of view and from a broader societal perspective (Van Hoboken 2016).

From a legal and fundamental rights point of view, the establishment of the legitimacy of processing of personal information is still very much connected to the situation that comes into being once personal data is collected. This is the case in Europe, where the fundamental rights guarantee for the protection of personal data in Article 8 of the EU Charter kicks in as soon as personal data is collected. Once personal data is collected, the legal framework requires that this happens transparently and in view of specified lawful and legitimate purposes, in observance of data subject rights and the guarantee of independent oversight.[54] In the United States, there is some more flexibility, considering the lack of a comprehensive regulatory framework for data privacy. Still, consent requirements in sectoral legislation tend to connect to the question of whether data is collected. In addition, the constitutionally grounded third-party doctrine in the United States, while ever under scrutiny, generally implies that once data has been collected by a third party, one loses one's expectation of privacy in relation to government surveillance (Kerr 2009, 561).

There may be a variety of reasons for hoping that people can be stopped from caring about privacy in terms of the mere access of organizations to information about their identity, behavior, and preferences in their personal, professional, and social lives. However, the empirical support that can help ground this wish is lacking. In fact, the growing impact that collected information has on the conditions for living one's life, through the potential use as well as misuse of such data, only makes such concerns about the mere collection of information more pertinent to address.

In conclusion, even if one were to support the attempt to answer the question about the legitimacy of pervasive personal data processing in terms of data use, instead of in terms of data collection, the legal and societal conditions for this attempt to succeed simply do not exist. If the use regulation argument is in essence a project of deregulation, as Chris Hoofnagle (2014) has argued, a shift to use regulation would increase the Privacy Disconnect even further. As long as the law provides legal standing to individuals, individually or in a more organized fashion, to investigate and contest personal data-processing practices from the moment of data collection, a shift to use regulation in practice would hardly respond to deeply entrenched legal data privacy dynamics. Perhaps even more importantly, a shift in privacy governance toward use regulation is not informed by empirical evidence that people will stop worrying about pervasive data processing from the moment data is being collected. In fact, the more data is collected about oneself for more purposes, ever more flexibly defined, the more reason there seems to be to simply worry about the accumulation of data-derived power in the first place. This does not mean this is a productive stance toward current pervasive data-processing operations but simply that a negotiation around use involves even more complexity than a realistic, be it abstract, concern about the existence of data-derived power. In sum, the argument for use regulation may be more informed by our current inability to find robust mechanisms for establishing the legitimacy of pervasive personal data processing than anything else.

Legitimacy and Informed Consent

The mechanisms for establishing the legitimacy of personal data processing lie at the core of any privacy theory and data privacy framework. The core mechanism for establishing this legitimacy in the commercial sphere

has been the mechanism of informed consent.[55] In the sphere of public administration, informed consent plays a diminished or differently constructed role. There, the legitimacy requirement is anchored in democratic legitimacy of legislation underlying personal data-processing operations by public administrations, including the observance of the principles of necessity and proportionality of the related interference in view of relevant constitutional and fundamental rights safeguards.

If we restrict ourselves for a moment to the commercial sphere, we are confronted with a paradoxical situation. Even though the conditions for realizing meaningful informed consent to work in practice seem weaker than ever,[56] current privacy regulations, such as the GDPR, place more focus than ever on informed consent and the control over personal data as the primary standard for legitimacy.[57] In the following, I will discuss some of the core challenges for informed consent to work and what lessons have been and could be drawn from that.

At the practical level, informed consent has been demonstrated to be difficult to realize. Even if privacy policies and related service architectures would provide the levels of transparency that would allow people to inform themselves about privacy-relevant practices, people would lack the time, let alone stamina, to inform themselves properly before making informed decisions (McDonald and Cranor 2008). The data-driven nature of the production of digital functionality and the increasingly dynamic nature of all the features that are offered make things significantly harder (Gürses and Van Hoboken 2018). If meaningful consent with respect to a certain data-processing operation has been established, when and how should and can consent be renegotiated? Once we add the integration of third-party services, as discussed previously, to the mix, the situation becomes even more challenging.

Take the situation of the smartphone ecosystems as an example. Smartphones are an ideal site for the offering of individualized data-driven services. They tend to be personal and contain and provide access to a host of sensors and personal data, such as photos, messages, contacts, rich behavioral patterns, and location (de Montjoye et al. 2013). Enforcement initiatives and research in academia and civil society continue to show a lack of respect for basic data privacy guarantees that would be necessary for the establishment of informed consent in this context.[58] For instance, many apps do not even have a privacy policy, the most basic means through

which transparency is offered to users.[59] While the relevant operating systems have implemented increased controls (and policies) for accessing personal data such as location, the permission architectures do not provide the granularity that would be needed to address integration of a growing number of third-party trackers.[60] Considering the high levels of standardization that are possible through the policies and designs of dominant smartphone ecosystem providers (Android and Google Play, Apple Store and iOS), smartphones would be one of the best places to hope for data privacy to work in practice.

In addition to the practical problems with respect to the establishment of informed consent, there are fundamental theoretical objections with informed consent as the primary mechanism for establishing legitimacy. And in fact, in the European context, informed consent is just one of the possible grounds for establishing the lawfulness for the processing of personal data.[61] There are two main other grounds available in the commercial realm. The first one requires that the processing of personal data is necessary for the delivery of a service, or more specifically "the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Article 6(1)(b), GDPR). The second is that the processing "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" (Article 6(1)(f), GDPR). Notably, these two standards are objective and subjective elements meant to play a role in individual cases only.[62] But the most striking aspect of the role of informed consent in the European legal framework is that regardless of consent being required or not, entities processing personal data always need to do so fairly, transparently, for specific, legitimate purposes, in observance of data subject rights, and subject to independent oversight by privacy regulators.[63]

There are further objections to data privacy frameworks relying on informed consent. First, the requirement of informed consent and the underlying conception of privacy as the control over one's personal data, as most famously articulated by Westin (1967), may get the value of privacy wrong. This argument has been made most eloquently and convincingly by Nissenbaum (2009) in her theory of privacy as contextual integrity. It may

be so that in a certain context, respect for privacy implies the respect for a norm regarding the flow of personal data that involves the negotiation of consent, but such a context-specific norm does not generalize to a theory of privacy (ibid.). Respect for privacy, Nissenbaum argues, involves the respect for contextual norms with respect to the flow of personal information. This more objective contextual definition of privacy places the respect for privacy firmly outside of the realm of individualized negotiations around the processing of "one's personal data."

In addition, the fact that informed consent aims to protect privacy by giving individuals (a certain amount of) control over the collection and use of *their* personal information runs into deeper trouble every year (see also Mai's chapter in this volume). First of all, the practical boundaries of what has to be negotiated are unclear as the boundaries of the concept of personal information (personal data under the European data protection framework) are contested and legally uncertain. In the United States, consumer privacy protections tend to focus on providing control mechanisms related to the personal information of individuals that is collected in the interaction of a particular service with that specific individual.[64] This implies that the collection and use of personally identifiable information gathered through other means, or the information related to others collected through those individuals, simply falls through the cracks.[65] If one follows the guidance of the European Union's Article 29 Working Party on the concept of personal data, one could wonder what would still escape this broad definition in the context of data flows in digitally mediated contexts.[66] In practice, many entities processing information falling under the definition of personal data do not easily acknowledge this (Christl and Spiekermann 2016). The removal of identifiers and the application of similar privacy engineering practices, however, do not easily lead to the legal conclusion that such information is no longer personal data. A similar problem with respect to the legal definition of personal data exists for the designated special categories of sensitive data, such as information revealing someone's ethnicity, race, sexual orientation, or medical data. The boundaries of this concept are legally consequential as EU law imposes some significant roadblocks for the processing of these data.[67]

Finally, the structures of relevant sets of personal data reflect the social and interconnected contexts in which data is collected and processed. It is difficult to meaningfully separate someone's personal data from the

personal data of others. As a result, the individualized negotiations around privacy in terms of informed consent are simply too narrow, while functional mechanisms for negotiating the pervasive collection of the personal information of nonusers are lacking.[68] But perhaps more fundamentally, because of predictive analytics and machine learning, the personal data "of others" may be as significant, from the perspective of privacy and related concerns about the data-driven exercise of power, as one's own data (Barocas and Nissenbaum 2014). In sum, it seems unwise to continue to frame data privacy issues in terms of a subjective concern over the relative control over one's "own" personal data, that is, the subset of information that relates to you.

International Data Flows and the US–EU Divide in Data Privacy Governance

Some of the differences between the US and EU approaches to data privacy have already been discussed in passing. These differences are many and exist at the level of legal culture, regulatory design, constitutional safeguards, and enforcement mechanisms.[69] While a deeper understanding of the differences is of theoretical as well as practical value, this is not the place to discuss these differences in depth. It seems entirely unsurprising that different approaches to data privacy exist in the world and would continue to exist in the future.

In fact, the diversity of approaches to data privacy in the European context is often overlooked. In Scandinavian countries, mandatory transparency requirements with respect to taxation data exist that would be unthinkable elsewhere in Europe. The right to be forgotten ruling came out of a minority position of the Spanish Data Protection Authority with respect to the application of data protection obligations on search engines.[70] It is quite unthinkable that a similar case would have emerged in the Netherlands, and a number of right to be forgotten rulings in the Netherlands have demonstrated the relative unease with the conclusions of the CJEU at the EU level.[71]

The European approach to privacy is the result of a combination of the concern for the protection of personal data, already codified into national data protection laws since the 1970s, with the project of European integration (Fuster 2014; Gutwirth 2002; Lynskey 2015; Schwartz 2013). The latter

project necessarily continues to involve harmonization efforts to allow for the free flow of personal data in the European context. To allow for such free flow of personal data, the Data Protection Directive established a European Union–wide framework for respect for privacy in the context of the processing of personal data.[72] To address legal fragmentation as a result of different implementation and enforcement practices of the directive, the new framework established by the GDPR provides for further harmonization in view of digital single-market aims.

The real complexity and trouble emerge, in the relationship with Europe, in the context of increasingly pervasive international data flows and the relative lack of legal and political integration outside the boundaries of the European integration project. The Organisation for Economic Co-operation and Development (OECD) principles and the increased interest in data privacy in the human rights context provide some legal baseline.[73] Furthermore, a variety of more specific intergovernmental and international regulatory initiatives have been undertaken. In addition, more pragmatic efforts exist, including through corporate privacy governance frameworks, as well as standardization and engineering practices. These can all serve to increase interoperability in view of differences in data privacy protections and the economic and political interests connected to international data flows. Even so, the divide between Europe and the United States on privacy has lately looked as wide and challenging as it ever may have been, and the stakes have grown considerably.

It is only since relatively recently that the EU has had its own binding fundamental rights instrument, including the newly established fundamental right to the protection of personal data. Until well into the 1990s the status of fundamental rights in the EU context was weak and heavily debated.[74] The European institutions, except perhaps for the Council of the European Union, have enthusiastically received the new charter right to the protection of personal data with far-reaching regulatory efforts and judgments. Such European harmonization in the area of personal data protection sometimes overlooks the lack of enforcement of relevant norms in the European Union and the member states itself, in favor of establishing a common ground. Also, often overlooked is the reality that national security and foreign intelligence surveillance practices, an area in which data privacy violations tend to be most severe, are not harmonized at the EU level in the first place. Clearly, Article 8 of the European Convention of Human Rights and

related Council of Europe instruments, including Convention 108, provide a fundamental baseline of protection. Still, it is sometimes hard to escape the impression that the increased attachment to the protection of fundamental rights at the EU level, which were predominantly informed by the European integration project, is causing international tensions about international flows of personal data partly for the sake of Europe's self-image.

Looking at the United States, the main challenges for data privacy in the international context exist at two levels. The first level is the relative inability and unwillingness of the US political system to adopt meaningful legislative reforms in the area of data privacy, including in relation to offering meaningful protection of the privacy-related rights and freedoms of non-US persons. Recent efforts to adopt a commercial privacy bill of rights have stalled, and internationally controversial United States surveillance laws remain in place without fundamental reforms, in the view of many observers. It seems entirely possible that such lack of reforms and the apparent lack of support of the current US administration to rigorously implement the recently adopted Privacy Shield will lead to another trans-Atlantic privacy breakdown now that the CJEU has been asked to look at it again.[75]

Second, the international dominance of US-based technology firms complicates dynamics in relation to the protection of privacy in commercial settings as well as in relation to the issue of government surveillance.[76] In a purely national setting the interaction between commercial data collection practices and lawful access regimes is already a complicated matter. Respect for privacy and the legitimacy of pervasive personal data processing involves consideration of the standards under which data held in private hands can become accessible to government agencies. This ideally requires the calibration of privacy standards for commercial and government surveillance at the national level. When lawful access is not meaningfully restrained, domestically or abroad, people are right to worry about entrusting their data to internationally operating private entities. Internationally operating cloud companies and the resulting transnational relationships between service providers and users in multiple jurisdictions across the world take place under the shadow of a multiplicity of lawful access regimes. The legal complexity is staggering, goes well beyond the EU–US relationship, and is likely to keep privacy researchers and practitioners busy for decades.

All of these transnational data privacy tension points put significant pressure on the existing international framework for data privacy at the

international level, and the human rights framework in particular. The extent to which the right to privacy as enshrined in human rights treaties will be able to trickle down and play a constructive role in addressing some of the challenges discussed in this chapter remains to be seen. There are positive signs in the establishment of a UN Special Rapporteur on the Right to Privacy and the increased attention to data privacy in the human rights area more generally, including in relation to the practices of online service providers. However, these are minor steps in comparison to what may be needed in terms of institutional and legal reform at the international level to ensure respect for data privacy in a globalized world in the long run.

Conclusion

This chapter has created a bleak picture in sketching some of the current challenges to data privacy. Specifically, I have argued that current privacy laws and policies fall short in providing for the legitimacy of current-day pervasive personal data-processing practices. This falling short, which I have summarized as the Privacy Disconnect, exists at the socio-technical, the regulatory, and the political levels. The Privacy Disconnect may not be new, but I find it safe to argue that the intensity of some of the challenges for the establishment of legitimacy has increased. The complexity of the socio-technical environment has increased, existing legal mechanisms and institutional arrangements are wearing out, and solutions are hard to come by.

When one takes a step back and looks at all the efforts that go into the protection of privacy, should not one conclude that the glass is at least half full? Undoubtedly so. Still, the reality is also that privacy laws, policies, and engineering practices respond to a multiplicity of concerns and values. This can easily lead to a situation in which significant resources are spent on protecting certain aspects of data privacy while other aspects remain unaddressed. Moving forward, it seems particularly important that privacy law and policy discussions become more firmly connected to the underlying power dynamics they aim to resolve. Although this is certainly ambitious, we should aim to ensure that data privacy law and policy respond more directly to the social, economic, and political needs of people confronted with a world in which power is increasingly mediated through data-driven practices.

Notes

1. I would like to thank the editor, Rikke Frank Jørgensen, the anonymous reviewers, and the participants in the Author Workshop for their valuable comments and suggestions with respect to this chapter.

2. Data privacy as a conceptual term referring to the subset of privacy issues that stem from the collection and use of (personal) information, including data protection.

3. Regulation 2016/679 of April 27, 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/EC (General Data Protection Regulation).

4. The European Commission also published a new proposal for a Regulation on the processing of personal data by EU institutions, a Communication on International Data Protection and a Regulation on the free flow of nonpersonal data.

5. In early 2018, the US Congress passed the Clarifying Lawful Overseas Use of Data Act (as a last-minute addition to a trillion-dollar spending bill), and the European Commission has put forward proposals in the area of law enforcement on electronic evidence gathering through Internet-based services. Internationally, the United Kingdom and the United States appear closest to reaching an agreement on cross-border access in the law-enforcement area.

6. In the last two years, the Article 29 Working Party has issued new guidelines on data portability, data protection officers, the lead supervisory authority, the data protection impact assessment, transparency, the rules on profiling and automated decision-making, and the setting of administrative fines.

7. See, for example, the proceedings of the European Court of Human Rights in the Big Brother Watch application relating to government surveillance, https://t.co/PyAhfgq5cc. See also CJEU (2014a, 2015). See *Europe v. Facebook* for more background on litigation of privacy advocate Max Schrems, mostly in relation to Facebook. Available at http://europe-v-facebook.org/EN/en.html. Schrems recently launched a new data privacy enforcement nongovernmental organization, called noyb ("none of your business").

8. Several (increasingly interdisciplinary) conferences have successfully established themselves in the area, including Institute of Electrical and Electronics Engineers Symposium on Security and Privacy, the Computers, Privacy and Data Protection conference, the Privacy Law Scholars Conference, the Amsterdam Privacy Conference, and the Privacy Enhancing Technologies Symposium.

9. IAPP recently reported it now has 40,000 members worldwide; see Ashford (2018).

10. For a discussion of the proposals, see Zuiderveen Borgesius et al. (2017).

11. For a discussion, see Van Hoboken (2016). See also Nissenbaum (2017).

12. For a discussion, see Nissenbaum (2017).

13. See Brian Fung (2017), Todd Shields and Eric Newcomer (2018), and Carole Cadwalladr and Emma Graham-Harrison (2018).

14. Article 8, Charter of Fundamental Rights of the European Union. The charter was solemnly proclaimed at the Nice European Council in 2000 and became binding with the entry into force of the Lisbon Treaty on December 1, 2009.

15. See Paul De Hert et al. (2017).

16. For a discussion, see, for example, Graef, Husovec, and Purtova (2017).

17. See recently, for example, Paul M. Schwartz and Karl-Nikolaus Peifer (2017).

18. See, for example, Nicole Bullock (2017). The most highly valued tech company in Europe is SAP, which is the world's sixtieth most valued company.

19. Basic information about these acquisitions can be found on Wikipedia.

20. For a discussion, see, for example, European Data Protection Supervisor Opinion, March 2014.

21. For a discussion, including of the potential rise of Amazon in ad sales, see Sorrell (2018).

22. See Miller (2017).

23. See, for example, Esteve (2017).

24. Note that the case of the right to be forgotten is different in character, as it does not relate to the processing of user data, but to the public accessibility of personal data through search engines.

25. See, for example, Dutch Data Protection Authority reports for 2014.

26. *Supra* note 7. See also Van Alsenoy et al. (2015), Samuel Gibbs (2018), European Commission (2017b), and Federal Trade Commission (2018).

27. See Bodoni (2017).

28. See http://www.housingmaps.com.

29. Consider the wide range of companies and organizations that are offering (information) goods and services, connecting to users through digital channels, including retailers, publishers, political parties, educational institutions, health services, government agencies, nongovernmental organizations, and so forth.

30. This is a nonexhaustive list meant to illustrate the argument. The question of what the current array of service components in different online service sectors

looks like is the kind of future research that we think needs to happen and is likely to provide further insights into how privacy governance may be organized.

31. Statcounter (https://statcounter.com) or market leader Google Analytics (https://analytics.google.com/analytics/web/provision).

32. RevenueHits (http://www.revenuehits.com) or market leader Google AdSense (https://www.google.com/adsense).

33. See, for example, SwiftID by CapitalOne (two-factor authentication; https://developer.capitalone.com/products/swiftid/homepage), OpenID (http://openid.net), or Facebook Login (https://developers.facebook.com/docs/facebook-login).

34. See, for example market leader Google reCaptcha (https://www.google.com/recaptcha/intro/index.html).

35. See, for example, Cloudflare (https://www.cloudflare.com); Symantec's Web Security Service, (https://www.symantec.com/products/web-security-services); or the free and open https as a service, Let's Encrypt (https://letsencrypt.org).

36. OpenStreetMap (https://www.openstreetmap.org) or market leader Google (https://developers.google.com/maps).

37. See, for example, Google Custom Search (https://cse.google.com/cse).

38. See one of the earliest movers to the cloud, Salesforce (http://www.salesforce.com).

39. See, for example, Oracle Data Cloud (https://www.oracle.com/applications/customer-experience/data-cloud/index.html) or Acxiom's LiveRamp Connect (https://liveramp.com/blog/customer-data-liveramp-connect).

40. See, for example, PayPal's Braintree v.zero SDK (https://developer.paypal.com).

41. See Eventbrite (https://developer.eventbrite.com) or Ticketmaster (http://developer.ticketmaster.com).

42. See, for example, Fulfillment by Amazon (https://services.amazon.com/fulfillment-by-amazon/benefits.htm).

43. See, for example, Amazon's Delivery Service Partner program (for delivery suppliers; https://logistics.amazon.com) and UPS Shipping API (for delivery demand) (https://www.ups.com/us/en/services/technology-integration/online-tools-shipping.page).

44. See, for example, Feefo (https://www.feefo.com/web/en/us).

45. See, for example, AddThis (http://www.addthis.com) and Facebook Sharing (https://developers.facebook.com/docs/plugins).

46. See, for example, Facebook Comments (https://developers.facebook.com/docs/plugins/comments) or Disqus (https://disqus.com).

47. See, for example, Google's YouTube (https://www.youtube.com/yt/dev/api-resources.html) and SoundCloud (https://developers.soundcloud.com/docs/api/sdks).

48. See CJEU (2017a). See also CJEU (2017b).

49. A discussion of whether cookie walls are permissible in Europe is ongoing. See, for example, Zuiderveen Borgesius et al. (2018).

50. See, for example, Koops (2014).

51. For an in-depth discussion, see Van Hoboken (2016).

52. See, for example, Mundie (2014), United States President's Council of Advisors on Science and Technology (2014), Cate et al. (2014), and Weitzner et al. (2008).

53. See Cate et al. (2014) for the application of this argument to the revision of international data privacy guidelines.

54. See Article 8 of the Charter of Fundamental Rights of the European Union.

55. In the United States, informed consent tends to be phrased as the requirement of "notice and choice."

56. For a discussion of core issues with consent, see Solove (2013), Reidenberg et al. (2015), Koops (2014), and Nissenbaum (2009).

57. See, for example, European Commission (2012, 2018).

58. Federal Trade Commission Protecting America's Consumers (2013); European Commission, Article 29 Working Party (2013); European Union Agency for Network and Information Security (2017); and Future of Privacy Forum (2016).

59. App distribution platforms (Google Play for Android and the Apple Store for iOS) require apps that process personal information to have a privacy policy and have started to enforce this requirement more strictly in the last year.

60. See, for example, European Union Agency for Network and Information Security (2017).

61. See Article 6 of the GDPR and Article 7 of the Data Protection Directive. See also Article 8 of the Charter of Fundamental Rights of the European Union.

62. See, for example, European Commission, Article 29 Working Party (2014) Opinion on the notion of legitimate interests of the data controller.

63. This stands in contrast to the market-oriented approach to data privacy in the United States.

64. See, for example, the California Online Privacy Act, which defines "personally identifiable information" as "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form."

65. For a discussion of the definition of the US concept of personally identifiable information, see Schwartz and Solove (2011).

66. European Commission, Article 29 Working Party, Opinion on the Concept of Personal Data (2007). See also Purtova (2018). Specifically, the definition of personal data includes information relating to an identified or identifiable individual. This, in the view of the Article 29 Working Party, encompasses information that is about an individual, information that has the purpose to be used in relation to an individual, or information that is likely to have an impact on a particular individual.

67. The CJEU is expected to rule on this definition in an upcoming ruling on the obligations of search engines with respect to sensitive personal data in their index.

68. Think of the implications to others of providing access to one's messages, e-mails, pictures, and contacts in the smartphone context.

69. See, for example, Bennett and Raab (2006) and Bygrave (2014).

70. The Spanish Data Protection Authority Agencia Española de Protección de Datos took a different position from the Article 29 Working Party in 2009, by arguing that a right to request delisting from search engines followed from the data protection directive. The Article 29 Working Party itself took a more careful approach in its Opinion 1/2008 on data protection issues related to search engines.

71. For a discussion of Dutch right to be forgotten cases, see Kulk and Zuiderveen Borgesius (2018).

72. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (European Parliament and the Council 1995).

73. See OECD (2013). In the human rights context, see, for example, United Nations (2014).

74. On the relation of the EU to fundamental rights, see Alston and Weiler (1999), Leben (1999), Williams (2004), and Coppell and O'Neill (1992).

75. The Irish High Court has recently referred questions to the CJEU, in a new case of Schrems, involving standard contractual clauses and the privacy shield. See the Irish High Court (2016).

76. For a US perspective, see, for example, Clarke et al. (2013). See also Van Hoboken and Rubinstein (2013).

References

Alston, Philip, and Joseph H. H. Weiler. 1999. "An Ever Closer Union in Need of a Human Rights Policy: The European Union and Human Rights." In *The EU and Human Rights*, edited by Philip Alston, 3–69. Oxford: Oxford University Press.

Article 29 Working Party. 2007. Opinion 4/2007 on the concept of personal data. June. https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

———. 2013. Opinion 02/2013 on apps on smart devices. February 27. https://www.datatilsynet.no/globalassets/global/regelverk-skjema/artikkel29gruppen/opinion_on_mobile_apps_wp_202_en_.pdf.

———. 2014. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. April 9. http://www.dataprotection.ro/servlet/ViewDocument?id=1086.

Ashford, Warwick. 2018. "Data Protection Is a Business Issue, Says IAPP." *Computer Weekly.com*, April 20. https://www.computerweekly.com/news/252439642/Data-protection-is-a-business-issue-says-IAPP.

Baldwin, Carliss Y., and Kim B. Clark. 2003. "Managing in an Age of Modularity." In *Managing in the Modular Age: Architectures, Networks, and Organizations*, edited by Raghu Garud, Arun Kumaraswamy, and Richard N. Langlois, 84–93. Oxford: Blackwell.

Barocas, Solon, and Helen Nissenbaum. 2014. "Big Data's End Run around Procedural Privacy Protections." *Communications of the ACM* 57 (11): 31–33.

Bennett, Colin, and Charles Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge, MA: MIT Press.

Bodoni, Stephanie. 2017. "Microsoft Faces European Privacy Probes over Windows 10." *Bloomberg*, February 21. https://www.bloomberg.com/news/articles/2017-02-21/microsoft-faces-european-privacy-probes-over-windows-10.

Bullock Nicole. 2017. "Tech Surge Boosts Year's Momentum Trade." *Financial Times*, November 23. https://www.ft.com/content/4c34a416-cfd4-11e7-b781-794ce08b24dc.

Bygrave, Lee A. 2014. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press.

Cadwalladr, Carole, and Emma Graham-Harrison. 2018. "50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, March 17. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cate, Fred H., Peter Cullen, and Viktor Mayer-Schonberger. 2014. "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines." https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf.

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. 2013. "Liberty and Security in a Changing World." Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies. https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Coppell, Jason, and Aidan O'Neill. 1992. "The European Court of Justice: Taking Rights Seriously?" *Common Market Law Review* 29: 669–692.

Court of Justice of the European Union. 2014a. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*. Joined Cases C-293/12 and C-594/12, April 8, 2014.

———. 2014b. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Case C-131/12, May 13, 2014.

———. 2015. *Maximillian Schrems v Data Protection Commissioner*. Case C-362/14, October 6, 2015.

———. 2017a. Opinion of Advocate General. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the Presence of Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*. Case C-210/16, October 24, 2017.

———. 2017b. *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*. Case C-40/17, January 26, 2017.

Christl, Wolfie, and Sarah Spiekermann. 2016. *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Vienna: Facultas.

De Hert, Paul, and Serge Gutwirth. 2006. "Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power." In *Privacy and the Criminal Law*, edited by Erik Claes, Antony Duff, and Serge Gutwirth, 61–104. Cambridge: Intersentia.

De Hert, Paul, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez. 2017. "The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services." *Computer Law & Security Review* 32 (2): 193–203.

de Montjoye, Yves-Alexandre, Cesar A. Hidalgo, Michel Verleysen, and Vincent Blondel. 2013. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* 3 (1376).

Dutch Data Protection Authority. 2013. "Investigation into the Combining of Personal Data by Google: Report of Definitive Findings." https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf.

Englehardt, Steven. 2017. "No Boundaries: Exfiltration of Personal Data by Session-Replay Scripts." *Freedom to Tinker*. November 15. https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts.

Esteve, Asunción. 2017. "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA." *International Data Privacy Law* 7 (1): 36–47.

European Commission. 2012. "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses." January 25. http://europa.eu/rapid/press-release_IP-12-46_en.htm.

———. 2017a. "Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions." January 10. https://ec.europa.eu/digital-single-market/en/news/commission-proposes-high-level-privacy-rules-all-electronic-communications-and-updates-data.

———. 2017b. "Mergers: Commission Fines Facebook €110 million for Providing Misleading Information about WhatsApp Takeover." May 18. https://europa.eu/newsroom/content/mergers-commission-fines-facebook-%E2%82%AC110-million-providing-misleading-information-about_en.

———. 2017c. "Proposal for a Regulation on Privacy and Electronic Communications." January 10. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

———. 2018. *It's Your Data—Take Control*. May 4. https://publications.europa.eu/da/publication-detail/-/publication/fe2cb115-4cea-11e8-be1d-01aa75ed71a1.

European Data Protection Supervisor Opinion. 2014. Preliminary Opinion Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy. March. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

European Parliament and the Council. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October Official Journal L 281, November 23, 1995, 31–50.

European Union Agency for Network and Information Security. 2017. "Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR." November. https://www.enis.europa.eu/publications/privacy-and-data-protection-in-mobile-applications/at_download/fullReport.

Federal Trade Commission Protecting America's Consumers. 2013. "Mobile Privacy Disclosures: Building Trust through Transparency." https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

———. 2018. "Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices." March 26. https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

Fung, Brian. 2017. "Equifax's Massive 2017 Data Breach Keeps Getting Worse." *The Washington Post*, March 1. https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach.

Fuster, Gloria González. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Berlin: Springer Science & Business.

Future of Privacy Forum. 2016. "FPF Mobile Apps Study." https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf.

Gibbs, Samuel. 2018. "Facebook Ordered to Stop Collecting User Data by Belgian Court." *The Guardian*, February 16. https://www.theguardian.com/technology/2018/feb/16/facebook-ordered-stop-collecting-user-data-fines-belgian-court.

Graef, Inge, Martin Husovec, and Nadezhda Purtova. 2017. "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law." TILEC Discussion Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071875.

Gürses, Seda, and Claudia Diaz. 2013. "Two Tales of Privacy in Online Social Networks." *IEEE Security and Privacy* 11 (3): 29–37.

Gürses, Seda, and Joris van Hoboken. 2018. "Privacy after the Agile Turn." In *Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene. Cambridge: Cambridge University Press.

Gutwirth, Serge. 2002. *Privacy and the Information Age*. Oxford: Rowman & Littlefield.

Hoofnagle, Chris J. 2014. "The Potemkinism of Privacy Pragmatism." *Slate*, September 2. http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html?via=gdpr-consent.

Irish High Court. 2016. "Request for Preliminary Ruling." http://www.europe-v-facebook.org/sh2/ref.pdf.

Kerr, Orin S. 2009. "The Case for the Third-Party Doctrine." *Michigan Law Review* 107 (2): 561–602.

Koops, Bert-Jaap. 2014. "The Trouble with European Data Protection Law." Tilburg Law School Research Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

Kulk, Stefan, and Frederik Zuiderveen Borgesius. 2018. "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe." In *Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 301–320. Cambridge: Cambridge University Press.

Leben, Charles. 1999. "Is There a European Approach to Human Rights?" In *The EU and Human Rights*, edited by Philip Alston, 69–99. Oxford: Oxford University Press.

Lynskey, Orla. 2015. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.

McDonald, Aleecia M., and Lorrie Faith Cranor. 2008. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4: 543–568.

Miller, Ron. 2017. "AWS Won't Be Ceding Its Massive Market Share Lead Anytime Soon." *TechCrunch*, July 28. https://techcrunch.com/2017/07/28/aws-wont-be-ceding-its-massive-market-share-lead-anytime-soon.

Mundie, Craig. 2014. "Privacy Pragmatism: Focus on Data Use, Not Data Collection." *Foreign Affairs*, March/April. https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

———. 2017. "Deregulating Collection: Must Privacy Give Way to Use Regulation?" SSRN Scholarly Paper ID 3092282. Rochester, NY: Social Science Research Network. https://ssrn.com/abstract=3092282.

Organisation for Economic Co-operation and Development. 2013. "Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Purtova, Nadezhda. 2018. "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10 (1): 40–81.

Reidenberg, Joel R., Cameron N. Russel, Alexander J. Callen, Sophia Qasir, and Thomas B. Norton. 2015. "Privacy Harms and the Effectiveness of the Notice and Choice Framework." *I/S: A Journal of Law and Policy for the Information Society* 11 (2): 485–524.

Schwartz, Paul. M. 2013. "The EU-US Privacy Collision: A Turn to Institutions and Procedures." *Harvard Law Review* 126 (7): 1966–2009.

Schwartz, Paul M., and Karl-Nikolaus Peifer. 2017. "Transatlantic Data Privacy." 106 *Georgetown Law Journal* 115 (November). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066971##.

Schwartz, Paul M., and Daniel J. Solove. 2011. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." *N.Y.U. Law Review* 86: 1814–1893.

Shields, Todd, and Eric Newcomer. 2018. "Uber's 2016 Breach Affected More Than 20 Million U.S. Users." Bloomberg. April 12. https://www.bloomberg.com/news/articles/2018-04-12/uber-breach-exposed-names-emails-of-more-than-20-million-users.

Solove, Daniel. 2013. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (7): 1880–1903.

Sorrell, Martin. 2018. "How Amazon Will Crash Google and Facebook's Advertising Duopoly." *Wired*, January 2. http://www.wired.co.uk/article/amazon-advertising-threaten-google-facebook.

United Nations. 2014. "The Right to Privacy in the Digital Age." Report of the Office of the United Nations High Commissioner for Human Rights. June 30. A/HRC/27/37. Geneva: Human Rights Council.

United States President's Council of Advisors on Science and Technology. 2014. Report to the President. "Big Data and Privacy: A Technological Perspective." https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

Van Alsenoy, Brendan, Valerie Verdoodt, Rob Heyman, Ellen Wauters, Jef Ausloos, and Gunes Acar. 2015. *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms*. SPION and EMSOC. Draft August 25. https://www.researchgate.net/publication/291147719_From_social_media_service_to_advertising_network_-_A_critical_analysis_of_Facebook's_Revised_Policies_and_Terms.

Van Hoboken, Joris. 2016. "From Collection to Use in Privacy Regulation? A Forward Looking Comparison of European and U.S. Frameworks for Personal Data Processing." In *Exploring the Boundaries of Big Data*, edited by Bart Van der Sloot, Dennis Broeders, and Erik Schrijvers, 231–259. The Hague: The Netherlands Scientific Council for Government Policy.

Van Hoboken, Joris, and Ira Rubinstein. 2013. "Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era." *Maine Law Review* 66: 488–533.

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 193–220.

Weitzner, Daniel J., Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, and Gerald J. Sussman. 2008. "Information Accountability." *Communications of the ACM* 51 (6): 82–87.

Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum.

Williams, Andrew. 2004. *EU Human Rights Policies: A Study of Irony*. Oxford: Oxford University Press.

Wolf, Martin. 2017. "Taming the Masters of the Tech Universe." *Financial Times*, November 14. https://www.ft.com/content/45092c5c-c872-11e7-aa33-c63fdc9b8c6c.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

Zuiderveen Borgesius, Fredrik. J., Joris van Hoboken, Kristina Irion, and Max Rozendaal. 2017. "An Assessment of the Commission's Proposal on Privacy and Electronic Communications." European Parliament's Committee on Civil Liberties, Justice and Home Affairs research paper. https://www.ivir.nl/publicaties/download/IPOL_STU2017583152_EN.pdf.

Zuiderveen Borgesius, Frederik J. J., Sanne Kruikemeier, Sophie C. Boerman, and Helberger Boerman. 2018. "Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation." *European Data Protection Law Review* 3 (3): 353–368.