Technology in Society 63 (2020) 101422

Contents lists available at ScienceDirect

Technology in Society

journal homepage: http://www.elsevier.com/locate/techsoc

Privacy as an aggregate public good

Henrik Skaug Sætra

Østfold University College, Remmen, N-1757, Halden, Norway

ARTICLE INFO

Keywords:
Privacy
Public good
Externalities
Liberalism
Surveillance
Regulation

ABSTRACT

Privacy relates to individuals and their ability to keep certain aspects of themselves away from other individuals and organisations. This leads both proponents and opponents of liberalism to argue that liberalism involves allowing individuals to determine for themselves the level of privacy they desire. If they are given adequate information and the ability to choose, the results are argued to be legitimate, even if individuals choose to bargain away all or most of their privacy in return for convenience, economic benefits, etc. However, the individualistic approach to privacy is insufficient, due to a set of externalities and information leakages involved in privacy issues. A crucial aspect of privacy is that it is an *aggregate public good,* and recognising this lets us see why government intervention is both beneficial and necessary for securing the provision of optimal levels of privacy. This conception of privacy enables us to treat it as a good that is underprovided due to market failure. The article shows how liberals can justify government interference for the protection of privacy by relying on the avoidance of harm, and not on paternalism or other arguments not easily reconcilable with liberalism.

1. Introduction

Privacy relates to individuals and their ability to keep certain aspects of themselves away from other individuals. As such, it seemingly makes sense for a liberal to argue that individuals should be allowed to determine for themselves the level of privacy they desire. If they are given adequate information and the ability to choose, the results are argued to be legitimate, even if individuals choose to bargain away all or most of their privacy in return for convenience, economic benefits, etc.

However, the individualistic approach to privacy is insufficient, due to a set of externalities and information leakages involved in privacy issues. One person's self-disclosure will have consequences for other people, and thus the individual calculus involved in making decisions on privacy leads to suboptimal outcomes for society. Furthermore, it is impossible for *me* to be fully unknown in a world where everyone *else* is fully known. In the terminology of economics, the public *bad* of zero privacy is non-excludable. If the public bad is provided, it is impossible for me avoid the harm that follows from it.

A crucial aspect of privacy is that it is an *aggregate public good* – a good that depends on the combined and sustained actions of most individuals in order for it to be provided. For liberals, one of the most important reasons for government is the need to solve such public good problems, and it is argued that government intervention is necessary in order to secure the provision of optimal levels of privacy. Liberal theory requires that state intervention be justified, and it is here justified by an appeal to pluralism and non-interference, and not on paternalism or other considerations that can be considered inimical to certain varieties of liberal theory. A liberal argument for government intervention and coercion in order to protect privacy is provided, and it is closer to libertarian liberalism than to the paternalistic liberalism of Allen [1].

The article begins with an examination of the key concepts involved and existing literature on privacy and surveillance. Then a discussion of the *social* nature of privacy follows, along with an analysis of what type of public good privacy is. Lastly, the need for government intervention in order to ensure the provision of optimal levels of privacy is examined, and it is shown that this intervention is not in conflict with liberal theory.

2. Privacy, technology, and the government

Before embarking on the quest to discover the nature of liberal privacy, a basic set of concepts must be established. What is privacy, how does surveillance relate to this, and how do new technologies challenge privacy and change surveillance?

2.1. Privacy

Privacy is a master at evading definition and has historically been used to express many different ideas [2]. As thoroughly detailed by Daniel Solove, privacy is a 'concept in disarray' [3,4]. He examines

E-mail address: Henrik.satra@hiof.no.

https://doi.org/10.1016/j.techsoc.2020.101422
Received 11 September 2020; Received in revised form 22 September 2020; Accepted 22 September 2020
Available online 23 September 2020

various conceptions of privacy, such as *the right to be let alone, limited access to the self, secrecy, control over personal information, personhood,* and *intimacy* [5]. Anita L. Allen [1], on the other hand, suggests that privacy today refers to a 'predictable range of conditions and liberties', both for laypersons and experts. Instead of seeing the concept as in disarray, she argues that there are different forms of privacy, all valid, that are part of the 'umbrella concept' of privacy [1,3].

As the purpose of this article is to examine a particular aspect of privacy related to the problems associated with treating it as an individual affair, emphasis is placed on *limited access* and *control* aspects of privacy. Limited access is similar to the conception of privacy as *boundaries*, protecting us from *intrusions* [6]. Scanlon [6] responds to Thomson [7], and they both agree that privacy is not a right in itself, but a derivative right.[1] Thomson [7] here emphasises the right over 'own persons' and 'our property'. Gavison [9] was an early proponent of privacy as restricted and limited access and, for example, *solitude* as a form of privacy [1]. Control aspects of privacy relate to Westin's [2] classical definition of privacy: 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'. Brey [10] refers to this as informational privacy, as it relates to the degree of control a person has over who has access to their personal information.

Limited access to the self and control of personal information involve two claims: the right to not be observed *and* the right to control the flow of information when someone *is* observed. Both are of great importance, but there is also a tension between the two. Someone might have a desire to act in public and still control who observes or at the very least who registers and stores information about their actions. People often expect *privacy* even in *public*, for example when they engage in conversation in a restaurant [11,12]. While Tavani and Moor [8] argue in favour of a clear distinction between *privacy* as 'protection from intrusion and data gathering' and *control* of information, both aspects are relevant in the following discussion of the nature of privacy.

If we only focus on an individual's control of information, full privacy might be achieved in a state of complete surveillance, if this is taken to mean that I am simply *observed* at all times. As such, Tavani and Moor [8] are right when they criticise conceptions of privacy that *only* entail the facets of control. According to such an approach, merely being observed is not necessarily a problem as long as the information is not communicated without consent. Solove [11] argues that observation without *human judgement* is not an invasion of privacy. Only then, he states, does *surveillance* lead to the negative effects of 'conformity, inhibition, and self-censorship' [11].

If we focus on a right not to be *observed*, the demands of privacy are strong. Sætra [13] argues that *who* (or what) is in charge of the surveillance is of little consequences. He constructs a thought experiment with the hypothetical *Observer* with no means of judging, interfering, or communicating what he observes, and argues that this form of observation would still influence the actions of many. The mechanisms leading to the conformity, inhibition, and self-censorship mentioned by Solove results from mechanisms in the *observed*, not in the observer [13]. Observation in itself can thus be construed as *interference.* This implies that those concerned with privacy as an element of liberty must focus both on the act of observation and the control of the information that could be the result of observation [13].

In the context of this article, control over *who* observes and control of *information derived from such observation* are considered necessary for *full* privacy. This implies that privacy is not a Boolean variable with *true* or *false* as its possible states. Privacy is by *degree*, and thus not a categorical right in the sense that it is something you either do or do not have. We can, however, have a right to *some* privacy and a right to control parts of our privacy space. Having privacy involves some withdrawal from the public, and Westin [2] states that it is *voluntary* and *temporary* and involves both physical and psychological states.

2.2. Surveillance and technology

From privacy, the focus is now shifted to *surveillance* and modern technologies. Surveillance concerns *observation* considered relevant to *privacy*, and new technologies both for gathering and analysing data must be understood in order to show why the individual approach to privacy protection is insufficient. New technologies exacerbate the mechanisms that make privacy a public good, and understanding these developments is crucial for understanding why government intervention in the provision of privacy is becoming increasingly important [1,14,15]. Rachels [16] notes that 'new social institutions and practices' can change human relationships in ways directly related to the *control* of privacy, and it is here argued that new technologies have profound implications for both our social institutions and practices.

2.2.1. Little brothers in a surveillant assemblage

Our age is somewhat special in that it is not primarily the *government* we fear when we discuss surveillance. Unlike in Orwell's [17] fictional Oceania, there is not one singular actor that surveils and binds us all. There is no *one* big brother, but many little (and some quite big) brothers – a variety of both private and public actors who jointly defy the metaphor of *Big Brother* [11,18]. Governments still gather information, and is also 'an important secondary beneficiary' of the information gathered by others [11,19].

However, unless one considers the way in which these little brothers act in concert, almost in unison, the overall effects of modern surveillance remain obscure [11,13]. Zuboff [15,20] uses the term big *other* to describe the beast of surveillance, and by this she refers to 'a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience […]'.

The way many different actors gather information in isolation, but then somehow simultaneously act in concert, is referred to as the *surveillant assemblage* [21]. Haggerty and Ericson [21] criticise the use of the metaphors of *Big Brother* and the *panopticon* of Bentham, and then Foucault, for understanding modern privacy issues. The importance of metaphor, and the errors resulting from relying on Orwell's metaphor, is also the subject of detailed examination by Solove [11]. These authors argue that the decentralised and dispersed nature of modern surveillance matters, and Haggerty and Ericson [21] use the term *surveillant assemblage* for understanding how a multiplicity of different actors that, without coordination or common plans and intentions, still operate as *functional* entities. The unity of the surveillant assemblage is not formal or institutionalised, but for analytical purposes it is treated as a *functionally* unitary threat to privacy – a threat involving privacy's gradual erosion [22,23].

Even if surveillant institutions do not operate in an institutionalised and collective manner, and even if there is no one *Big Brother,* many of us still have the feeling of being under someone's surveillance. We can ask, with Delacroix and Lawrence [24]: 'How do we control for this death by a thousand cuts?' Gaining control is exceedingly difficult, as each little cut is seemingly innocuous, and we usually do not even know who is responsible for cutting us.

2.2.2. A taxonomy of surveillance

Before moving on to the role of government regulation some key distinctions between different *types* of surveillance will be presented. While the purpose of this paper is not to create a typology of surveillance, establishing an understanding of different perspectives on surveillance helps us see various facets of privacy. Privacy as a concept is here linked to protection from intrusions *and* control of information, and *surveillance* is thus a highly relevant phenomenon.

Lyon [25] defines surveillance as 'focused, systematic and routine'

[1] I do not problematise the notion of privacy as a *right*, or *normative privacy* [8]. Whenever I refer to privacy as a right, it results from a) referring to others who see privacy as a right or b) pragmatically referring to actual legal rights.

attention with a *purpose* [19,26,27]. Lyon [28] also defines it as the 'the operations and experiences of gathering and analysing personal data for influence, entitlement and management'.

These two definitions describe forms of surveillance that are *purposeful*, which is sometimes referred to as *strategic* surveillance [29]. The purpose could be anything from preventing crime to gaining more in-depth knowledge of one's customers. A broader approach is seen in Macnish's [26] definition of surveillance as 'sustained monitoring of a person or people'. Such a definition allows for the inclusion of everyday monitoring with unclear intent and focus. A broad definition of surveillance is beneficial, if one simultaneously introduces a way to differentiate the types of surveillance discussed.

Surveillance can also be *direct* or *indirect* [2]. Direct surveillance involves the focus on particular persons for particular reasons, while indirect surveillance involves gathering specific information in which the target and final purpose of the surveillance are sometimes determined later on. Indirect surveillance is vividly described by Solove [11]. He describes a modern form of surveillance that results in the creation of *digital dossiers* – files with personal data – that are gathered, shared, and combined in various ways by a multitude of actors. There is often no clear reason why a *particular* individual is observed, and the surveillance at times results from the general idea that personal information is valuable. Such surveillance leads to a system akin to Kafka's *The Trial*, Solove [11] argues. Such a system is only purposeful in a *general* and non-specific sense, in that it is a manifestation of the idea that data is beneficial and valuable. It is indirect in that we are *all* targets of such surveillance, merely by being potential customers, voters, patients, criminals, etc.

Another typology is found in Sætra [13]. Here, surveillance is divided into *passive observation, active observation*, and *surveillance proper*. In the first, there is no intent to use the information to influence or manage us. Passive observation might occur if an electricity meter in our home is *only* used to determine the size of the bill we receive. Active observation involves gathering information in order to *retroactively* use it to influence or manage us through, for example, sanctions. Video surveillance at a store, used as evidence of me breaking in, is active surveillance. The final type is labelled *surveillance proper* as it most clearly manifests the form of surveillance referred to in popular usage of the term, particularly related to government surveillance. It involves *proactive* use of surveillance in order to uncover information and change the actions of individuals. If the government uncovers information and apprehends potential terrorists *before* a crime has been committed, this is labelled surveillance proper.

It is accepted as a fact that technologies have led to changes in the pervasiveness of surveillance, and the technical details of the technologies used to connect and analyse Big Data is beyond the scope of the article. Technological advances have led to the growth of the surveillant assemblage discussed earlier, and the data gathered through this surveillance is increasingly used to create personality profiles which are used to influence us in a variety of ways [1,11,15,21,30–32].

These developments imply that the importance of understanding and possibly regulating the market for privacy is becoming increasingly important. One reason for this is that targets of surveillance will often not be able to accurately identify or uncover *whether* they are surveilled by use of new technologies and the use of the various sources of data in existence. Neither will they necessarily be able to perceive which form of surveillance they are under. They might not notice *that* they are observed, and if they do, they will often not know if or how the information is used. Cohen [19] states that '[n]etworked information enable[s] surveillant attention to become continuous, pervasively distributed, and persistent', and Nissenbaum [33] writes that new information technologies have led to practices of surveillance that are both pervasive and 'among the least understood and controversial challenges to privacy'. Such a system of surveillance might be highly effective, while remaining unperceived and poorly understood by the targets of surveillance. If so, and if the inherent complexities in such a system make it difficult to create *informed* consent by giving *notice*, an individual market-based solution might be insufficient.

We have now arrived at a concept of privacy as protection against interference and control over personal information, and an understanding of surveillance in modern society as both indirect and often non-strategic. These forms of surveillance, which might be *passive* or *active* observation and not necessarily surveillance proper, are all problematic when we examine privacy as protection against interference. It is also important to understand how technology has changed surveillance, as the indirect and unfocused nature of modern surveillance has implications for the provision of privacy as a *public good*, as discussed in section 3.

2.3. Individualist vs. collectivist regulation

Before examining how policy makers should regard privacy, an approach touched upon in the introduction, namely that of *notice* and *choice*, must be briefly explained. Particularly in the US, this regime has been prevalent, and its modern privacy law is based on Westin's conception of privacy as the right to control personal information [34]. This *control-based* approach has led to the idea of *notice* and *choice* as the basis of privacy regulation. As Allen [1] and Bennett [35] note, the US is different from, for example, Europe in terms of the approach to privacy as an individual good. Writers focused on the US, Bennett [35] argues, fail to fully recognise how other regions have taken a different path, and gone for 'a more comprehensive statutory approach to information privacy'.

While the European approach has placed more emphasis on empowering individuals, Tisné [36] argues that the *collective* aspect of privacy 'continues to be ignored' even there. This, he states, leads to the need for legal privacy standards that take into account the harm caused by collective data analysis. Modern surveillance is *indirect* and *non-strategic*. This explains why an individual struggles, as it is often difficult for individuals to prove harm to their individual rights [36].

The individualist approach is problematic for reasons already discussed. If people are informed about surveillance and are subsequently allowed to choose what information they share, they can be argued to have *control*. This approach is not sufficient, due to factors such as *externalities*, as discussed in more detail in section 3, and due to limited knowledge of the consequences involved.

The current purpose is to understand the nature of privacy, and the specific details related to the judicial, regulatory, or legislative aspects of privacy is thus beyond the scope of the article. However, one proposed solution to the problem of privacy protection must be briefly discussed, as it is superficially related to, but in reality very different from, the propositions developed in this article. It is based on what Tisné [36] labels *collective rights*. Taylor et al. [37] write about *group rights*, and argue that while privacy *used to* be about individuals and small groups, it is now more about larger groups. This, they argue, makes it necessary to explore the extent to which it might benefit regulators to see a group as *it* instead of *them* – of not reducing social units to their constituent individuals [37]. It could, on the other hand, be argued that the surveillance discussed in this article makes surveillance *more* individualised than ever before, as surveillors constantly improves their prospects of knowing *you* and not just your *type*. Knowing a person's *type* is old-style surveillance, developed in part by marketing agencies and others with an interest in shaping and controlling behaviour [11].

While Taylor et al. [37] and the contributors of the edited volume highlight important collective aspects of privacy, a different route towards seeking an improved understanding of the problem at hand is here taken. It is a liberal route aimed at maintaining that individual rights are all there is, and that the government should not deal with us on the basis of our gender, religion, occupation, etc. While *existing* individual-based approaches to privacy have failed, that is because we have failed to see the nature of privacy as a *public good*, prone to *market failure*.

3. Common goods, public interest, and public goods

It is time to consider what type of public good privacy really is. Privacy, Richards and Hartzog [38] argue, 'is only occasionally conceptualised as a group or even a social project', which implies that the individualist approach to the concept is still dominant. This is the case particularly in the US, as we have seen in the discussion of the notice and choice regime as opposed to, for example, a more comprehensive European approach. Even if Westin [2] is at times portrayed as the originator of the individualised approach to privacy, he states in Westin [39] that privacy is 'a social good in democratic societies, requiring continuous support from the enlightened public'. Others have also emphasised the non-individual – or *social* – aspects of privacy, but there is much disagreement as to what this entails and what type of good privacy really is – or should be considered to be.

The social nature of privacy can be understood in a number of ways. First, there is the sense that privacy is something that is appreciated by a *group*. It is not only beneficial for individuals, but also for the groups individuals belong to. While related to the idea of *group privacy* discussed in Taylor et al. [37], this aspect of privacy is referred to by the term *common* good, which is discussed in more detail in section 3.1.

A quite different form of analysing privacy is to use the term *public good* from economic literature. This approach lets us emphasise and understand how it is possible to consider privacy an *individual* good in the sense that it relates to an individual's control and protection from intrusion, while still showing how market dynamics lead to what we label suboptimal outcomes. This relates to network effects of privacy, which are for now illustrated by the adage: *tell me who your friends are, and I will tell you who you are* [40].

In the following, a set of examples of how the terms *common* and *public* goods are used in the literature on privacy is presented. Firstly, it is shown how authors use the terms in ways referring to *common* goods, before the focus is shifted to what economists call *public* goods. After the terminology and concept of a public good from economic theory is established, different *types* of public goods are presented, and it is shown that privacy is the type referred to as an *aggregate* public good [41].

3.1. Privacy as a common good and the public interest

The *social dimensions* of privacy are emphasised in a recent edited volume by Roessler and Mokrosinska [42]. They argue that the *individual* interests and rights are at the core of 'contemporary privacy scholarship', and that this perspective is ill-suited to account for concerns raised by new technologies [42]. Regan [43–45] is one of the most prominent voices arguing for the social nature of privacy. In Regan [43] she notes how while privacy *seems* to become more and more important, it is increasingly often heralded as *dead* or *dying*. One reason for this paradox, she argues, is a 'failure to conceptualize privacy in a way that sustains public interest and support' [43]. She explains that being overly focused on individual rights erodes privacy, as it places each isolated individual's interests in opposition to social interests and values. While societal values, such as fraud detection, effective policing, etc., are easily understood and considered to be good, privacy is seen as an individual interest that is in opposition to these [46]. Solove [4] similarly argues that privacy is an abstract term that is more difficult to explain and garner support for than, for example, innovation and security.

However, in modern societies, privacy concerns 'cross the boundary between public and private', as it relates to individual, group, and societal relations and affects core social mechanisms such as 'friendship, love, and trust', which have great implications for society as a whole [43]. Here, Regan [43] distinguishes between three ways of conceptualizing the social nature of privacy. First, it can be a *common value*, in that we all value privacy in some sense. Second, it is a *public value*, as the value is not limited to individuals, but is applicable to our societies and political systems in general. Third, she mentions the notion of *collective value*, which is a basis 'for the social importance of privacy [as] derived from the theoretical literature in economics'. This is the concept referred to as a *public good* in this article, and it relates to how 'technology and market forces are making it hard for any one person to have privacy without all persons having a similar *minimum* level of privacy' [43].

Before examining the third type of value in more detail, a couple examples of how the three different terms are often conflated or confused in discussions of privacy is in order. Lane et al. [47], for example, discuss privacy and the 'public good', but they here refer to *common* goods such as improved public services, etc., which are *not* public goods in the sense used in this article and in economic theory. Similarly, Pullman, et al. [46] discuss how certain 'public goods' such as biobanks for research are related to the private good of privacy. The public, they say, 'view biobanks as a public good and as such are not as concerned about their individual privacy' as they are with the public benefits.

3.2. Privacy as a public good

The preceding examples relate to privacy as a social good in the sense that *they are good things for society, that most people appreciate,* what Regan [43] calls *public* and *common* values. This version of a 'public good' is not what is referred to in this article. When the term *common* good is used, it is often to illustrate the difference between *private interests* and the *public good*; the nuisance that individuals experience is, for example, outweighed by the *public* good. Analysing privacy as a common or public value involves normative theory, and in the following we turn to *economic theory* and privacy as a public good, or what Regan [43] calls collective value. We might, however, note that seeing privacy as an economic public good does not *necessarily* imply advocacy for more individual privacy and stronger regulation. Daughety and Reinganum [48] analyse privacy as a public good, but they mainly focus on how too *much* privacy may lead to what in economics are known as public *bads*, in the sense that useful information is concealed and becomes unavailable to other actors.

Public goods are defined as *non-excludable* and *non-rival*. Once the good is provided, no one can be prevented from enjoying the good, and neither will one actor's use of the good impact other potential users' ability to enjoy the good [41]. Commonly used examples of such goods are lighthouses, a national defence, and clean air. While *theoretical* non-excludability might be of interest, Papacharissi [49] shows why *actual* access to a good also matters. With a notice-and-choice regime, all could be said to have a hypothetical access to privacy. However, individual management of privacy requires 'a level of computer literacy that is inaccessible to most' [49]. Nissenbaum [50] similarly notes that the 'fundamental flaw' in the notice and choice regime is the assumption that people 'can understand all facts relevant to true choice at the moment of pair-wise contracting between individuals and data gatherers'. One reason for this is that private information says *more* than we imagine 'when aggregated with billions of other data points' [51]. Yeung [32] details the nature of Big Data, which according to her leads to a complexity and uncertainty about *future* implications of granting access to personal data in which a notice-and-choice approach '*cannot* be relied upon to protect the right to informational privacy'. In short, the *surveillant assemblage* is a wily beast, and assuming that everyone will be able to gather sufficient knowledge to tame it on an individual basis seems overly optimistic.

Such considerations, Papacharissi [49] argues, makes privacy today more akin to a *luxury* good – a good accessible only to a privileged group. This relates the discussion of privacy as a public good to the *regulation* of privacy. Ackerman et al. [52] state that privacy 'forms a *co-design* space between the social, the technical, and the regulatory' and that technological innovation must aim at producing public goods. The cost of keeping track of the various impacts everyday life has on our privacy is too high. Such transaction costs imply that individual market solutions become inefficient, and Ackerman et al. [52] 'wish to shift the transactional cost for privacy from each user to the public'. In other words:

privacy as a *public good*.

If privacy is to become a good which is *actually* accessible and useful to all, people's resources and abilities must be taken into account, and the government might be required to intervene in order to prevent market failure. One of the key insights from the theory of public goods is that they will often be underprovided in free markets, as there is little incentive to produce a good that anyone can freely enjoy without paying. This is the problem of *free riding*, which is explained in more detail below.

3.3. Understanding public goods

A key aspect of public goods is that they are prone to what is called *market failure*. When individuals do not bear the full cost of their actions, individually rational actions lead to collectively suboptimal outcomes. I may, for example, have a preference both for clean air and for driving a highly polluting car. I know that driving my polluting car will not deteriorate the air quality to such a degree that the air becomes unclean, so I believe that I can enjoy *both* clean air and my preferred car. It is thus individually rational for me to buy a gas-guzzler. However, if everyone reasons as I do and acts according to this reasoning, we will find ourselves in a collectively suboptimal situation *without* clean air.

This is known as a coordination problem, because individuals need some way to coordinate their actions so that they can jointly achieve a satisfactory balance between their desire to burn gasoline and for clean air. Similarly, individuals in a society must together find a satisfactory balance between privacy and other goods, such as ready access to fully personalised recommendations and entertainment. One particularly famous type of coordination problem is what game theorists refer to as the *prisoners' dilemma*.[2]

But how does clean air and prison time relate to privacy? The tragedy of the commons is an example often used to explain the problems of public goods [54]. When individuals have joint and unrestricted access to common resources, self-interested actors will be inclined to increase their exploitation of the resource, as they alone will get the added benefit, while the costs are divided by all actors. This, in turn, leads to the degradation of the resource. When privacy is seen as a public good, where externalities are important, we get the tragedy of the privacy common. Each individual will be inclined to accept a slight degradation of the common in order to derive an individual increase in other goods. For each individual, this is rational, and if only one individual did so, it would not necessarily degrade the common. The problem, however, is that all actors have the same incentive, and when many act on this incentive, the common is significantly degraded. Choi et al. [55] show how a market-based approach to privacy, with choice and full information, leads to suboptimal outcomes with excessive privacy loss. This, they argue, is due to *information externalities* and *coordination failure* – key characteristics of public good problems. It will first be shown how *relational leakages* and the use of *general personality profiles* create the conditions of a public good.

3.3.1. Relational leakages

Understanding *externalities* is crucial for understanding public goods. Externalities refer to a situation in which *my* actions have consequences for others. One example could be the pollution from a factory. Without any regulation of emissions, the factory owner's budget would not accurately reflect the cost *others* have to pay for his polluting activities, which would lead him to produce and pollute more than he would have done had he been required to take account of these external costs. An important privacy externality is that one individual's disclosed information can be used to infer information about other individuals [55]. Barocas and Levy [56] focus on three *dependencies* that help us understand the types of information leakage and privacy externalities that make privacy a public good: our *social relations* and our *similarities* to and *differences* from others. The first relates to the *relational leakages* discussed here, while the latter two are the topic of the next section. Relational leakages are also referred to as the *network effect* [57].

When some people are careless with their privacy, it has an impact not only on themselves, but also on a wide range of people *associated* with them [1,43,48]. In addition, it has effects for people both *similar* and *different* to them. This is the *ethical aspect of privacy management*, as one person's self-disclosure has an impact on others [58]. MacCarthy [59] critiques the regime of notice-and-choice and emphasises *privacy externalities*. When my disregard for privacy leads to consequences for the privacy of others, this can be due to 'information leakage' [59].

Recognising our social natures, we see that information about *me* will by necessity involve some information about *others*. My relations and my social life are part of *me*, and even seemingly purely private information may be used to deduce information about, for example, my spouse or my friends. Knowledge of me involves knowledge of my relations [51].

Even if one of my friends does not have a profile in social networks, surveillance agents might create 'shadow profiles' for non-members, in order to (a) prepare their entry into the network and (b) better model the full social network, in order to improve their understanding of the actions of all involved [60,61].

3.3.2. General profiles

Another aspect that makes privacy *public* is how the aggregation of various personal information lets the surveillance agents build highly detailed generic profiles. When enough people *like* me willingly provide information about themselves, this information can subsequently be used to better understand and target *me*. This is related to the calls for *group* privacy, as knowledge of a group can be used to effectively target individuals in the group [37].

No one can ever be fully private, so there is always the option of superimposing highly detailed profiles onto individuals about which the surveillers only have information about a limited set of variables. We might be unique, but we are also alike enough for this to be a problem. Fairfield and Engel [51] use the example of deriving the chances of me getting cancer by using information about my brother. Even if we had *no* actual social relations, similarities mean I am potentially hurt by his self-disclosure, for example by having to pay a higher premium on my insurance.

It is, in short, impossible for *me* to be fully unknown in a world where everyone *else* is fully known. In public good terms, the public *bad* of zero privacy is also non-excludable. If the public bad is provided, it is impossible for me avoid the harm that follow from it.

Morozov [58] mentions how my disclosure to an insurance company may subsequently harm other clients, 'many of them less well off'. Insurance is a particularly good example of an industry in which companies have a strong interest to identify those most likely to *need* insurance. If these can be identified and the proper premiums charged in a more targeted manner, the premiums for other clients would fall. This will arguably lead to a situation in which, for example, those most likely to have health problems will pay the highest premiums. If we consider that health problems are also correlated with other socio-economic challenges, we see how the least well off might be made even worse off by decreased levels of privacy.

Furthermore, there is a slippery-slope argument involved in, for example, allowing companies access to our fitness trackers or GPS systems: when enough early adopters do so, the rest of us' will be considered deviants with something to hide' [58]. *Not* providing information could, for example, be seen as a sign of 'guilt' and lead to higher premiums. This would be akin to insurance companies demanding a premium for clients without smoke alarms in their homes, etc. Morozov [58] argues that these considerations make it clear that privacy questions are *not* only about 'pure economic self-interest'. They are *moral* questions [58].

[2] See Kuhn [53] for a detailed analysis of this example.

3.4. Privacy as an aggregate public good

Having established that there are good reasons to examine privacy as a public good, it becomes important to examine *what type* of public good it is. This is an aspect of privacy as a public good that is not sufficiently examined, and a framework for public goods and a classification of privacy as a public good is here proposed. Brunton and Nissenbaum [62] ask: 'Can your obfuscation project be carried out effectively by one person, or does it require collective action?' This is related to what *sort* of public good privacy really is.

Barrett [41] has developed a typology of public goods related to global public goods such as environmental challenges, and privacy can be categorised as an *aggregate good* in Barrett's terms. In the following quote, he explains the core idea of the concept:

> Imagine a group of rowers trying to propel a boat. Their speed depends not on the weakest rower, nor on the strongest, but on the efforts of all the rowers. Some global public goods likewise depend on the total efforts of all countries. Environmental issues are typically of this type. Pollution is determined by aggregate emissions, overfishing by the fishing efforts of all countries [41].

The prime example of an *aggregate* public good is climate change, and this is a better parallel to privacy than one might first assume. There are four reasons, Barrett [41] argues, why the optimal provision of aggregate public goods are hard to achieve. First, the dangers involved are somewhat diffuse and not immediate. Second, the consequences are different for different actors. Some will be harmed by a lack of privacy, while others will *benefit*. With climate change, the worst off are the ones least equipped to combat the problem. The same might be the case for a loss of privacy. Third, protecting privacy will have consequences for our political and economic systems, and we must be prepared to forego certain opportunities for economic growth and innovation. Finally, and centrally, protecting privacy requires the *aggregate* effort of the actors involved. It is an essential feature of this type of public good that it does not require that *all* participate – only that *enough* do.

The other main types of goods in Barrett's [41] framework are *single best effort* and *weakest link* goods. If a good is of the type *single best effort*, one powerful agent may solve the problem singlehandedly, for example the US alone preventing an asteroid from destroying the earth [41]. The weakest link good requires *all* to participate for the good to be provided. The eradication of disease through, for example, vaccination programs, is an example [41]. Privacy is a good of the *aggregate* type, as no single actor can solve it alone but it does not require *all* to take part in its provision. Privacy as a public good is provided to the degree that *most,* or at the very least the most *influential*, actors actively take part in its provision.

Barrett [41] emphasises one problem with aggregate public goods, which might not be as prevalent with regard to privacy as it is with regard to, for example, combatting climate change: the incentives to *free ride*. Since full participation in solving the problem is not required, some could have the incentive to shirk – to not take part in the provision of the good – while still enjoying the benefits. This is particularly relevant because privacy is often *unpopular*, and many will gladly trade it for other goods when given the chance [1].

How does free riding impact the protection of privacy? First, if one individual is careless with their own personal information while others *are* careful, the harm that befalls the careless individual is less than it would have been if all were careless. The general personality profiles would not be as effective, and the incentives to build systems that exploit personal information in the way described by Zuboff [15] might not exist. However, the *benefits* to the free rider that derive from sharing information would *also* be less than they would have been if all shared their information, due to the same systems of producing value from information not being created. Free riding does not seem to be the major problem involved in the provision of privacy as a public good.

Diffuse effects and consequences, combined with limited individual attention and processing, seem to the be two most important factors that explain why we fail to provide the public good of optimal levels of privacy. The *main* factor, however, could be the uneven division of harm and benefit involved. Certain structures of harm and benefit give rise to *rent seeking* behaviour, which is highly relevant to the issue of data protection. Whenever a market is not fully free, a competition for influence over whomever controls a market begins. Competition for favourable regulation, for example, is called seeking *rents* and is often (but not necessarily) associated with corruption, bribery, and outcomes that are not beneficial for society as a whole [41,63]. The ones with the most to gain have a great interest in combatting any regulation of government involvement that will change the current privacy regime. The people harmed, however, are many, and as each bears a relatively small burden of the cost, they will not have the same incentives to mobilise and act. This implies that tougher regulation and other forms of government intervention will be fought by those with much to lose. As Zuboff [15] shows, some have *a lot* to lose, as there is great value in our information.

In short, privacy is an aggregate public good, which is highly susceptible to market failure if privacy concerns are left to individuals and a free market for privacy. This implies that unregulated markets for privacy will not be able to provide collectively optimal levels of the good. When individuals attempt to individually optimise their privacy levels, the result on a collective level will that too little of the public good is provided. This explains the need for coordination and government intervention.

4. Government and the provision of public goods

> Individuals do not always care or recognize that their privacy is important; privacy is so valuable that individuals must sometimes be forced to accept it for the good it does them or others [64].

What are the implications of understanding privacy as an aggregate public good? First of all, a major reason for government intervention is the need to solve coordination problems and prisoner's dilemma-situations [65]. Privacy is such a problem. While some, such as Fairfield and Engel [51], focus on *individual's* choices related to privacy, it is also important to have an eye on the organisations involved in surveillance. The organisations that are involved 'in the collection, use, and disclosure of personal information' become the targets of regulation, as the government aims to create a market for privacy that is conducive to desirable overall levels – or *optimal* levels – of privacy in any given society [34]. As Hirsch [34] notes, stronger regulation should not be seen as a detriment to these organisations. It is in their interests, as well as in the interests of individuals and society in general, that we are able to establish a market in which sustainable privacy interactions between individuals, organisations, and the government are acceptable to those affected.

While most agree that coordination is required to solve the problem of public goods being underproduced, not all agree that it is the *government* that must facilitate cooperation. Fairfield and Engel [51] point to the findings from experimental economics, where it has been shown that groups *can* achieve cooperation through the ability to communicate, punish and sanction shirkers, and *framing*. Thus, they argue, the tragedy of the 'privacy common' can be avoided *without* resorting to government intervention. Such avenues towards voluntary cooperation aimed at producing public goods should, of course, also be pursued. However, the argument here developed suggests that the government is needed in this case. This is mainly due to the diffuse nature of the harm and benefit involved, which means that it is exceedingly difficult to inform and mobilise at a level sufficient to achieve voluntary cooperation. Privacy has value beyond what most individuals are able to foresee and the government has a duty to prevent new technologies from disrupting the provision of this good. Allen [1] argues strongly in favour of

coerced privacy based on paternalistic and dignitarian grounds. The liberal argument for government intervention proposed in this article is quite different, as it is based on the classical liberal values of pluralism and harm avoidance.

4.1. A liberal argument for government intervention

> Until we know how we can produce such a state all we can hope for is to create conditions in which people are prevented from coercing each other. But to prevent people from coercing each other is to coerce them. This means that coercion can only be reduced or made less harmful but not entirely eliminated [66].

Coercion is perceived to the be anti-thesis of liberalism. However, as the quote from F. A. Hayek shows, coercion is an integral part of liberalism, while great care is simultaneously taken to *limit* the amount of legitimate and necessary government coercion [67]. Like John Stuart Mill, Raz, in his version of the harm principle, explains why liberals may 'employ coercion to prevent harm' while refusing to employ it for other services [65,68].

Others have also argued that coercive power should be employed to protect privacy. Devins [69] states that 'some government-sponsored invasions of privacy may be necessary to protect privacy from itself'. This is akin to the Hobbesian and liberal notion that some liberty must be surrendered in order to protect liberty [66,70]. Devins [69] writes in response to Allen [71], who argues that the imposition of regulation of privacy in order to safeguard liberty and autonomy is consistent with liberalism and necessary for the protection of privacy. While Devins [69] agrees that some coercion is necessary, he objects strongly to what he perceives as Allen's belief in the 'possibility of a beneficent government able to overcome its prejudices'.

Allen [1] argues that an 'egalitarian liberal democracy', on 'dignitarian grounds', may use coercion to protect privacy. She considers privacy to be a *foundational* good on par with foundational liberty, and that coercive paternalism is warranted for protecting the harms that follow a lack of both these foundational goods. Foundational goods are 'extremely important human goods … on which access to many other goods rests', and without such goods 'a nation state fails to be good and just' [1]. Griffy-Brown et al. [72] names freedom, democracy, well-being, justice, and sustainability as foundational values for the good society, and Allen [1] then suggests that privacy should also be included in this list. Allen's [1] ideological foundation is 'comprehensive deontic liberalism'. She also states that she identifies with 'libertarian liberalism', while acknowledging that coerced paternalism is generally considered to be somewhat difficult to reconcile with this [1].

The type of liberalism advocated in this paper is more easily reconcilable with libertarianism, and it is based on non-interference and value pluralism [73,74]. According to such a position, individuals have a wide variety of individual values, and these are non-commensurable. This is combined with a fundamental respect for the individual's right to determine their own values and life goals, as long as this does not involve the infliction of harm on others [68]. With such a position, paternalism is not the reason to protect privacy. It is the need to create the conditions in which people can pursue and enjoy a variety of different goods and life styles without undue interference that is centrally important. In order to achieve this, privacy must be protected, and due to the nature of privacy as a public good, such protection requires government interference and a certain restriction of individual liberty.

The reasons people have for valuing privacy are diverse, and while it may be illegitimate to force all to value privacy in a certain way, it can be legitimate to protect privacy so that people can individually enjoy privacy in various ways. One reason to value privacy is that a lack of it can be seen as interference. Being observed influences a person's actions, and general surveillance deprives individuals of freedom of choice as it constitutes a form of forced participation [13]. Furthermore, according to Warren and Brandeis [75], privacy invasions can cause 'mental pain and distress, far greater than could be inflicted by mere bodily injury'. Privacy is also required in order to restrict the power of others to manipulate us and to restrict individuality [31,76]. This relates to the republican liberty of Pettit [77], which allows us to account for the potential for *domination*, and not just direct and actual interference [1].

Allen [1] emphasises privacy's foundational value, with a particular focus on privacy's role for protecting dignity and autonomy. Coerced privacy is for her a form of coerced duty of self-care, and the approach is clearly and admittedly paternalistic. Privacy must be coerced for the good of the specific individuals that are coerced, according to this argument. Privacy cannot be waived, because doing so will harm the one waiving their privacy [1]. While Cohen [19] does not share Allen's faith in government coercion, she does share her view on the value of privacy as conducive to autonomy, individuality, and personal development.

However, a liberal need not resort to paternalism and conceptions of autonomy often associated with what Berlin labelled positive liberty in order to advocate for coerced privacy. Since privacy incursions can be argued to constitute harm, the fact that it is a public good necessitates coercion on the basis of simple harm avoidance. People's liberty to dismiss their own privacy is not reduced in order to protect themselves, but in order to prevent them from inflicting harm on others.

A classical liberal position based on a respect for individual liberty and value pluralism recognises that all are assumed to desire freedom from coercion, and this requires privacy. Some will only desire a minimum level of privacy required to avoid the harms described by Warren and Brandeis [75], but others will legitimately value privacy as a foundational good necessary for their self-development, self-care, dignity, and autonomy [19]. No one can demand that the first group should value privacy in the same way as the latter group, but the first group can be coerced to protect their privacy if this is necessary for preventing the infliction of harm on the other group.

Unlike Allen's [1] proposition, the position here presented justifies the coercion of privacy not mainly for the coerced person's own good, but for the preservation of a liberal democracy and the avoidance of harm. A society that does not respect privacy, and allows for the 'unchecked ascendancy of surveillance infrastructures' cannot, according to Cohen [19], 'hope to remain a liberal democracy'. While Berlin [74] did not extensively discuss privacy, he states that the loss of it 'would mark the death of a civilisation, of an entire moral outlook'.

4.2. Government and technology

In order to understand the role of government in relation to technologies, it must be recognised that *technological processes* – together with social and economic processes – constantly change the opportunity space of individuals in society [2,65]. Warren and Brandeis [75] plainly state that technologies evolve, and with them, our governments and laws must also change. Allen [1] shows how new technologies has led to what she terms the 'great privacy give-away', due both to the increased benefits associated with waiving privacy and the obscure nature of privacy loss associated with new technologies. The erosion of privacy is often portrayed as one of the key ethical challenges associated with Big Data and modern technological advances more broadly [14,78,79]. With such changes, a change in the government's approach to privacy is also warranted.

While Downes [80] has noted that there is a *pacing problem* involved when innovation outruns 'social, economic, and legal systems', this is not a reason *not* to attempt to control new technologies and innovations, such as the growth of Big Data and artificial intelligence. Technology is seen by some as a powerful historical force that determines social change, and this perspective is known as technological determinism [81]. As noted by Heilbroner [81], such determinism is a heuristic and not a defeatist position that implies that all human agency and responsibility is illusory. There are several *forms* of technological determinism, and it is used both a *method* for understanding social change and

as a descriptive statement about technology's potential to cause social change [82,83].

In this article, it is argued that new technologies have clear and profound effects on social and political phenomena. The complexity of modern privacy makes it particularly hard to fathom and gain control of. It is somewhat akin to the difference between an old water mill, immediately understandable for most that observe it, and modern electricity-driven mills, fully understandable only to experts and scientists [84].

Despite this complexity, it is imperative that we evaluate the implications of new technologies through the political system, and examine whether or not these implications are conducive to society's core values and goals. If we as societies do not dare to question and control technology, we might soon find ourselves in a situation in which '[t]he cogwheels have drawn us into the very machine we thought was our slave' [85]. Technology is not and will never be neutral, and it must be subject to 'evaluation in normative systems' [85].

A classical *liberal* argument for government intervention is presented in this article. While a liberal may have a desire for the government to intervene as little as possible, all agree that it must do so at times. The market is a powerful mechanism for the distribution of knowledge and goods, but it is also prone to failure. Market failure in the market for privacy is the topic of this article, and this makes the regulation of privacy a classical candidate for government regulation.

Government intervention to prevent surveillance may sound paradoxical in a historical context, but we have already established how surveillance has become prevalent and how *private* organisations now perform a substantial part of surveillance. Since 'private corporations … have as much, if not more, power than many public authorities', preventing the abuse of *private* power is one of the most important justifications for *political* power [65]. This perspective provides us with a coherent account of why the government should *limit* private enterprise when it causes harm and interference with individual liberty, and while so doing must itself *refrain* from using the possibilities that technology provides in a similar way.

While the proposal to regulate privacy as a public good gives a more active role to the government than other liberal proposals, it also places clear boundaries on government action, and it is combined with a recognition of the fact that 'power is corruptible, fallible and inefficient' [65]. We should not *trust* the government, but hedge and fence its power while giving it enough authority to create the conditions for living a wide variety of what we perceive to be *good lives* [41,65].

5. Conclusion

Modern surveillance is pervasive and ubiquitous, and consists of the actions of individuals, organisations, *and* the government. The various diverse actors constitute a surveillant *assemblage*, which poses historically unique challenges to privacy. Modern privacy entails challenges related to externalities and information leakages to a degree not previously seen.

Privacy is an *aggregate* public good and government intervention is required in order to ensure the provision of collectively optimal levels of privacy, as individual rationality will lead to too little of the good being produced. Government involvement is required because the diffuse and long-term nature of the consequences of harm to privacy prevents individuals from comprehending the danger, and this precludes forms of voluntary cooperation that are sometimes effective for solving public good problems.

Government has a crucial role to play in dealing with the threats to privacy, and it is a *dual* role. Government must refrain from engaging in harmful activities while simultaneously protecting citizens from the threats posed by individuals and private organisations. Such government intervention is based on the avoidance of harm and a basic value pluralism, and not on paternalism and a desire to impose on individuals a particular conception of the good life. People's liberty to dismiss their own privacy is not reduced in order to protect themselves, but in order to prevent them from inflicting harm on others.

The exact nature of a regulatory scheme for public good privacy is not discussed in this article, and this remains a vital point for future inquiry. While technology can be a powerful historical force, so can human beings and their political institutions. The power to regulate and control technology is sometimes obscured by both the complexity of the technologies in question and the professed benefits of free markets and private initiative.

Such a liberal view of technology hands the reins back to human beings. Individuals in societies must start their quest for control by discovering what types of societies are conducive to their core values, and then it must be acknowledged that human beings, through politics, *have* the power to drastically alter the impact of technological innovation on their societies. The result depends on which core values are emphasised and how the harm of privacy loss is weighed against the benefits of new technologies based on the gathering of personal data. While allowing the collection, storage, and use of personal data has certain benefits, there is nothing apart from a desire for these benefits that prevents societies from severely restricting the same collection, storage, and use. These are *political* questions, and it is important to note that not all coercion by government is negative. Even for the most ardent liberal, some coercion is required in order to achieve well-functioning and flourishing societies.

Author statement

Henrik Skaug Sætra: All parts of the article.

Declaration of competing interest

No conflicting interests.

Acknowledgements

I wish to thank the anonymous reviewers who have read and commented upon earlier versions of this manuscript. They have contributed in a major way to the improvement of the published article.

References

[1] A. Allen, Unpopular Privacy: what Must We Hide? Oxford University Press, 2011.
[2] A.F. Westin, Privacy and Freedom, IG Publishing, New York, 1967.
[3] D.J. Solove, A taxonomy of privacy, U. Pa. L. Rev. 154 (2005) 477.
[4] D.J. Solove, Understanding Privacy, Harvard University Press, Cambridge, 2008.
[5] D.J. Solove, Conceptualizing privacy, Calif. Law Rev. 90 (2002) 1087.
[6] T. Scanlon, Thomson on Privacy, Philosophy & Public Affairs, 1975, pp. 315–322.
[7] J.J. Thomson, The Right to Privacy, Philosophy & Public Affairs, 1975, pp. 295–314.
[8] H.T. Tavani, J.H. Moor, Privacy protection, control of information, and privacy-enhancing technologies, Comput. Soc. 31 (1) (2001) 6–11.
[9] R. Gavison, Privacy and the limits of law, Yale Law J. 89 (3) (1980) 421–471.
[10] P. Brey, The strategic role of technology in a good society, Technol. Soc. 52 (2018) 39–45.
[11] D.J. Solove, The Digital Person: Technology and Privacy in the Information Age, NyU Press, 2004.
[12] H. Nissenbaum, Protecting Privacy in an Information Age: the Problem of Privacy in Public, Law and philosophy, 1998, pp. 559–596.
[13] H.S. Sætra, Freedom under the gaze of Big Brother: preparing the grounds for a liberal defence of privacy in the era of Big Data, Technol. Soc. 58 (2019) 101160.
[14] R. Herschel, V.M. Miori, Ethics & big data, Technol. Soc. 49 (2017) 31–36.
[15] S. Zuboff, The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019, Profile Books, 2019.
[16] J. Rachels, Why privacy is important, Philos. Publ. Aff. (1975) 323–333.
[17] G. Orwell, New York: Harcourt 1949 (1984).
[18] D. Lyon, The Electronic Eye: the Rise of Surveillance Society, U of Minnesota Press, 1994.
[19] J.E. Cohen, What privacy is for, Harv. Law Rev. 126 (2012) 1904.
[20] S. Zuboff, Big other: surveillance capitalism and the prospects of an information civilization, J. Inf. Technol. 30 (1) (2015) 75–89.
[21] K.D. Haggerty, R.V. Ericson, The surveillant assemblage, Br. J. Sociol. 51 (4) (2000) 605–622.
[22] D. Lyon, Theorizing Surveillance, Routledge, 2006.

[23] G. Deleuze, F. Guattari, A Thousand Plateaus: Capitalism and Schizophrenia, Bloomsbury Publishing, 1988.
[24] S. Delacroix, N.D. Lawrence, Bottom-up data Trusts: disturbing the 'one size fits all'approach to data governance, Int. Data Privacy Law 9 (4) (2019) 236–252.
[25] D. Lyon, Surveillance Studies: an Overview, 2007. Polity.
[26] K. Macnish, The Ethics of Surveillance: an Introduction, Routledge, Oxon, 2018.
[27] D.M. Wood, K. Ball, D. Lyon, C. Norris, C. Raab, A Report on the Surveillance Society, Surveillance Studies Network, UK, 2006.
[28] D. Lyon, The Culture of Surveillance: Watching as a Way of Life, John Wiley & Sons, 2018.
[29] K. Ball, D. Lyon, K.D. Haggerty (Eds.), Routledge Handbook of Surveillance Studies, Routledge, London, 2012.
[30] D. Lupton, Data Selves: More-Than-Human Perspectives, John Wiley & Sons, 2019.
[31] H.S. Sætra, When nudge comes to shove: liberty and nudging in the era of big data, Technol. Soc. 59 (2019) 101130.
[32] K. Yeung, 'Hypernudge': big Data as a mode of regulation by design, Inf. Commun. Soc. 20 (1) (2017) 118–136.
[33] H. Nissenbaum, Privacy as contextual integrity, Wash. Law Rev. 79 (2004) 119.
[34] D.D. Hirsch, Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel, Duke LJ Online 65 (2015) 67.
[35] C.J. Bennett, Review of Nissenbaum's privacy in context, Surveill. Soc. 8 (4) (2011) 541–543.
[36] M. Tisné, The Data Delusion: Protecting Individual Data Isn't Enough when the Harm Is Collective, 2020.
[37] L. Taylor, L. Floridi, B. Van der Sloot, Group Privacy: New Challenges of Data Technologies, Springer, 2016.
[38] N. Richards, W. Hartzog, Privacy's Trust Gap: A Review, HeinOnline, 2016.
[39] A.F. Westin, Social and political dimensions of privacy, J. Soc. Issues 59 (2) (2003) 431–453.
[40] N.G. Packin, Y. Lev-Aretz, On social credit and the right to be unnetworked, Columbia Bus. Law Rev. 339 (2016).
[41] S. Barrett, Why Cooperate? the Incentive to Supply Global Public Goods, Oxford University Press, 2007.
[42] B. Roessler, D. Mokrosinska (Eds.), Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge University Press, 2015.
[43] P.M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill: University of North Carolina Press, 1995.
[44] P.M. Regan, Privacy as a common good in the digital world, Inf. Commun. Soc. 5 (3) (2002) 382–405.
[45] P.M. Regan, Privacy and the common good: revisited, in: B. Roessler, D. Mokrosinska (Eds.), Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge University Press, 2015, pp. 50–70.
[46] D. Pullman, et al., Personal privacy, public benefits, and biobanks: a conjoint analysis of policy priorities and public perceptions, Genet. Med. 14 (2) (2012) 229–235.
[47] J. Lane, V. Stodden, S. Bender, H. Nissenbaum, Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press, 2014.
[48] A.F. Daughety, J.F. Reinganum, Public goods, social pressure, and the choice between privacy and publicity, Am. Econ. J. Microecon. 2 (2) (2010) 191–221.
[49] Z. Papacharissi, Privacy as a Luxury Commodity, First Monday, 2010.
[50] H. Nissenbaum, A contextual approach to privacy online, Daedalus 140 (4) (2011) 32–48.
[51] J.A. Fairfield, C. Engel, Privacy as a public good, Duke Law J. 65 (2015) 385.
[52] M. Ackerman, T. Darrell, D.J. Weitzner, Privacy in context, Hum. Comput. Interact. 16 (2–4) (2001) 167–176.
[53] S. Kuhn, Prisoner's dilemma, in: E.N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy, Spring, 2020, 2019.
[54] G. Hardin, The tragedy of the commons, Science 162 (1968) 1243–1248.
[55] J.P. Choi, D.-S. Jeon, B.-C. Kim, Privacy and personal data collection with information externalities, J. Publ. Econ. 173 (2019) 113–124.
[56] S. Barocas, K. Levy, Privacy dependencies, Wash. Law Rev. 95 (2020) 555.
[57] A. Ramachandran, A. Chaintreau, The network effect of privacy choices, Perform. Eval. Rev. 43 (3) (2015) 59–62.
[58] E. Morozov, The real privacy problem, Technol. Rev. 116 (6) (2013) 32–43.
[59] M. MacCarthy, New directions in privacy: disclosure, unfairness and externalities, ISJLP 6 (2010) 425.
[60] E.-Á. Horvát, M. Hanselmann, F.A. Hamprecht, K.A. Zweig, One plus one makes three (for social networks), PloS One 7 (4) (2012), e34740.
[61] E. Sarigol, D. Garcia, F. Schweitzer, Online privacy as a collective phenomenon, in: Proceedings of the Second ACM Conference on Online Social Networks, 2014, pp. 95–106.
[62] F. Brunton, H. Nissenbaum, Obfuscation: A User's Guide for Privacy and Protest, Mit Press, 2015.
[63] A.O. Krueger, The political economy of the rent-seeking society, Am. Econ. Rev. 64 (3) (1974) 291–303.
[64] A.L. Allen, Unpopular privacy: the case for government mandates, Oklahoma City Univ. Law Rev. 32 (2007) 87.
[65] J. Raz, The Morality of Freedom, Clarendon Press, 1986.
[66] F.A. Hayek, Freedom and coercion: some comments on a critique by Mr. Ronald Hamowy, in: Studies in Philosophy, Politics, and Economics, Chicago University Press, Chicago, 1967, pp. 348–349.
[67] F.A. Hayek, The Constitution of Liberty: the Definitive Edition, Routledge, 2013.
[68] J.S. Mill, On Liberty, Yale University Press, Yale, 2003.
[69] N. Devins, Reflections on coercing privacy, William Mary Law Rev. 40 (1998) 795.
[70] T. Hobbes, Leviathan, Basil Blackwell, London, 1946, p. 1651.
[71] A.L. Allen, Coercing privacy, William Mary Law Rev. 40 (1998) 723.
[72] C. Griffy-Brown, B.D. Earp, O. Rosas, Technology and the good society, Technol. Soc. 52 (2018) 1–3.
[73] G. Crowder, In defense of Berlin: a reply to James Tully, in: B. Baum, R. Nichols (Eds.), Isaiah Berlin and the Politics of Freedom: 'Two Concepts of Liberty' 50 Years Later, vol. 50, Routledge, New York, 2013, pp. 52–72, ch. 2.
[74] I. Berlin, Liberty, Oxford University Press, Oxford, 2002.
[75] S.D. Warren, L.D. Brandeis, The right to privacy. Harvard Law Review, 1890, pp. 193–220.
[76] H.S. Sætra, The tyranny of perceived opinion: freedom and information in the era of big data, Technol. Soc. 59 (2019) 101155.
[77] P. Pettit, Republicanism: a Theory of Freedom and Government, Clarendon Press, 1997.
[78] M.G. Hough, Keeping it to ourselves: technology, privacy, and the loss of reserve, Technol. Soc. 31 (4) (2009) 406–413.
[79] V. Kumpu, Privacy and the emergence of the "ubiquitous computing society": the struggle over the meaning of "privacy" in the case of the Apple location tracking scandal, Technol. Soc. 34 (4) (2012) 303–310.
[80] L. Downes, The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age, Basic Books, New York, 2009.
[81] R. Heilbroner, Technological determinism revisited, in: L. Marx, M.R. Smith (Eds.), Does Technology Drive History, MIT Press, Cambridge, 1994, pp. 67–78.
[82] S. Wyatt, Technological determinism is dead; long live technological determinism, in: The Handbook of Science and Technology Studies, vol. 3, 2008, pp. 165–180.
[83] L. Marx, M.R. Smith, Does Technology Drive History? the Dilemma of Technological Determinism, MIT Press, Cambridge, 1994.
[84] B. Russell, The Scientific Outlook, Routledge, London, 2009.
[85] A. Næss, Ecology, Community and Lifestyle: Outline of an Ecosophy, Cambridge university press, 1989.