de Brouwer, Simeon

Article

Privacy self-management and the issue of privacy externalities: Of thwarted expectations, and harmful exploitation

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: de Brouwer, Simeon (2020) : Privacy self-management and the issue of privacy externalities: Of thwarted expectations, and harmful exploitation, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 4, pp. 1-29, https://doi.org/10.14763/2020.4.1537

This Version is available at:
https://hdl.handle.net/10419/233114

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Privacy self-management and the issue of privacy externalities: of thwarted expectations, and harmful exploitation

Simeon de Brouwer *Independent*

DOI: https://doi.org/10.14763/2020.4.1537

Published: 21 December 2020
Received: 26 May 2020 **Accepted:** 16 October 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: de Brouwer, S. (2020). Privacy self-management and the issue of privacy externalities: of thwarted expectations, and harmful exploitation. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1537

Keywords: Interdependent privacy, Privacy externalities, Notice and consent, Data protection by design, Joint controllership

Abstract: This article argues that the self-management of one's privacy is impossible due to privacy externalities. Privacy externalities are the negative by-product of the services offered by some data controllers, whereby the price to 'pay' for a service includes not just the provision of the user's own personal data, but also that of others. This term, related to similar concepts from the literature on privacy such as 'networked privacy' or 'data pollution', is used here to bring to light the incentives and exploitative dynamics behind a phenomenon which, I demonstrate, benefits both the user and the data controller to the detriment of third-party data subjects. Building on these novel elements and on the relevant concepts and examples found in the existing literature, this article draws a comprehensive picture of the phenomenon, and offers two promising paths to address it—better enforcing the principle of data protection by design and by default, and relying on the framework of joint controllership.

1. Introduction

This article examines the interdependent dimension of privacy and criticises the individualistic framework of notice and consent (hereafter 'N&C') through which one's personal data is in practice protected. This framework is presented as problematic due to the way it obscures the role of data subjects other than the 'main' data subject (the user of the product or service, henceforth 'the user' of the 'service'), and thereby prevents privacy externalities from being confronted and adequately addressed. 'Externality' is a term from the field of economics which designates the by-product of a business activity; it occurs when the production or consumption of a good or service by an agent imposes a cost or benefit on an unrelated third party (Tietenberg and Lewis, 2018, p. 26). A textbook example of the concept would be the activity of an industry which pollutes a water stream, generating profits for those actively engaged in the activity but also covertly impacting the health of locals. By extension, the concept of privacy externality refers to the inclusion of others' personal data in the processing activity agreed to between the controller and the user, whereby costs are imposed on these third-party data subjects: the undermining of their privacy and of their right to data protection, as well as potential harm.

For example, we routinely upload pictures of others to proprietary platforms such as Facebook. We disclose the genetic data of our whole family, together with our own, when we get DNA testing kits from companies such as MyHeritage. The discussions we have with our friends fuel the training of Amazon's AI when they enter our Alexa-equipped 'smart home'. None of the aforementioned individuals in practice benefits from adequate privacy protection, because the means we too often primarily rely on to ensure the protection of data subjects' personal data (such as contract-like Terms of Service between user and service provider), allow the exercise of data protection rights to the user only (Solove, 2013). This article thus shows that, independently and *in spite of* one's effort to manage it, one's privacy and right to data protection can be fundamentally undermined by the behaviour of others; further, that this disclosure can be (and often is) exploited by data-hungry organisations whose business model is the insatiable extraction, accumulation and monetisation of personal data (Shoshana Zuboff's *surveillance capitalism* (2015, 2019); see also European Data Protection Supervisor (EDPS) (2020, p. 5).

The economics' aspect of privacy externalities has hitherto often remained absent from the debate about the phenomenon. Indeed, the interdependent dimension of privacy, as well as the issue of privacy externalities, are being directly addressed in legal, policy and philosophical scholarship at least since the 2010s. Part of the

contribution made by this article is the collection of relevant literature, which otherwise stands in isolated clusters and refers to a similar phenomenon using different concepts, such as: *joint controllership*, and *privacy infringements* (Helberger and van Hoboken, 2010; van Alsenoy, 2015; Edwards et al., 2019) or *infringements of data protection law* and *networked services* (Mahieu et al., 2019); *collective privacy* (Squicciarini et al., 2009) and *collective action problems in privacy law* (Strahilevitz, 2010); *multi-party privacy* (Thomas et al., 2010); *collateral damage* and *spillover* (Hull et al., 2011; Symeonidis et al., 2016); *interpersonal management of disclosure* (Lampinen et al., 2011); *networked privacy* (boyd, 2011; Lampinen, 2015; Marwick and boyd, 2014); *interdependent privacy* (Biczók and Chia, 2013; Symeonidis et al., 2016; Pu and Grossklags, 2017; Kamleitner and Mitchell, 2019); *peer privacy* (Chen et al., 2015; Ozdemir et al., 2017); *multiple subjects personal data* (Gnesi et al., 2014); *privacy leak factor*, *shadow profiles* and *online privacy as a collective phenomenon* (Sarigol et al., 2014); *privacy externalities* (Laudon, 1996, pp. 14-6; MacCarthy, 2011; Humbert et al., 2015, 2020; Symeonidis et al., 2016; Choi et al., 2019), especially as compared to externalities in the context of environmental pollution (Hirsch, 2006, 2014; Hirsch and King, 2016; Froomkin, 2015; Nehf, 2003; Ben-Shahar, 2019); [1] *genetic groups* (Hallinan and De Hert, 2017); or *sociogenetic risks* (May, 2018). [2]

While the phenomenon has thus been addressed in scholarly and policy settings already (although often with a different goal or scope), the present article frames it in a way which puts into light an important aspect hitherto mostly unaddressed. This aspect is the financial incentives and the exploitative dynamics behind these disclosures of others' data; it is not only a major factor in making the phenomenon ethically problematic, it is also the very reason the phenomenon is perpetuated. These incentives and dynamics give competition and consumer-protection ramifications to this data protection issue, and failing to pick up on them has hindered scholars and authorities from adequately grasping and addressing the problematic

1. While these authors also use the term *privacy externalities*, they do not analyse the same dynamics that this paper addresses at length in section 3. Further, the scope of the phenomenon they examined is not exactly the same, and some even use the concept of externality in a very different (though relevant) sense.

2. In addition to this list of directly-related work, the topics of interdependent privacy or privacy externalities have been more tangentially or briefly touched upon by the following: Bloustein, 1978; Roessler and Mokrosinska, 2013 (*the network effect*); Kitchin, 2014a (*data shadows*); Hull, 2015; Jia and Xu, 2016 (*collective privacy*); Taylor et al. , 2017 (some aspects of *group privacy*); Facebook Inc., 2018 (the sharing of one's friends information with third-party apps in the Fracebook-Cambridge Analytica scandal); Garcia-Murillo and MacInnes, 2018. See also Section 3.1 below for authors who address particular cases of privacy externalities.This article's topic itself is situated within a wider context of more theoretical critiques of individualistic notions being applied to the networked self; the article puts these aside to focus on concrete cases and dynamics.

phenomenon.

This concern about externalities is moreover different from more traditional data protection issues of inappropriate disclosure such as leaks and hacks: privacy externalities are not only about *bad* personal data management, but also about *impossible* personal data management. Privacy cannot adequately be managed alone, as it is in some aspects necessarily an interdependent matter. Whereas this is a neutral fact about the world, the way we (do not) deal with it is problematic, because individual users and controllers take advantage of it and allow costs to be imposed onto others, undermining their privacy. This is even more deeply problematic as the current data ecosystem (which generally harvests every bit of data for monetisation or exploitation) has been designed in a way that often amplifies the negative nature of privacy externalities. Framing the issue as one of privacy externalities and exploitation, instead of as the mere downside of certain technologies, is moreover important if we want to have an adequate philosophical, societal and juridical debate on the issue of privacy externalities, because it allows us to recognise the responsibilities upon which the relevant parties fail to act.

In this article, I begin by introducing the ideal of privacy self-management which, in an ecosystem that heavily relies on consent as the legal basis for data processing, is *de facto* commonly imposed onto data subjects through the 'Notice and Choice' (N&C) framework; this self-management ideal is contrasted with the reality of the interdependent dimension of privacy (section 2). I argue that improperly taking this dimension into account allows for the creation of privacy externalities, whereby others inconspicuously and unfairly pay (part of) the price for others' benefit; moreover, I argue that this is the term most appropriate to conceptualise and analyse the phenomenon (section 3). Building upon the concepts and concrete examples discussed in the existing body of literature collected, I then attempt to draw a systematic and comprehensive picture of the phenomenon, analysing the various forms it takes (section 3.1). Finally, I briefly explore two possible ways of addressing the issue of privacy externalities (section 3.2).

In terms of methodology, this article does a conceptual analysis of a concrete issue (privacy externalities), combining theoretical insights from the field of economics with knowledge of data protection legislation and real-life examples. This analysis responds to, and is informed by relevant works in the existing literature.

2. Privacy self-management and interdependent privacy

The 2016/679 General Data Protection Regulation (GDPR) states (art. 5) that personal data shall be (a) processed lawfully, fairly and in a transparent manner in relation to the data subject, (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, and (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. While additional principles are important in the European data protection regulation, these 'lawfulness,' 'fairness,' 'transparency,' 'purpose-limitation' and 'data minimisation' principles are its pillars.

To ensure the lawfulness of their processing, however, the majority of processors in practice rely on only one of the multiple grounds available: consent. Consent, as an expression of individual autonomy, is accorded great value in Europe and particularly in the field of data protection, with the consequence that some controllers over-rely on it or use it to (erroneously attempt to) legitimise routine or even disproportionate data processing (for an in-depth analysis of this topic, see van Alsenoy et al., 2013, pp. 4-6). In consequence, the framework of N&C (especially through online privacy notices) has sprung forward as the *de facto* preferred means by controllers to ensure the transparency of their practices and to collect the consent of data subjects (see also Barocas and Nissenbaum, 2014; Hull, 2015; Mantelero, 2017, p. 72). In practice, this, together with a widespread business model relying on the collection and monetisation or exploitation of personal data (EDPS, 2020, p. 5; Holloway, 2019), has led to an individualistic system of personal data protection where the consent of individuals is repeatedly queried for a multitude of purposes, whereas in theory, a data subject would not necessarily have to micromanage their privacy as much as they currently do.

This means that privacy management often takes the contractual form of two parties agreeing about the processing (the collection, use, disclosure, etc) of the data subject's personal information (personal data), in exchange for a service offered by the controller. It is furthermore reflected in one of the currently dominant legal and philosophical definitions of privacy, which is: the relative control over the ways and the extent to which one selectively discloses (information about) oneself to others. [3]

3. 'Relative', because there is a continuum of degrees of control that fall under the concept of 'having privacy'. It is difficult to specify what degree of control is required, especially as privacy is at least partly subjective and context-sensitive (Kupfer, 1987; Nissenbaum, 2004).For references to this understanding (i.e., definition) of privacy, see Westin, 1967, p. 7; Culnan and Armstrong, 1999; Culnan,

This (over-)reliance on consent has the impractical effect that the privacy of individuals is only protected *per* individual, i.e., it is achieved in an individualistic fashion, where data subjects have to (and are expected to) micro-manage their privacy (Whitley, 2009; Solove, 2013; van Alsenoy et al., 2013; Mantelero, 2014; Taylor et al., 2017, p. 6). In addition to the burden of self-management it creates for individuals, it will become clear that this individualism is also problematic because it obscures the fact that, in many instances, the data subject's choice to consent in fact impacts other data subjects, and thereby pre-empts these third parties' own consent. Indeed, privacy has both a collective and an interdependent dimension to it.

To see this, one has to understand the scope of the GDPR's definition of personal data, which is

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (GDPR, art. 4.1)

This definition is extensive, and protects data subjects whenever information about them is processed. Crucially for this article, the scope of this definition also entails that one's personal data may also be another's personal data. When I upload material on a website, it is related to me (and, therefore, is my personal data) in that it is uploaded *by* me, and *about* me—two relations of 'identifiable relatedness' arguably relevant for constituting personal data. Accordingly, when I upload content clearly about someone else (henceforth a 'third-party subject'), it is both my personal data *and* theirs—as long as they are identifiable—because, although it is uploaded *by* me, it is *about* them. These relations can be referred to as 'causal agency' and 'personal relevance.' [4]

If they do not also have a 'causal agency' relation to it, controllers rarely (if ever) provide N&C or other rights to data subjects who have a 'personal relevance' rela-

2000; Cohen, 2000; Weinreb, 2000; Hann et al., 2002; Whitman, 2004, p. 1161; Bygrave, 2004, pp. 324-5; Moore, 2007; Bennett and Raab, 2003 ch. 1; De Hert, 2008; Solove, 2008 ch. 2; Whitley, 2009; Mantelero, 2014, 2017 pp. 71-72. Although privacy may be defined in different ways (see Introna, 1999; Solove, 2002), it is unfortunately out of the scope of this article to discuss other conceptions.

4. An even broader perspective would be that "[i]nformation can 'relate' to an individual in content, purpose, or result" (Purtova, 2017, p. 54).

tion with the material (data) processed. For instance, Facebook has a portal dedicated to the provision of their personal data to Facebook users; yet, this access is restricted to "information you've entered, uploaded or shared [yourself]." [5] This is incoherent, when one realises that the range of our personal data processed (often knowingly) by Facebook exceeds the data we have provided ourselves. This also means that a narrow understanding of personal data is often applied, and therefore that many data subjects' right to effective data protection is unfairly restrained.

The distinction made between the two kinds of 'identifiability' is important, because it allows me to identify and frame a major obstacle to privacy self-management: the interdependent dimension of privacy, i.e., the idea that in a networked world, one's privacy depends at least partly on others (and on the choices they have themselves made regarding their own privacy). While I may decide what information about myself I give to the world (and to individual controllers), others may decide it for me as well; I am thus at least partly dependent on others for retaining my informational privacy. This interdependent dimension is an obstacle insofar as privacy is framed as an individualistic matter (through the N&C mechanism that is the favoured tool of many controllers to achieve appropriate data protection), an aspect of one's life which is self-(sufficiently-)manageable.

3. Privacy externalities

As mentioned earlier, an externality is a cost or benefit imposed on a third party who did not choose to incur that cost or benefit, and which is the by-product of an activity (such as the production or consumption of a service). Externalities often occur when the equilibrium price (i.e., the price when supply and demand are balanced) for the production or consumption of a service does not reflect the true costs or benefits of that service for society as a whole (see Heath, 2007). In the context of informational privacy, this article argues that people's decisions to use certain services, or to share their personal information, may allow the data controller to know more about them, but also about others. To the (limited) extent that people can be said to 'pay' for a service with their data, [6] part of the price is actually also other people's data. That is, the full costs of the production or consumption of the service include the impact on others' privacy and the (dis)utility

5. Facebook Inc. https://www.facebook.com/your_information/ (accessed 17/03/2020).

6. While this narrative is not particularly accurate—as the reality is closer to users providing the controller with information about themselves which can then be exploited for e.g. advertising purposes—it is useful to convey the message that the 'price' of a service can be shared (i.e., shared among all those whose data is provided). See specifically EDPS, 2014b, p. 37, and Zuboff, 2019, p. 94.

resulting therefrom—a form of latent harm peculiar to the 21st century (Calo, 2011; Laudon, 1996, pp. 16-17; see also Article 29 Data Protection Working Party (WP29), 2014, p. 37; see also van Dijk et al., 2016, on "increased risks to rights"; see also Ben-Shahar, 2019, on how these externalities "undermine and degrade public goods and interests"); [7] the problem is that this is neither transparent nor accounted for in the transaction between user and service-provider. Hence the term *privacy externalities*.

Referring to the phenomenon as *privacy externalities* allows me to capture a crucial aspect of the issue: the cost of services in the digital, hyperconnected era and, furthermore, the externalisation of these costs. While other terms used to refer to the phenomenon (see section 1) conceptualise it as a mere side-effect of certain digital practices, using the concept of externality brings to light the fact that this side-effect is not neutral, i.e., that users and/or controllers are not indifferent to it (whether they are conscious of it or not). On the one hand, by not investing as much as they should in the design of their service, and by not addressing all their obligations toward (third-party) data subjects, controllers can *de facto* dump costs and responsibilities onto the user (such as the duty to notify the user's peers of the data processing, in the case of smart homes), [8] thereby saving resources. On the other hand, by not carefully choosing privacy-respecting services (when that is possible), and/or by not taking adequate precautions for others' privacy when using these services, users may often themselves be dumping costs onto third-party subjects: the infringement of their privacy, increased risks to their rights, potential harm, as well as the time and energy required for taking the appropriate measures (when possible). [9] This means that privacy externalities can cause distortions in

7. Privacy externalities can be both negative and positive for third parties; however, while the benefits are often appropriated and internalised by the controller, the costs remain orphan—affecting groups too broad and dispersed, and causing injuries that are too abstract for private remedies to be effective (Ben-Shahar, 2019, p. 115).Moreover, when considering harm, it is good to go beyond mere monetisation and to note that privacy externalities can also serve for the surveillance of specific individuals, as they amount to a form of (often unintended) lateral and decentralised surveillance, i.e., monitoring by one's peers, the recordings of which can be consulted by the controller or requested by law enforcement (on this, see also Zuboff's surveillance capitalism (2015)).

8. See Google's statement that "[y]ou (and not Google) are responsible for ensuring that you comply with any applicable laws when you use Nest devices and services, including any video recording, biometric data or audio recording laws that require you to give notice or obtain consent from third parties" (Google, https://support.google.com/googlenest/answer/9327735?hl=en&ref_topic=7173611, accessed 28/03/20).

9. To keep the same example, Google's smart home system Nest has a voice recognition feature which allows guests to add their own account to the owner's device, following which their interactions will be stored in their own communication history at myactivity.google.com. When unrecognised data subjects interact with the device, their communication history is stored in the activity history of the Google Account used to set up the device (i.e. the owner's). Google therefore recommends

the production and consumption of social goods, by making the perceived price of a service lower than the actual total cost, and therefore more attractive than it should be.

Moreover, because some service providers' business model relies on the accumulation and monetisation of as much data as possible (Zuboff, 2015; EDPS, 2020, p. 5; Holloway, 2019), privacy externalities are costs for third-party subjects not only in the sense that they expose the latter and undermine their rights to privacy and data protection, but also in the sense that they make way for profit-driven controllers to (illegally) exploit this data for their own benefits at the expense of the data subjects (see esp. Court of Justice of the European Union (CJEU), 2019, para 80, and Ben-Shahar, 2019, p. 115; see also Humbert et al., 2020, on service providers as "adversaries"). For instance, exploiting the externalities generated through the sharing of users' contact data is part of Facebook's massive targeted prediction and advertising endeavour, which is how the company makes most of its profit (Venkatadri et al., 2019). Similarly, direct-to-consumers genetic testing services which offer to predict medical risk factors and to reveal ancestry or genealogy actually make profit through reusing the data for medical research, profiling, and offering their services to law enforcement (EDPS, 2020, pp. 5, 25). Thus not only does the flawed price of the relevant services allow controllers to save resources, it also leads users to consume more of these services, feeding the controllers even more data to extract value from. Realising the potential residing in these troves of data, some rogue controllers may even intentionally design the structure of their services so as to encourage and capture such privacy externalities, leading powerless, careless or unaware users to provide the system with not only data about themselves, but also about others.

These passively and actively beneficial aspects of privacy externalities are thus, effectively, incentives for the perpetuation of the phenomenon. They are crucial to understanding and tackling it, and their absence from the existing literature on the topic is therefore regrettable. Moreover, in addition to not picking up on the economic aspect of the phenomenon, the authors of the works cited in section 1 often only addressed it in relation to a unique context—such as social networks or databases. Similarly, when the issue was addressed at court- or policy-level, the kind of privacy externalities taken into account did not necessarily reflect the whole range

the user to make sure any guests "understand that their interactions will be stored by Google in [the owner's] Google Account and that [the owner] can view and delete that information", and adds that the owner "may consider muting the microphone or unplugging and putting the device away" when there are guests (Google, https://support.google.com/googlenest/answer/7177221?hl=en, accessed 06/12/2020).

of the phenomenon (see the categories discussed below). This substantially limited the scope of both their analysis and the solutions they sought, with for instance the CJEU and the WP29 focusing on the 'disclosure to [a certain number] and [a certain kind] of peers' as a criterion determining the wrongness and illegitimacy of the processing (CJEU, 2003; WP29, 2013, p. 2).

Further, and especially as these works are scattered in 'clusters' that do not necessarily refer to each other, [10] the absence of the broader perspective in these studies would lead one to believe, at first sight at least, that these works (or clusters) address a different issue from one to the other. By abstracting the contingencies from each case and putting them all under the umbrella of privacy externalities, however, one can identify the different clusters, and it becomes apparent that there actually is a whole body of literature on the phenomenon, instead of scattered studies of different phenomena.

Still in contrast to the works referenced above, the present article brings about the clear distinction between two separate things that their authors often discuss inextricably interwoven, and unites their work as revolving around this distinction. This distinction is between the interdependent (or networked, interpersonal, collective, social) aspect of privacy—which is a necessary fact about the world—and the phenomenon of privacy externalities (or spillovers, collateral damages, disclosures, leaks)—which is partly contingent on controllers' and users' decisions. This distinction, and especially this contingency (i.e., the fact that it depends on other factors, such as default privacy settings or on the way a service is used), is important when (if) the responsibility of the various actors is addressed (section 3.2).

We may thus start to see the broader picture, and to focus on the cause of the problem instead of its symptoms. This article argues that privacy externalities are mostly the result of the necessarily interdependent dimension of individual privacy being *coupled* with economic incentives to externalise certain costs (and to exploit and monetise them further in complex and obscure ways when possible). The phenomenon is widespread and may produce or amplify future harm (including intrusive predictions and advertising), at least when the issue is systemic and the externalities accumulate. Besides, the phenomenon violates individuals' right to privacy and threatens the ideal of privacy self-management itself, independently from whether it produces concrete (latent, tangible or intangible) harm or not, and inde-

10. This was also demonstrated by Humbert et al. (2020) regarding interdependent privacy. However, through my analysis of privacy externalities, yet more of these clusters have been uncovered—accentuating the point that "research on the topic has been conducted in isolation in different communities" (*ibid*, pp. 2, 4).

pendently from whether it is exploited by the controller or not; it is yet another risk to the rights of data subjects. Like Martin Tisne (2019, n.p.) succinctly puts it, "we are not only bound by other people's data; we are bound by other people's consent [… and] this effectively renders my denial of consent meaningless. […] The issue is systemic, it is not one where a lone individual can make a choice and opt out of the system" (see also Barocas and Nissenbaum, 2014). This practice, whereby one's consent is overridden, should receive the attention it deserves, especially in light of the expectations of privacy self-management.

Disclosure of others' personal data through one's activities can be repetitive, commonplace, extensive and substantial, and is thus a serious issue. Building upon the concepts and examples discussed in the existing literature, I will now have a closer and systematic look at the various forms privacy externalities can take.

3.1. Four different kinds of disclosure

Privacy externalities can take multiple forms, each problematic in their own way. Once abstracted from their individual contingencies, they can be separated into the following four (possibly overlapping) categories:

1. Direct disclosure: data is revealed about subject A when subject B discloses data about subject A.
2. Indiscriminate sensing: data is revealed about subject A when subject B reveals data about subject B that was formed through an indiscriminate process of capture, and which therefore *included* data about subject A alongside the data of subject B.
3. Fundamentally interpersonal data: data is revealed about subject A when subject B reveals data about subject B, which *necessarily is* also data about subject A.
4. Predictive analytics: subject B discloses data about subject B, from which the data controller is able to infer or predict *more* data about subject B as well as about subject A.

The difference between categories (2) and (3) is that in the former, the *interpersonal data* (the term used here for data which is about more than one subject) is only contingently interpersonal, whereas in the latter it is necessarily so. In the former, the data could have been only about the user, if she had been cautious for instance; that is not an option in the latter category. The distinction becomes clearer with examples from each category:

1. Direct disclosure: as long as it is digitally-recorded, any activity that consists in explicitly discussing about someone counts as revealing that person's personal data, and thus as an activity relevant to interpersonal

privacy. This includes blogging about people (Solove, 2007, p. 24); talking about them and posting pictures of them on social networks (Wong, 2009, p. 143 et seq.; van Alsenoy et al., 2009, p. 70; Helberger and van Hoboken, 2010; College Bescherming Persoonsgegevens ('CBP'), 2007, pp. 12-13; Belgisch Commissie voor de Bescherming van de Persoonlijke Levenssfeer, 2007, pp. 21-22); outing a sexual preference online, broadcasting a traumatic experience, public shaming or posting 'revenge porn' (van Alsenoy, 2015); or "tagging" others (see Privacy International, 2019 about the app 'TrueCaller'). Beside this, category 1 also involves directly handing over other people's data to the data controller, like when Facebook apps ask the user to access her friends' list and their data (Besmer and Lipford, 2010; Hull et al., 2011; Bizcók and Chia, 2013; Symeonidis et al., 2016, Facebook Inc., 2018). Moreover, embedding a Facebook "Like" button into one's personal website (CJEU, 2019, para 76-7) *de facto* means handing over the personal data of visitors to Facebook, and similarly for other buttons and third-party services allowing behavioural targeting and user analytics (Mahieu et al., 2019).

2. Indiscriminate sensing: recording one's voice or environment often also implies indiscriminately recording others. Sensors capture all the available data of a given category (e.g., sound or image) within a perimeter, and do not discriminate between consenting and non-consenting data subjects. Therefore, the following activities will also capture the personal data of other people who may neither be aware nor capable of resisting the invasion of their privacy: uploading pictures of crowded places on social media; using a drone or Google Glass (van Alsenoy, 2015; EDPS, 2014 a); driving someone in one's connected car (EDPS, 2019b, p. 3) or just driving a self-driving car around; 'Netflix & Chilling' in front of a smart TV; relying on a Ring doorbell (Herrman, 2020); using 'voice assistants' [11] or 'smart' speakers in one's home (EDPS, 2019a, p. 3). Recording events in sound or image can be a sensitive practice, because many personal aspects of one's and others' life can be thus made available to data controllers, including sensitive data like political opinions, religious beliefs, or health data (Vallet, 2019). This data can moreover be automatically 'mined' by image-processing, voice-processing, and facial-recognition software. This category is quite broad, and includes CCTV (ICO, 2017; CJEU, 2014b); Internet of Things objects; or smart homes (see Kitchin, 2014b).
3. Fundamentally interpersonal data: there are some kinds of data which necessarily constitute or reveal personal data of multiple persons. A striking example is genetic data: giving rights to a data controller to process your genetic data not only affects you and your privacy, but also potentially countless individuals to whom you are related—knowingly or unknowingly (Chadwick et al., 2014; Olejnik et al., 2014; Hallinan and De

11. For a discussion of privacy issues and related risks brought about by voice assistants, see Veale et al., 2018. Their discussion of privacy harms, rights and data protection by-design for Apple's Siri is applicable to the risks and harms highlighted here for third-party subjects.

Hert, 2017; Taylor et al., 2017, p. 9; Erlich et al., 2018; May, 2018; Molteni, 2019). Because certain genetic traits are necessarily shared with family members, it suffices that a single person undertakes such an analysis for a kind of 'family-wide sharing of personal data' (i.e., a generational data breach). Other practices involving such interpersonal data include telecommunications (where the metadata reveals at least the identity of correspondents and the frequency of calls); the use of certain email providers (Dodds and Murphy, 2018; Ben-Shahar, 2019, p. 115); or the use of a shared system (such as smart grids, see McDaniel and McLaughlin, 2009). Finally, the category of fundamentally interpersonal data also includes relational data (Jernigan and Mistree, 2009; boyd, 2011; Backstrom and Kleinberg, 2014; see also the activity of address book sharing described in section 3.2.1), but also data about groups (such as households or neighbourhoods) (Taylor et al., 2017).

4. Predictive analytics: when enough people disclose ample information about themselves, data controllers (especially data brokers) are able to understand the relation between having a given trait and a specific characteristic. For example, there is a correlation between, on the one side, buying felt-pads to prevent one's furniture from scratching the floor, and on the other side paying one's bills on time (Duhigg, 2009). When correlations like these have been found (through mining massive troves of data), the small, seemingly-insignificant pieces of information that even prudent people disclose (willingly or not) will reveal more data about them, whether they like it or not (Barocas and Nissenbaum, 2014, the "tyranny of the minority"; Choi et al., 2019, p. 8, Wachter and Mittelstadt, 2019). This is the case of the 'dynamic' groups from profiling categories, 'Big Data' analytics, predictive analytics and recommendation systems (Vedder, 1997; boyd et al., 2014; Mantelero, 2014, 2017). [12]

These four categories and the examples provided show how important and diverse the cases are where one's behaviour can negatively impact (the privacy of) others, and thus that the issue at stake here is not a rare or minor one. Each of the non-sensitive pieces of data that are thereby processed may seem innocuous on their own; however, not only does their processing remain an encroachment on and increased risk to third-party subjects' fundamental rights, but when the phenomenon is widespread, the aggregation of all its instances will worsen its potential to do harm. Furthermore, even the smallest disclosures are significant, due to the possibility of the data being exchanged with others (such as data brokers, see

12. Category 4 represents a very important kind of privacy externality. However, it may be valuable to note that the category relates both to the *collective* dimension of privacy (Mantelero, 2016) and to its *interdependent* dimension. The two dimensions are distinct (neither necessarily implies the other), even though it is sometimes difficult to distinguish between them, due to significant overlap. Acting as if these two dimensions of privacy were the same would limit us, because an important element would be missing from the analysis of privacy.

Symeonidis et al., 2016; Choi et al., 2019, p. 8). Finally, in some cases (such as with biometric or genetic data) the data can be very sensitive, and the harm brought by the disclosure can be lifelong.

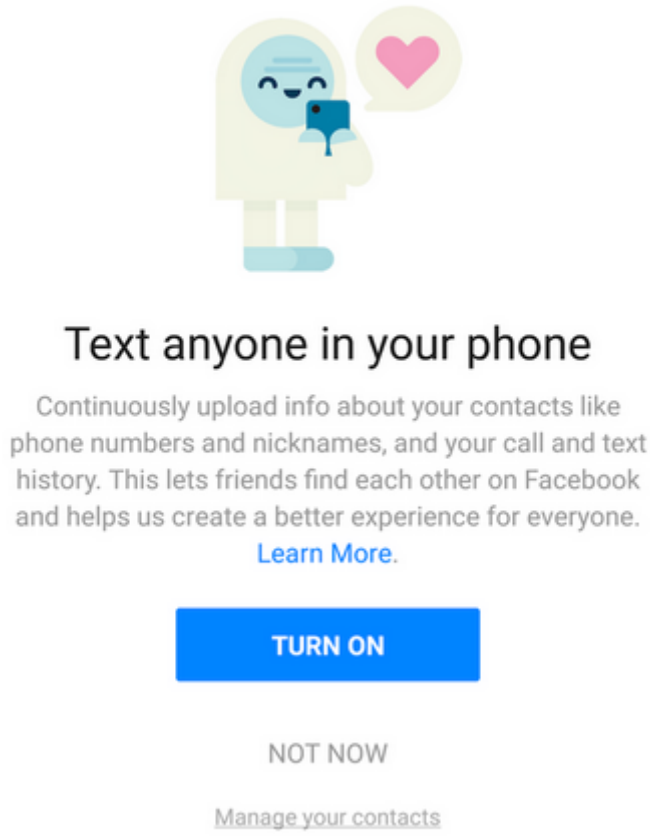

FIGURE 1: Notification from the Facebook Messenger app requesting access to the user's contacts

3.2. Whose responsibility?

Different categories of privacy externalities will plausibly require different coping strategies; for instance, categories 1 and 4 seem to be unavoidable, to a certain extent, and would motivate a mitigating strategy rather than a prevention strategy. It is out of the scope of this article to solve the issue of privacy externalities; however, what the article can still do before closing, is briefly exploring two promising paths.

The common denominator to the most problematic kinds of privacy externalities is the perpetuating force behind them, i.e., the passive and active benefits of externalities—respectively: dumping costs, and (the potential for) exploiting the third-

party subjects' data. Tackling these incentives should be at the heart of any response to the phenomenon. However, it should be noted that while the active benefits are enjoyed by data controllers alone, the passive ones (cheaper prices, less effort required, etc) are enjoyed by both the controllers and the users. While focusing on data controllers is therefore the logical place to start (and thus the first path examined), the roles of users should not be overlooked.

3.2.1. Enforcing data protection by design and by default

The controller often plays an important role in the generation of externalities. For instance, some controllers offer services through which the acquisition of the personal data of the subject's peers is requested, even though such services could do without it. The comparison between messaging apps Facebook Messenger and Signal illustrates this well.

Messenger asks the user to (consent to) *upload* her contacts to Facebook's servers, and to do so *continuously* (see figure 1). Facebook thus stores internally the contacts' data, with the ensuing function creep Facebook is notorious for (Gebhart, 2018; Venkatadri et al., 2019). Signal, on the other hand, periodically sends the user's contacts' phone numbers to its servers in truncated, cryptographically-hashed form; it then identifies the overlap (i.e., the user's contacts who also use Signal) and indicates this overlap on the user's device exclusively, after which the server discards the information it received about the user's contacts. [13]

In general, even if only limited data, such as the nickname and a phone number, were disclosed for each contact in the user's list, it would remain a potentially fruitful acquisition for the controller, as the widespread disclosure by users of their contact list would allow the controller, if it were as privacy-invasive as Facebook is, to identify the overlapping contacts in users' phones, create network maps and start building 'shadow profiles' about non-users (WP29, 2009, p. 8; Sarigol et al., 2014; boyd et al., 2014; Levy, 2020, p. 222). Even solely knowing about this network of relations is valuable to the data controller, based on homophily—the tendency people have to interact with others who are similar to them. Homophily can be relied on to infer the "ethnicity, gender, income, political views and more" of people based on their communication networks (Caughlin et al., 2013, p. 1; see also Sarigol et al., 2014; Garcia, 2017; Jernigan and Mistree, 2009 (the "Gaydar")). Thus, my ability to remain under Facebook's (or others') radar is heavily under-

13. See "How does Signal know my contact is using Signal?" at https://support.signal.org/hc/en-us/articles/360007061452-Does-Signal-send-my-number-to-my-contacts- (Accessed 18/03/20). This system became notorious as a 'compare and forget' system when WhatsApp came under scrutiny by the Dutch data protection authority (DPA) for the way it handled contact data (see CBP, 2013, p. 30).

mined by other individuals' seemingly innocuous actions, which not only disclose information about them, but also (foreseeably) about me—even if I am not a Facebook user myself. This is not the case for data subjects using Signal.

While Facebook in this case is invasive by design, Signal follows the approach of Data Protection by Design and by Default (DPbDD) which requires (GDPR art. 25) taking technical and organisational measures to (a) implement data-protection principles in an effective manner and to (b) ensure that only personal data which are necessary for each specific purpose of the processing are processed. DPbDD forces complying controllers to take the necessary steps to prevent, contain and mitigate the privacy externalities that might result from (the way they offer) their services. As such, the strength of DPbDD is that it is a solution generic enough to be applied to privacy externalities beyond messaging services (i.e., to "handle various data types and adversaries" (Humbert et al., 2020, p. 33)). For instance, Facebook incorporated some mechanisms to reduce privacy externalities on its platform, such as requiring the peers' assent before a user can tag them in a picture or make them appear on her Facebook wall. Another example of useful DPbDD is found in clinics, where there are legal and other mechanisms governing conduct when genetic information about an inherited disease is relevant to the tested person's relatives, or for cases where a diagnostic incidentally indicates misattributed paternity.

While DPbDD requirements are specified in the GDPR and are thus the remit of data protection authorities, privacy externalities hitherto persist nearly unchallenged (perhaps due to these authorities' lack of adequate funding, see Ryan and Toner, 2020; Satariano, 2020). In light of the harm certain practices can cause to third-party subjects, it could be argued that other authorities, especially consumer-protection authorities, should take data protection issues more seriously into consideration (without prejudice to the data protection authorities' powers) (on this, see Rhoen, 2016; see also EDPS, 2014b). Further research is needed to explore the extent to which this is possible; either way, the idea is that the stricter enforcement of DPbDD requirements—especially for services that seem to be *invasive* by design (rather than merely not designed with privacy in mind (see Helberger and van Hoboken, 2010, p. 106; see also CJEU, 2019, para 80))—could efficiently address part of the privacy externalities (van Alsenoy, 2015, p. 32, Edwards et al., 2019), i.e., the part where controllers are otherwise incentivised to dump certain costs and obligations onto the user and third-party subjects.

One should be held accountable when one facilitates risks and harms for the peers of the users of one's services; inaction is unacceptable, even more when one is

profiting from this inaction, and taking advantage of the issue should be a no-go. Yet, the whole issue cannot be averted through the enforcement of these DPbDD requirements alone, because the user often plays an important part in the creation of externalities (through the way they use certain technologies, or the invasive practices they opt-in for), and because the issue can sometimes be most effectively and cost-efficiently addressed by users themselves. [14] The question is, in the current state of affairs, how much can we rely on individuals to adequately internalise the costs of their behaviour? This question leads us to a second, arguably more intricate, way out: the framework of joint controllership.

3.2.2. Joint controllership

To illustrate the need for this complementary strategy, let us take the case of the smart home. A smart home is a data-driven premise which necessarily monitors all its occupants to provide its services, since its sensors most of the time cannot distinguish between the user and her relatives or visitors. In such a scenario, it is inevitable that the service will generate privacy externalities, and it is unclear whether thorough DPbDD would adequately prevent or mitigate them all.

In essence, when multiple natural or legal persons determine the purpose and means of processing of the personal data, under the GDPR they are joint controllers and each is responsible for the part of the processing that it controls, to the degree it has control over it (see GDPR art. 26). Following European jurisprudence (CJEU, 2018) and guidance from the WP29 (2010, p. 18), it appears that "[i]nfluencing the processing (or agreeing to the processing and making it possible) [is] enough to qualify as determining both the purposes and the means of that processing operation" (Mahieu et al., 2019, p. 95).

If the user may indeed be considered a joint controller in such cases (but we will see shortly that this claim may be contested), privacy externalities would be internalised (or their negative impact reduced) insofar as the user would be legally responsible for any inadequate processing of her peers' personal data, and would hence be incentivised to take measures to avoid such unlawful processing—such as giving appropriate notice to visitors, or turning the smart devices off before they enter the premises. [15] However, important uncertainties remain regarding how this

14. The discussion about the most appropriate way to address illegal content online may be relevant here (Le Borgne-Bachschmidt et al., 2008). See also Helberger and van Hoboken, 2010, p. 106.

15. Power imbalance between the smart home owners (the 'user') and their peers will however give rise to higher risk of abuse. The user will often be in a position of greater control (e.g. by owning the smart home, and by being able to 'turn it off' (or on) remotely), and there will always be a risk that the third-party subject (e.g. children or the plumber) is not even made aware of the privacy-inva-

framework is to be applied, which raise substantial doubts as to the extent to which joint controllership could form (part of) the solution to the issue of privacy externalities. They are briefly listed below:

1. A first issue is that "the framework for assigning responsibilities to different stages of processing and different degrees of responsibilities is underdeveloped; there are no guidelines for assigning specific responsibilities to specific 'stages', no clear principles to determine different 'degrees of responsibility', nor criteria to connect particular consequences (enforcement actions) to particular levels of responsibility" (Mahieu et al., 2019, p. 99). That is, joint controllership as an effective framework of governance might not be mature enough yet, for this specific context at least.

2. A second issue comes from the GDPR's 'household exemption', which states (Recital 18) that the GDPR "does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity," though it "applies to controllers or processors which provide the means for processing personal data for such personal or household activities". [16] When it comes to its application to privacy externalities, recent judgements from the CJEU (2003, 2014a, 2014b, 2018, 2019) advance criteria for determining whether data subjects using certain services should (a) be considered joint controllers and (b) benefit from the household exemption. The criteria put forward in these judgements would exclude many of the privacy externalities discussed above, [17] but not all externalities would be dismissed: depending on the weight accorded to a criterion endorsed in the Fashion ID CJEU ruling (2019, para 80: that the "processing operations are performed in the economic interests of both" parties), all the externalities passively beneficial to both the user and the controller would be admissible. Furthermore, the active exploitation (in various forms) of third-party subjects' data by controllers, which is a crucial component of the privacy externalities that are most problematic, may also mean that the household/personal activity actually often has an important connection to a commercial activity (or at least that the distinction between personal

sive practice. These predictable power imbalances should prevent data controllers from fully allocating the responsibility for privacy externalities on the smart home user.

16. For a more detailed discussion of the household exemption with regards to data subjects, see Helberger and van Hoboken, 2010; van Alsenoy, 2015; Edwards et al., 2019; van Alsenoy et al., 2009.

17. The criteria include: the processing activity being carried out "in the course of private and family life," and not being made accessible to an "indefinite number of people" (CJEU, 2003); the scale and frequency of the processing, the potential adverse impact on the fundamental rights and freedoms of others (CJEU, 2014b, para 29), or the processing being 'directed outwards from the private setting of the person processing the data' (ibid, para 33).

and commercial is blurred), and may thus not benefit from the exemption (see also WP29, 2017, p. 8). [18] For a more in-depth discussion of privacy externalities, joint controllership and the household exemption, see also De Conca, 202 0.

3. A third issue to be considered comes from the burden of data protection and privacy (self-)management, and from the complexity of being a controller. The GDPR's framework of joint controllership was primarily intended to adequately divide tasks and responsibilities between controllers of organisations—it was not *intended* to make private individuals take on the burden of being a data controller (see OECD, 2011, pp. 27-28). Being a controller entails legal duties and requires thorough understanding of both the legal landscape and the technicalities of data processing; the framework of joint controllership could hence plausibly be too burdensome in practice to be realistically applicable to private individuals (on this issue, see Helberger and van Hoboken, 2010, p. 104; van Alsenoy, 2015, pp. 6, 24, 28; Edwards et al., 2019). And let's not even discuss the increased strain on data protection authorities' limited resources that this solution would entail (see Ryan and Toner, 2020).

4. Finally, if, as the term 'privacy externalities' suggests (as well as the analysis of the incentives behind the phenomenon), this data protection issue can be linked to the context of externalities in environmental pollution, then there may be valuable policy lessons to learn from the latter field. This is what Omri Ben-Shahar (201 9) does, as he frames privacy externalities as "data pollution" (see also Hirsch, 2006, 2014; Froomkin, 2015; Hirsch and King, 2016). However, a central element of his argument is that, just like in environmental protection, "[t]he optimism that contracts and behaviorally-informed choice architecture would help people make wise data sharing decisions and reduce data pollution is fundamentally misplaced, because private bilateral contracts are the wrong mechanisms to address the harm to third parties" (2019, p. 108). He adds that "[i]t is not people who need to be protected from a mesh of data-predatory contracts; but rather, it is the ecosystem that needs to be protected from the data sharing contracts that people endlessly enter

18. It is worth noting that, in its draft for the GDPR, the European Commission (2012, p. 20) restricted the criteria for the household exemption to the "processing of personal data by a natural person […] *without any gainful interest* and thus *without any connection with a professional or commercial activity*" (emphasis added). My framing of the issue of privacy externalities as an (at least partly) incentive-based and exploitable phenomenon means that the latter two criteria considered by the Commission would have been particularly relevant in assessing the scope of the household exemption for the issue at hand. Furthermore, discussing these criteria, the WP29 added (2013, p. 8) that "[t]hought should also be given as to whether non-commercial, non-personal activity […] also needs to be addressed". This grey zone in-between the purely personal and the purely commercial could bring nuance to the debate (although it could arguably just as well muddy it) and allow to better grasp the issue of exploitative privacy externalities.

into" (ibid). If this is right and the analogy with environmental protection holds, then joint controllership will be inadequate to solve privacy externalities, and DPbDD (as part of a wider data protection *ex ante* package, which Ben-Shahar includes within the promising solutions he analyses) is the way to go. [19]

4. Conclusion

Many people remain to this day oblivious to the fact that 'free' services online only mean 'without a monetary cost', and that they actually 'pay' (to a limited and imperfect extent) with their data, i.e., by providing information (*presumably* about themselves) and agreeing that it be leveraged, in particular for intrusive advertising, prediction services or research. However, even those who realise this may not realise that it is not just *their* data they give away: it is often also the data of others. This 'cost' that is imposed on others, the article argued, is a form of disclosure most adequately conceptualised as *privacy externalities*.

This article has demonstrated, in concord with existing literature, that one's privacy is sometimes dependent on others—that is, that there is an interdependent aspect to individual informational privacy. This dimension makes it fundamentally impossible for a data subject to be fully in control of her personal data, despite such expectations. Part of the issue is that, in contempt of other important elements and legal bases in the GDPR, the protection of personal data nowadays still largely relies on consent. This happens through an individualistic mechanism of N&C, whereby only the data subject in direct relation to the controller providing the service is consulted, even if she will foreseeably also provide the personal data of other data subjects as part of the service. This individualistic framework obscures the possibility that one's peers might need to be consulted, or that measures should be taken to mitigate the collateral processing of their personal data, for example.

However, because the existing literature has often conceived of the issue precisely in this sense—that is, as a *collateral* damage, a neutral side-effect—the important dynamics behind the phenomenon have hitherto been poorly highlighted, if at all.

19. Other potential solutions I have not discussed include: reconsidering the framework of privacy protection (see Mantelero, 2014); publishing a list of guidelines for private uses of each relevant technology, and instituting generic provisions in civil and criminal codes (van Alsenoy, 2015, pp. 28, 32); generating a public debate by raising awareness on the privacy implications of relevant technologies, or assisting controllers with compliance (EDPS, 2014a, para 56 *et seq.*; OECD, 2013, p. 32); adapting social norms about privacy; or creating a "lite" framework for individuals who are *de facto* amateur controllers (WP29, 2013, p. 5). Furthermore, the methods to resolve externalities used in economics, i.e., regulation, subsidies and taxation, could also be applied to the issue of privacy externalities (Ben-Shahar, 2019).

The advantage of talking of interdependent privacy, and of taking the economic lens of externalities, is that it allows us to uncover the unethical incentives perpetuating the phenomenon. These are, first and foremost, the passive benefits of dumping costs on others: data controllers on users, and users on their peers. The savings realised are the time, resources and energy that would otherwise be invested in: designing a product of appropriate quality; putting in place legal and other mechanisms governing appropriate conduct in case externalities are created; due diligence; or taking steps to mitigate the externality. As a result, the services offered by data controllers can be offered for cheaper than if the appropriate efforts had been taken to ensure their quality—something which may distort the market by increasing the production and the consumption of these lower-grade services, at the expense of services of better quality (the price of which reflect better their true costs). The negative externalities resulting from the use of these cheaper services are the invisible price for these users' peers. Concretely, these externalities are the unlawful processing of the peers' personal data, the increased risks to their rights that result from it, as well as possible latent, tangible or intangible harm.

Notwithstanding the risks and harms that result from the 'passive' benefits from externalities, additional risks and harms arise when some data controllers also actively create and/or harvest privacy externalities. In a hyperconnected world marked by surveillance capitalism, to rogue data controllers the privacy externalities are only a bonus—a bonus that *further subsidises* their cheap (or 'free') services. However, when the externalities become a feature rather than just a bug, their inexcusable exploitation undermines even further the data protection rights of countless unaware data subjects. This is highly problematic, both ethically and legally, and should be addressed by data protection, but also perhaps by competition and consumer-protection authorities. I briefly pointed toward two possible solutions, marking a preference for the path of better enforcement of data protection by design and by default.

This article has furthermore served the goal of drawing together and listing the abundant and diverse scholarly (and policy) works on the topic. Pertaining to different fields and jurisdictions, using different terms to conceptualise a similar phenomenon, or simply not referring to related publications, the existing literature can be found in clusters that do not make reference to each other. The two lists found in Sections 1 and 3.1 can therefore be used to connect, learn from, and avoid repeating what has already been expressed.

This article, however, does no literature analysis, comparison or evaluation of this

existing body of works and of the solutions (if any) each put forward. What it does, besides framing the phenomenon in a particular way and scrutinising the elements revealed under this particular light, is using the different examples and conceptions of privacy externalities discussed in this body of works to draw a holistic picture of the phenomenon and of the four different forms it can take—something which had not been done before and which is indispensable to fully understand privacy externalities, and hence to appropriately address them.

References

Article 29 Data Protection Working Party ('WP29'). (2009). *Opinion 5/2009 on Online Social Networking (WP163)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

Article 29 Data Protection Working Party ('WP29'). (2010). *Opinion 1/2010 on the Concepts of 'Controller' and 'Processor' (WP169)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

Article 29 Data Protection Working Party ('WP29'). (2013). *Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package—Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities*. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf

Article 29 Data Protection Working Party ('WP29'). (2014). *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Article 29 Data Protection Working Party ('WP29'). (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk*. http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Barocas, S., & H, N. (2014). Big Data's End Run around Procedural Privacy Protections. *Communications of the ACM*, *57*(11), 31–33. https://doi.org/10.1145/2668897

Belgisch Commissie voor de Bescherming van de Persoonlijke Levenssfeer. (2007). *Aanbeveling Uit Eigen Beweging Inzake de Verspreiding van Beeldmateriaal*. Belgisch Commissie voor de Bescherming van de Persoonlijke Levenssfeer (Belgian data protection authority).

Bennett, C. J., & Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd and updated ed.). MIT Press. https://doi.org/10.1080/19331680801979039

Ben-Shahar, O. (2019). Data Pollution. *Journal of Legal Analysis*, *11*, 104–159. https://doi.org/10.1093/jla/laz005

Besmer, A., & Lipford, H. R. (2010). *Users' (Mis)Conceptions of Social Applications*. Proceedings of Graphics Interface. https://doi.org/10.1007/978-3-319-07509-9_2

Biczók, G., & P.H, C. (2013). *Interdependent Privacy: Let Me Share Your Data. Financial Cryptography and Data Security*. Springer. https://doi.org/10.1007/978-3-642-39884-1_29

Bloustein, E. J. (1978). *Individual and Group Privacy. Transaction Publishers.*

Boyd, d. (2011). *Networked Privacy*. Personal Democracy Forum. https://www.danah.org/papers/talks/2011/PDF2011.html.

Boyd, d, K., L., & Marwick, A. E. (2014). The Networked Nature of Algorithmic Discrimination. In S. P. Gangadaranwith, V. Eubanks, & S. Barocas (Eds.), *Data and Discrimination: Collective Essays*. Open Technology Institute and New America. http://www.newamerica.org/downloads/OTI-Data-an-Discrimination-FINAL-small.pdf

Bygrave, L. A. (2004). Privacy Protection in a Global Context. A Comparative Overview. *Scandinavian Studies in Law*, *47*. https://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf

Calo, R. (2011). The Boundaries of Privacy Harm. *Indiana Law Journal*, *86*(3). http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf

Caughlin, T. T., Ruktanonchai, N., Acevedo, M. A., Lopiano, K. K., Prosper, O., Eagle, N., & Tatem, A. J. (2013). Place-Based Attributes Predict Community Membership in a Mobile Phone Communication Network. *Angel Sánchez. PLoS ONE 8*, *2*. https://doi.org/10.1371/journal.pone.0056057

Chadwick, R. F., Levitt, M., & Shickle, D. (Eds.). (2014). *The Right to Know and the Right Not to Know: Genetic Privacy and Responsibility* (Second). Cambridge Bioethics and Law. Cambridge. https://doi.org/10.1017/CBO9781139875981

Chen, J., Ping, J. W., Xu, Y., & Tan, B. C. Y. (2015). Information privacy concern about peer disclosure in online social networks. *IEEE Transactions on Engineering Management*, *62*(3), 311–324. https://doi.org/10.1109/TEM.2015.2432117

Choi, J. P., Jeon, D., & Kim, B. (2019). Privacy and Personal Data Collection with Information Externalities. *Journal of Public Economics*, *173*, 113–124. https://doi.org/10.1016/j.jpubeco.2019.02.001

Cohen, J. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, *52*, 1373–1438. https://doi.org/10.2307/1229517

College Bescherming Persoonsgegevens. (2007). *Publicatie van Persoonsgegevens Op Internet* [Guidelines]. College Bescherming Persoonsgegevens (Dutch Data Protetection Authority). https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf

College Bescherming Persoonsgegevens. (2013). *Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc* (Report No. Z2011-00987; Issue Z2011). College Bescherming Persoonsgegevens (Dutch Data Protetection Authority). https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-whatsapp-dutchdpa-final-findings-en.pdf

Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing*, *19*(1), 20–26. https://doi.org/10.1509/jppm.19.1.20.16944

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

De Conca, S. (2020). Between a rock and a hard place: Owners of smart speakers and joint control. *SCRIPT-Ed*, *17*(2), 238–268. https://doi.org/10.2966/scrip.170220.238

De Hert, P. (2008). Identity Management of E-ID, Privacy and Security in Europe. A Human Rights View. *Information Security Technical Report*, *13*(2), 71–75. https://doi.org/10.1016/j.istr.2008.07.001

Edwards, L., Finck, M., Veale, M., & Zingales, N. (2019). Data Subjects as Data Controllers: A Fashion(Able) Concept? *Internet Policy Review*. https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400

Erlich, Y., Shor, T., Pe'er, I., & Carmi, S. (2018). Identity Inference of Genomic Data Using Long-Range Familial Searches. *Science*, *362*(6415), 690–94. https://doi.org/10.1126/science.aau4832

European Commission. (2012). *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

European Data Protection Supervisor. (2014a). *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on 'A New Era for Aviation Opening the Aviation Market to the Civil Use of Remotely Piloted Aircraft Systems in a Safe and Sustainable Manner, COM(2014) 207 Final*. https://edps.europa.eu/sites/edp/files/publication/14-11-26_opinion_rpas_en.pdf

European Data Protection Supervisor. (2014b). *Preliminary Opinion of the European Data Protection Supervisor on Privacy and Competitiveness in the Age of Big Data*. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

European Data Protection Supervisor. (2019a). *Connected Cars* (TechDispatch). Publications Office of the European Union. https://doi.org/10.2804/70098

European Data Protection Supervisor. (2019b). *Smart Speakers and Virtual Assistants* (TechDispatch). Publications Office of the European Union. https://doi.org/10.2804/755512

European Data Protection Supervisor. (2020). *A Preliminary Opinion on Data Protection and Scientific Research*. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

Fashion ID, C-40/17, EU:C:2019:629 (Court of Justice of the European Union 29 July 2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CA0040&qid=1590355470801&from=EN

Froomkin, M. (2015). Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *University of Illinois Law Review*, *2015*(5), 1713–1790. https://doi.org/10.2139/ssrn.2400736

Garcia, D. (2017). Leaking Privacy and Shadow Profiles in Online Social Networks. *Science Advances*, *3*(8). https://doi.org/10.1126/sciadv.1701172

Garcia-Murillo, M., & MacInnes, I. (2018). Così Fan Tutte: A Better Approach than the Right to Be Forgotten. *Telecommunications Policy*, *42*(3), 227–40. https://doi.org/10.1016/j.telpol.2017.12.003

Gnesi, S., Matteucci, I., Moiso, C., Mori, P., Petrocchi, M., & Vescovi, M. (2014). My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data. In B. Preneel & D. Ikonomou (Eds.), *Privacy Technologies and Policy* (Vol. 8450, pp. 154–171). Springer International Publishing. https://doi.org/10.1007/978-3-319-06749-0_11

Google Spain and Google, EU:C:2014:317 (Court of Justice of the European Union 13 May 2014). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&qid=1590355288547&from=EN

Hallinan, D., & Hert, P. (2017). Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law. In Linnet Taylor, L. Floridi, & B. Sloot (Eds.), *Group Privacy* (pp. 175–196). Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_10

Hann, I.-H., Hui, K.-L., Lee, T. S., & Png, I. (2002). Online Information Privacy: Measuring the Cost-Benefit Trade-Off. *Proceedings of the International Conference on Information Systems (ICIS*. https://aisel.aisnet.org/icis2002/1

Heath, J. (2007). An Adversarial Ethic for Business: Or When Sun-Tzu Met the Stakeholder. *Journal of Business Ethics*, *72*(4), 359–374. https://doi.org/10.1007/s10551-006-9175-5

Helberger, N., & Hoboken, J. (2010). Little Brother Is Tagging You—Legal and Policy Implications of Amateur Data Controllers. *Computer Law International*, *11*(4), 101–109. https://hdl.handle.net/11245/1.337383

Hirsch, D. (2006). Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law. *Georgia Law Review*, *41*(1), 1–63. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021623

Hirsch, D. (2014). The Glass House Effect: Big Data, the New Oil, and the Power of Analogy. *Maine Law Review*, *66*(2), 373–395. https://digitalcommons.mainelaw.maine.edu/mlr/vol66/iss2/3

Hirsch, D., & King, J. H. (2016). Big Data Sustainability: An Environmental Management Systems Analogy. *Washington and Lee Law Review Online*, *72*(3), 406–419. https://scholarlycommons.law.wlu.edu/wlulr-online/vol72/iss3/4

Holloway, D. (2019). Surveillance capitalism and children's data: The Internet of toys and things for children. *Media International Australia*, *170*(1), 27–36. https://doi.org/10.1177/1329878X19828205

Hull, G. (2015). Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data. *Ethics and Information Technology*, *17*(2), 89–101. https://doi.org/10.1007/s10676-015-9363-z

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual Gaps: Privacy Issues on Facebook. *Ethics and Information Technology*, *13*(4), 289–302. https://doi.org/10.1007/s10676-010-9224-8

Humbert, M., Ayday, E., Hubaux, J.-P., & Telenti, A. (2015). On Non-Cooperative Genomic Privacy. In R. Böhme & T. Okamoto (Eds.), *Financial Cryptography and Data Security* (pp. 407–426). Springer. https://doi.org/10.1007/978-3-662-47854-7_24

Humbert, M., Trubert, B., & Huguenin, K. (2020). A Survey on Interdependent Privacy. *ACM Computing Surveys*, *52*(6). https://doi.org/10.1145/3360498

Inc, F. (2018). *Facebook Post-Hearing Responses to Commerce Committee: "Facebook, Social Media Privacy, and the Use and Abuse of Data*. https://www.judiciary.senate.gov/imo/media/doc/Zuckerberg%20Responses%20to%20Commerce%20Committee%20QFRs1.pdf

Information Commissioner's Office. (2017). *In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information* [Report]. Information Commissioner's Office. https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Introna, L. D. (1997). Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy*, *28*(3), 259–75. https://doi.org/10.1111/1467-9973.00055

Jernigan, C., & Mistree, B. F. T. (2009). Gaydar: Facebook Friendships Expose Sexual Orientation. *First Monday*, *14*(10). https://firstmonday.org/article/view/2611/2302

Jia, H., & Xu, H. (2016). Measuring Individuals' Concerns over Collective Privacy on Social Networking Sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1). https://doi.org/10.5817/CP2016-1-4

Kamleitner, B., & Mitchell, V. (2019). Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements. *Journal of Public Policy & Marketing*, *38*(4), 433–450. https://doi.org/10.1177/0743915619858924

Kitchin, R. (2014a). *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. SAGE Publications.

Kitchin, R. (2014b). The Real-Time City? Big Data and Smart Urbanism. *GeoJournal*, *79*(1), 1–14. https://doi.org/10.1007/s10708-013-9516-8

Kupfer, J. (1987). Privacy, Autonomy, and Self-Concept. *American Philosophical Quarterly*, *24*(1), 81–89.

Lampinen, A. (2015). Networked Privacy Beyond the Individual: Four Perspectives to "Sharing". *Aarhus Series on Human Centered Computing*, *1*(1). https://doi.org/10.7146/aahcc.v1i1.21300

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011). We're in It Together: Interpersonal Management of Disclosure in Social Network Services. *Proceedings of the 29th International Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/1978942.1979420

Laudon, K. C. (n.d.). Markets and Privacy (1996. *Communications of the ACM*, *39*(9), 92–104. https://doi.org/10.1145/234215.234476

Le Borgne-Bachschmidt, F., Girieud, S., Leiba, M., Munck, S., Limonard, S., Poel, M., Kool, L., Helberger, N., Guibault, L., Janssen, E., Eijk, N., Angelopoulos, C., Hoboken, J., & Swart, E. (2008). *User-Created-Content: Supporting a participative Information Society*. https://www.ivir.nl/publicaties/download/User_created_content.pdf

Levy, S. (2020). *Facebook: The inside Story*. Dutton.

Lindqvist, C-101/01, EU:C:2003:596 (Court of Justice of the European Union 6 November 2003). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

MacCarthy, M. (2011). New Directions in Privacy: Disclosure, Unfairness and Externalies. *I/S: A Journal of Law and Policy for the Information Society*, *6*(3), 425–512. https://kb.osu.edu/handle/1811/72971

Mahieu, R., Hoboken, J., & Asghari, H. (2019). Responsibility for Data Protection in a Networked World: On the Question of the Controller, 'Effective and Complete Protection' and Its Application to Data Access Rights in Europe. *JIPITEC*, *10*(1). https://nbn-resolving.org/urn:nbn:de:0009-29-48796

Mantelero, A. (2014). The Future of Consumer Data Protection in the EU: Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics. *Computer Law & Security Review*, *30*(6), 643–660. https://doi.org/10.1016/j.clsr.2014.09.004

Mantelero, A. (2016). Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. *Computer Law & Security Review*, *32*(2), 238–55. https://doi.org/10.1016/j.clsr.2016.01.014

Mantelero, A. (2017). Towards a Big Data Regulation Based on Social and Ethical Values. The Guidelines of the Council of Europe. *Revista de Bioética y Derecho*, *41*, 67–84. http://hdl.handle.net/1

1583/2687425

Marwick, A. E., & boyd, d. (2014). Networked Privacy: How Teenagers Negotiate Context in Social Media. *New Media & Society*, *16*(7), 1051–67. https://doi.org/10.1177/1461444814543995

May, T. (2018). Sociogenetic Risks—Ancestry DNA Testing, Third-Party Identity, and Protection of Privacy. *New England Journal of Medicine*, *379*(5), 410–12. https://doi.org/10.1056/NEJMp1805870

McDaniel, P., & McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy Magazine*, *7*(3), 75–77. https://doi.org/10.1109/MSP.2009.76

Moore, A. D. (2007). Toward Informational Privacy Rights. *San Diego Law Review*, *44*(4), 809–846. https://digital.sandiego.edu/sdlr/vol44/iss4/8/

Nehf, J. P. (2003). Recognizing the Societal Value in Information Privacy. *Washington Law Review*, *78*(1), 1–92. https://digitalcommons.law.uw.edu/wlr/vol78/iss1/2

Nissenbaum, H. F. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(119), 101–139. https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

Olejnik, L., Konkolewska, A., & Castelluccia, C. (2014). I'm 2.8% Neanderthal—The beginning of genetic exhibitionism? *PETS Workshop on Genome Privacy. 14th Privacy Enhancing Technologies Symposium (PETS 2014)*. https://hal.inria.fr/hal-01087696

Organisation Economic Co-operation. (2013). Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. In *OECD Privacy Guidelines 2013* (pp. 19–37). Organisation for Economic Co-operation and Development. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Organisation Economic Co-operation and Development. (2011). *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines* [176]. OECD Publishing. http://dx.doi.org/10.1787/5kgf09z90c31-en

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642–660. https://doi.org/10.1057/s41303-017-0056-z

Privacy International. (2019). *Betrayed by an App She Had Never Heard of—How TrueCaller Is Endangering Journalists*[Case Study]. Privacy International. https://www.privacyinternational.org/node/2997

Pu, Y., & Grossklags, J. (2017). Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter? *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. https://www.usenix.org/system/files/conference/soups2017/soups2017-pu.pdf

Purtova, N. (2018). The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Rhoen, M. (2016). Beyond Consent: Improving Data Protection through Consumer Protection Law. *Internet Policy Review*, *5*(1). https://doi.org/10.14763/2016.1.404

Roessler, B., & Mokrosinska, D. (2013). Privacy and Social Interaction. *Philosophy & Social Criticism*, *39*(8), 771–91. https://doi.org/10.1177/0191453713494968

Ryan, J., & Toner, A. (2020). *Europe's governments are failing the GDPR: Brave's 2020 report on the enforcement capacity of data protection authorities* (Brave Insights) [Report]. Brave. https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf

Ryneš, C-212/13, EU:C:2014:2428 (Court of Justice of the European Union 11 December 2014). https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:62013CA0212&qid=1590355384101&rid=3

Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online Privacy as a Collective Phenomenon. *Proceedings of the Second ACM Conference on Online Social Networks (COSN '14)*, 95–106. https://doi.org/10.1145/2660460.2660470

Solove, D. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*, 1888 – 1903. https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.2307/3481326

Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press. https://doi.org/10.24908/ss.v6i3.3300

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Squicciarini, A. C., Shehab, M., & Paci, F. (2009). Collective privacy management in social networks. *Proceedings of the 18th International Conference on World Wide Web - WWW*, 521–531. https://doi.org/10.1145/1526709.1526780

Strahilevitz, L. J. (2010). Collective Privacy. In S. Levmore & M. C. Nussbaum (Eds.), *The Offensive Internet: Speech, Privacy and Reputation* (pp. 217–236). Harvard University Press. https://doi.org/10.2307/j.ctvjf9zc8

Symeonidis, I., Shirazi, F., Biczók, G., Pérez-Solà, C., & Preneel, B. (2016). Collateral Damage of Facebook Apps: Friends, Providers, and Privacy Interdependence. In J.-H. Hoepman & S. Katzenbeisser (Eds.), *ICT Systems Security and Privacy Protection* (Vol. 471, pp. 194–208). Springer International Publishing. https://doi.org/10.1007/978-3-319-33630-5_14

Taylor, L., Floridi, L., & Sloot, B. (Eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8

Thomas, K., Grier, C., & Nicol, D. M. (2010). unFriendly: Multi-party Privacy Risks in Social Networks. In M. J. Atallah & N. J. Hopper (Eds.), *Privacy Enhancing Technologies* (Vol. 6205, pp. 236–252). Springer. https://doi.org/10.1007/978-3-642-14527-8_14

Tietenberg, T. H., & Lewis, L. Y. (2018). *Environmental and natural resource economics* (11th edition, international student). Routledge.

Vallet, F. (2019, May 13). Les droits de la voix (1/2): Quelle écoute pour nos systèmes ? [Blog post]. *Laboratoire d'Innovation Numérique de La CNIL (LINC)*. https://linc.cnil.fr/fr/les-droits-de-la-voix-12-quelle-ecoute-pour-nos-systemes

Van Alsenoy, B. (2015). *The Evolving Role of the Individual under EU Data Protection Law* (Working Paper No. 23/2015). KU Leuven Centre for IT & IP Law (CiTiP). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641680

Van Alsenoy, B., Ballet, B., Kuczerawy, A., & Dumortier, J. (2009). Social Networks and Web 2.0: Are Users Also Bound by Data Protection Regulations? *Identity in the Information Society*, *2*, 65–79. http

s://doi.org/10.1007/s12394-009-0017-3

Van Alsenoy, B., Kosta, E., & Dumortier, J. (2013). Privacy Notices versus Informational Self-Determination: Minding the Gap. *International Review of Law, Computers & Technology*, *28*(2), 185–203. https://doi.org/10.1080/13600869.2013.812594

van Dijk, N., Gellert, R., & Rommetveit, K. (2016). A Risk to a Right? Beyond Data Protection Risk Assessments. *Computer Law & Security Review*, *32*(2), 286–306. https://doi.org/10.1016/j.clsr.2015.12.017

Veale, M., Binns, R., & Ausloos, J. (2018). When Data Protection by Design and Data Subject Rights Clash. *International Data Privacy Law*, *8*(2), 105–23. https://doi.org/10.1093/idpl/ipy002

Vedder, A. H. (1997). Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations. In G. Moore (Ed.), *Business Ethics: Principles and Practice*. Business Education Publishers. https://doi.org/10.1177/1468018105053677

Venkatadri, G., Lucherini, E., Sapiezynski, P., & Mislove, A. (2019). Investigating Sources of PII Used in Facebook's Targeted Advertising. *Proceedings on Privacy Enhancing Technologies*, *1*, 227–44. https://doi.org/10.2478/popets-2019-0013

Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2*, 494 – 620. https://doi.org/10.7916/cblr.v2019i2.3424

Weinreb, L. L. (2000). The Right to Privacy. *Social Philosophy and Policy*, *17*(2), 25–44. https://doi.org/10.1017/S0265052500002090

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum Press.

Whitley, E. A. (2009). Informational Privacy, Consent and the "Control" of Personal Data. *Information Security Technical Report*, *14*(3), 154–59. https://doi.org/10.1016/j.istr.2009.10.001

Whitman, J. (2003). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*, 1151–1222. https://doi.org/10.2307/4135723

Wirtschaftsakademie, C-210/16, EU:C:2018:388 (Court of Justice of the European Union 5 June 2018). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016CJ0210&qid=1590355426224&from=EN

Wong, R. (2009). Social Networking: A Conceptual Analysis of a Data Controller. *Communications Law*, *14*(5). http://irep.ntu.ac.uk/id/eprint/18914/1/200497_6128%20Wong%20Publisher.pdf

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75 – 89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

centre internet et societe

R&I IN3 Internet interdisciplinary Institute

Universitat Oberta de Catalunya