



# Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defence of privacy in the era of Big Data

Henrik Skaug Sætra

Østfold University College, Remmen, 1757, HALDEN, Norway

## ARTICLE INFO

### Keywords:

Big data  
Liberty  
Negative liberty  
Surveillance  
Privacy

## ABSTRACT

'Big Brother is watching you!' the posters in Orwell's Oceania told all its inhabitants. We have no such posters, but we live in the *era of Big Data*, and someone is watching us. Here, I discuss how Big Data is an omniscient and ubiquitous presence in our society. I then examine to what degree Big Data threatens liberty in both the negative and positive conception of the term. I arrive at three propositions: a) Big Data threatens privacy and enables surveillance, b) the lack of alternatives to lifestyles that involve feeding into Big Data leads to something akin to forced participation in the surveillance of Big Brother, and c) surveillance and lack of privacy are a threat to freedom, because i) the information gathered can be abused, ii) people have a right not to be observed (even if the surveillance is completely benign), and iii) being observed is an intervention that can affect those who are observed. Together, these propositions lead to the conclusion that Big Data threatens liberty. I argue that the positive conception of liberty provides the strongest argument against how we currently employ Big Data, but that the negative conception can also provide a sufficiently strong argument. On this basis, a liberal defence of privacy, and thus also of liberty, against this new form of surveillance can be established.

## 1. Introduction

'Big Brother is watching you!' proclaim the posters in Orwell's Oceania [35]. We have no such posters, but someone *is* watching us. The websites we visit, the products we like, who we find attractive and how we move around – all this is observed, stored and finally analysed. We live in the *era of Big Data* [1–3].

The concept of Big Data links up with the idea of Big Brother, in that Big Data is a kind of omniscient and ubiquitous presence. I examine whether or not Big Data threatens freedom, both in the negative and in the positive sense [4]. I argue that privacy is threatened by how we employ Big Data, and that the various forms of surveillance that ensue constitute a threat to liberty.

I arrive at three propositions in the course of this paper, and they will serve as premises for my main argument. These propositions are: a) Big Data threatens privacy and enables surveillance, b) the lack of alternatives to lifestyles that involve feeding into Big Data leads to something akin to forced participation in the surveillance of Big Brother, and c) surveillance and the lack of privacy are a threat to freedom, because i) the information gathered can be abused and ii) people have a right not to be observed (even if the surveillance is completely benign). Using these propositions as premises for my overall argument, I show that liberty, in both the negative and the positive

sense, is threatened. It is a two-pronged threat to liberty since a) we experience a lack of alternatives to taking part in the collection of Big Data, and b) taking part involves a loss of liberty by placing us under surveillance. The positive conception of liberty provides the strongest argument against how we currently employ Big Data, but the negative conception can also provide a sufficiently strong argument. On this basis, a liberal defence of privacy, and thus also of liberty, against this new form of surveillance can be established. Finally, I wish to note that my concern in this paper is *liberty*, and while it is obvious that Big Data provides great benefits, my concern is not to find the proper trade-off between *utility* and *liberty*. I merely argue that Big Data poses a threat to liberty. Liberty is a foundational value of what Griffy-Brown, Earp & Rosas [5] refer to as the *Good Society*, and this is thus an effort to understand how technology can be detrimental to our society. While we may state that the benefits it brings are well worth it, we should not accept such technologies without at the same time clearly recognising the costs incurred in terms of lost privacy and lost liberty.

## 2. Big Data in modern society

The term *Big Data* is often defined by the *three Vs*: *volume*, *velocity*, and *variety* [6]. Volume refers to the massive amounts of data collected, velocity to the speed of data generation and analysis, and variety to the

E-mail address: [Henrik.satra@hiof.no](mailto:Henrik.satra@hiof.no).

<https://doi.org/10.1016/j.techsoc.2019.101160>

Received 24 January 2019; Received in revised form 19 June 2019; Accepted 5 July 2019

Available online 08 July 2019

0160-791X/ © 2019 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

'structural heterogeneity' of the data [7]; p. 137). Big Data is not only new in the sense that we now create *bigger* data sets than we used to, but also because this bigness has led to new requirements for data analysis and data processing [8]; p. 45 [1]; p. 662).

A related concept is *machine learning*. In order to analyse the data we gather, we no longer rely on human insight or old style statistical analysis. Some even argue that we may no longer need humans in science etc. Since the machines can now replace us [9]. We have created machines that can learn without being told explicitly what to look for. We simply give them certain goals, and these systems 'improve their performance on a given task over time through experience' [10]; p. 9). As these systems learn, we use the knowledge gained to perform tasks historically thought to require intelligence, such as determining who should be granted loans, suggesting what movies I might be interested in etc. When employed in this way, we have *artificial intelligence* [10]; p. 9).

### 2.1. The gathering of Big Data

We leave countless traces of our daily activities in the rapidly growing collections of databases. A multitude of companies and institutions gather the different snippets of data, and the whole structure that has been set up to gather data has been called the 'surveillant assemblage' [11]. This term refers to the combined effects of private and public efforts, markets and institutions that, together, form an assemblage of surveillance. Much of the information is gathered by private companies, but government 'is an important secondary beneficiary' [12]; p. 1916).

I work on the assumption that we can meaningfully consider Big Data a phenomenon that involves a unitary threat to liberty. As such, I speak of a Big Brother, and not many small brothers. This assumption is not uncontroversial, and I fully accept that there is not *one* large company, organisation or government that collects, or organises the collection of, data. However, I agree with the view of Haggerty & Ericson ([11], p. 605) that we are seeing a 'convergence of once discrete surveillance systems' – not a convergence in the sense of corporate consolidation, but in the sense that the countless separate streams of information about individuals is subsequently combined, shared, traded and reassembled to provide a comprehensive and full description of individuals and their actions. Big Data consists of a large number of surveillance sources that function as an *assemblage* – the unity of this Big Brother is not formal, but *functional* [13].

### 2.2. From Big Data to Big Brother

Big Data is valuable in various ways, and the benefits are both well-known and extensively covered. I fully accept the utility of Big Data, and this is not a statement *against* Big Data in general. I focus on its implications for *liberty*, while recognising that liberty is not everything. The trade-off between utility and liberty is a complicated one, and I merely ask that, when we side with utility, we do so while recognising that it comes at the cost of lost liberty.

Alan Westin's [37] *Privacy and Freedom* discussed the challenges to privacy from new technologies and public concern about the dangers of *Big Brother*. More than fifty years later, the book is arguably more relevant than ever before. Big Data has changed things, since Big Brother has never had a better chance to work his magic while both keeping an eye on what is happening and preventing what he does not like. Overt surveillance may have given way to covert surveillance – a form that feels quite cosy, and that is less dependent on authority and police enforcement, and more on the apparently voluntary provision of data. We agree to terms most of us do not even read [14]. The data collected are today's gold, and we happily give them away to gain access to various services. We connect with people and companies, get news and laughs, and in living our lives this way, we provide all the information required to *really* know us well.

The price we pay for 'free' services is to open the curtains that once hid our private sphere. If all the information I provide to various sites were kept isolated from other data, this would weaken my assumption that Big Data is a kind of assemblage that works as a functional entity. We know, however, that the different sites *do* sell the information we provide, and some major controversies have highlighted such problems, for example the Cambridge Analytica scandal involving Facebook [15,16].

Besides information that is provided voluntarily, information is also gathered from various other sources, such as GPS signals, satellite images, surveillance footage, information from mobile phone companies, smart electricity meters etc. Some of this information requires consent, and some of it is gathered with government blessing.

In sum, Big Data might turn into a form of Big Brother, in that it is *omniscient* and *ubiquitous*. While Big Data Brother is actually watching you, the political aspects of our societies and Orwell's Oceania are still quite different [35]. Big Brother is the head of an imaginary totalitarian society, but this form of surveillance is not restricted to societies such as Orwell's Oceania. Big Data *may* take us there, though, and both Cohen and Berlin argue that the loss of privacy could lead to societies that are less liberal, and less well functioning [4]; p. 176 [12]; pp. 1904–5).

### 2.3. The first proposition

Based on these considerations I have arrived at the first proposition:

Big Data in modern society involves gathering vast amounts of data, even the most private data, from individuals. Big Data thus threatens privacy and enables surveillance.

Firstly, Big Data involves gathering large amounts of people's private data. It is possible to deny that this is happening, or to state that Big Data is not *necessarily* connected to private data. I argue that *I have* shown that it is in fact happening today, and it is this phenomenon I am discussing – not some ideal and limited, alternative implementation of Big Data.

Secondly, if massive amounts of private data are being gathered, privacy is, naturally, under threat.

Thirdly, the tools and routines used to gather the information described in this section *enable* surveillance. We may assert that the collection of data constitutes surveillance in and of itself, but we need not. It suffices to state that the data, when gathered, exist and *may* be used for surveillance purposes in some unknown future.

## 3. Liberty, positive and negative

*Liberty* has many meanings, and I have chosen Berlin's [4] concepts of positive and negative liberty as my frame of reference when evaluating the impact Big Data has on liberty. Coeckelbergh [38] calls for political philosophy to be used when analysing the effects of technology, and I agree with him that this tradition 'offers excellent resources for thinking about' issues such as technology and liberty [38].

Berlin [4] describes *negative* liberty as 'the degree to which no man or body of men interferes with my activity' [4]; p. 169). Negative liberty involves being allowed to 'act unobstructed' and 'not being prevented by others from doing what I could otherwise do' [4]; p. 169). A certain minimum of 'contraction' by other men is inevitable, but anything beyond this would make me 'coerced, or it may be, enslaved' [4]; p. 169). If I am unable to achieve something, this does not give me occasion to speak of unfreedom, unless that inability is caused by other men [4]; p. 169).

*Positive* liberty involves a desire 'on the part of the individual to be his own master' [4]; p. 178). It is sometimes referred to as *self-mastery* [17]. Wanting my life to be the result of nothing but my own volition and actions, I would label any external influence that prevents me from achieving what I desire a violation of my liberty [4]; p. 178). Furthermore, the focus is on being a *subject*, not an object, and 'deciding,

not being decided for, self-directed, and not acted upon by external nature or by other men as if I were a thing, or an animal, or a slave incapable or playing a human role, that is, of conceiving goals and policies of my own and realising them' [4]; p. 178). Positive liberty involves more than being free to *act*, it also requires that my actions are the result of my own autonomous reflective activity.

Positive liberty involves some far-reaching conditions that must be satisfied. For me to be free, it is not sufficient that I am unobstructed, if I am fundamentally *enslaved* in some way. Slavery to nature, slavery to the passions, and spiritual slavery are examples. Emancipation may lead to a 'higher' understanding of the self, in which one can, for example, identify the self with all other beings [4]; p. 179). If we move along this path, there is little that cannot be argued to stand in the way of an individual's freedom. It even becomes possible to *force a person to be free*, by releasing her from whatever slavery we find her to be in Ref. [4]; p. 179). Positive liberty is thus not a *goal* for most liberal theorists, but rather a danger to be warned against. I use both the negative and the positive concepts of liberty to elucidate the different requirements that follow from them, without deciding which one we *should* pursue.

I will also refer to the proposal that liberty is *non-domination* [18]. This is elsewhere referred to as *republican* liberty. Pettit places this concept *between* positive and negative liberty. It is negative in the sense of requiring the absence of domination by others and not requiring *self-mastery*, and positive in the sense that it demands something more than the mere absence of interference – it requires *protection* against interference as well [18]; p. 51). When non-domination is considered a prerequisite of liberty, I consider the mere fact that someone *has* power to coerce you and dominate you to be a violation of liberty, and not just *active* use of this force to control your actions. I will propose an argument akin to Hobbes's view of war as the *possibility* of war, and not only active fighting, when I consider the possible threat to freedom posed by Big Data [19]. The uncertainty that follows from the risk of data leaks, human error, hostile hacking attempts, the sale of data, change of ownership of companies, change of government, or simply a change in the intentions and plans of the actors we once trusted, makes the mere existence of data a threat.

Negative liberty focuses on physical and legal obstructions, while positive liberty opens up for a much broader examination of the condition one is in. The scope of the current paper does not allow for a thorough examination of the implications of the two forms of freedom, and I refer to Berlin's *Two Concepts of Liberty* [4] and Taylor's [20] critique of the concept of negative liberty in his paper *What's wrong with negative liberty* for a fuller description. See also MacCallum [21] and Skinner [22] for a more general critique of the concept of two separate kinds of liberty.

## 4. When Big Brother sees you

### 4.1. Privacy and private information

*Privacy* refers to the sphere in which one can expect to be completely unobserved, and it denotes both *information* and *acts* that are considered private. As such, privacy is a concept whose content can change depending on the user's views of what is properly private and public. It is a difficult term to define, and it has been used to express a confusing variety of concepts [37]. Westin ([37], p. 7) ventures the following definition:

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

It is characterised by being *voluntary* and *temporary*, and it involves withdrawal from the public – either physically or psychologically [37]. Privacy is thus a constant battle between my desire to withdraw and the curiosity of both the government and other people. The judicial aspects of privacy are beyond the scope of this article, and I posit that people

have a *right* to privacy [23].

In order to provoke as few objections as possible, I will assume that this right protects only a minimal sphere that most people would agree should be private. This right entitles me to object when, for example, my neighbour wants to survey my house out of curiosity, or when the government has a desire to track my movements using a GPS tracker. There must be *some* sphere I can retreat into in order to meaningfully experience privacy. I therefore reject the proposition that liberty is consistent with the position that everything is political. Individuals must be able to deny the public access to certain parts of their lives.

Big Data threatens privacy in several ways. Firstly, if I live a standard life, using regular tools and services that are ubiquitous in our society, I will have to surrender private information. Secondly, even if I attempt to keep my strictly personal information to myself, many groups and organisations are now virtual, meaning that information about meetings, communication etc. is gathered, and sometimes made public. This can also be construed as a violation of my privacy. Finally, some information is gathered against our wishes or without our knowledge, justified by concerns such as safety and security, anti-terror legislation etc.

#### 4.1.1. Big Data and superficial voluntariness

It may be objected that the first two threats are agreed to voluntarily, and that everyone has the option to refrain from such activities. One of the reasons why it is so hard to *not* feed into Big Data, is that a lot of the services that collect *most* data are practically a necessity for people today. Social media sites such as Facebook are where friends and family communicate, colleagues coordinate social events, and parents meet in various groups to coordinate their children's various activities etc. Not taking part is *possible* but comes at a high social price. Saying 'no' to the user agreements provided by, for example, social media sites is of course *possible*, but may involve being 'deprived of critical services' [24]; p. 586).

For participation to be voluntary, alternatives must exist. When people are required to have accounts with, for example, Facebook, in order to get crucial information about their children's activities, studies, social events etc., freedom of choice disappears. People are left with the choice between either grudgingly complying with the new normality of surveillance, or becoming like Luddites in a new social pariah caste. In addition, banks and government services are becoming increasingly digital, while traditional alternatives disappear.

As regards negative liberty, we do not have to agree with Thomas Hobbes that a person threatened with grave consequences is still at liberty to act freely. Hobbes relates the story of a man in trouble at sea who faces the dilemma of either a) throwing his goods overboard, or b) sinking. According to Hobbes, the man is free to sink, so no liberty is lost [19]; p. 137). In a similar vein, we are free to reject everything digital. *Voluntary* acts are *free* acts for Hobbes, but it is Berlin who defines our liberty. Within the framework of Berlin's negative liberty, a robber with a gun obstructs and disrupts the liberty of the person he robs. His interference is clear, and his intention is to constrict our liberty and coerce us into acting in a certain way. The specifics of this debate is beyond the scope of this article, and I refer to Carter's [17] discussion for more detail on how such situations does not necessary lead to a loss of *specific* freedom, while still leading to a loss of *overall* freedom. Lanier [25] and Zuboff [26] provide detailed accounts of the difficulties of escaping the gaze of Big Brother.

Foreshadowing one of my conclusions, it seems likely that privacy is a good that is not best served by an individualised approach. I will argue that privacy is a public good, and that we must consider it a task for government to prevent situations where people are forced to abandon privacy in order to live what would be considered normal lives. What constitutes a normal life, and when liberty is lost by not being allowed such a life, are big questions that are beyond the scope of this article. I will also note that in the current setting, we do not need to say that privacy has intrinsic value. It may simply be valuable because it

has *constitutive* value, in that it is a necessary condition for liberty [17]; p. 54).

#### 4.2. The second proposition

Based on these considerations, I arrive at the second proposition:

A lack of alternatives to lifestyles that involve feeding into Big Data leads to something akin to forced participation in the surveillance of Big Brother

Freedom can be said to consist of having alternatives to choose between. In modern society, we are running out of alternatives that let us live *outside* the gaze of Big Brother. I fully recognise that, theoretically, we may avoid much of the surveillance. However, doing so involves incurring higher and higher costs because essential societal functions are organised through, for example, social media. Other parts of the surveillance are performed by government decree. Examples here would be the requirement that households install smart electricity meters in their homes or that all cars are required to have GPS transmitters etc.

#### 4.3. Surveillance and freedom

Surveillance can be defined as *attention* that is focused on an individual in order to obtain some kind of information. Surveillance can also be general, i.e. information on *all* or most people is gathered. While the focus is broad, there is still attention on each individual and those behind the surveillance will be able to identify the actions of each observed person. Westin [37] distinguishes between *direct* surveillance and *indirect* surveillance. The first involves actively watching a particular person, whereas indirect surveillance involves gathering records and information that are subsequently used to determine the need for direct surveillance.

I distinguish between three kinds of surveillance. Firstly, it is important to note that surveillance does not necessarily lead to interference in people's lives. Someone might gather information about others without doing anything to steer, guide or prevent the actions of the person observed. If so, *observation* is all this is, and the person is, technically, as free to *act* as he would have been without being observed. The electricity meters in our homes provides such information. Certain forms of video surveillance that are installed merely to observe and document behaviour etc. are of this kind. This I label *passive observation*.

Secondly, we can imagine that an act is committed under surveillance, and that the person observing uses the information as evidence in order to punish or reward the actor in retrospect. This form of surveillance could, of course, also be benign. Perhaps the information gathered is used to reward pro-social behaviour, or in order to give good citizens credits in a government-run reward scheme. China is planning such a scheme whereby citizens will be given a 'Citizen Score' that will determine their chances of obtaining loans, visas etc. [27]. However, such schemes would strike most of us as totalitarian rather than benign, even if they were designed to provide rewards instead of punishment. While the first situation constituted passive observation, I call this *active observation*.

The third kind of surveillance is the one we most often think of, where those behind the surveillance use it actively to both punish and reward actions already performed *and* to prevent *planned actions*. If a government agency receives information that a group of individuals is planning a terrorist attack, it will intervene rather than use this information to punish the individuals afterwards. This is *surveillance proper*. See Fig. 1 for a description of the three forms of surveillance.

##### 4.3.1. The threat of passive surveillance

How do the three forms of surveillance affect liberty? To examine the situation that is *least* likely to be problematic, let us conduct a

	1. Passive observation	2. Active observation	3. Surveillance proper
Observation	X	X	X
Retro-active use	-	X	X
Pro-active use	-	-	X

Fig. 1. The three forms of surveillance.

thought experiment. Assume that we have discovered a new form of being that we call the Observer. The Observer does not exist in physical space, has no memory and has no possible means of communicating. It can, however, observe whatever it desires. Would we have cause to complain about being observed by this being that has no possible means of using, or abusing, the information it gathers and no possibility of influencing our lives in *any* other way than by the fact that it can observe us?

Imagine yourself at home, alone with your spouse. You have a desire for intimacy with your spouse, but suddenly you become aware that the Observer is watching you. Would this affect your behaviour in any way? If we assume that his lack of memory and inability to store information is real, there is no reason to worry about the possible *abuse* of actions the Observer observes. I could, however, cite my *right* to privacy, and state that, for me, liberty partly consists in this right being protected. If the Observer sees me, I am not free, because my right to privacy is obstructed – purposefully – by another being. The *reason* I demand privacy is of little consequence, but I could cite reasons such as modesty and the desire to do things that would cause me to feel shameful if I knew that someone was observing me. Observation alone would hinder me. I could, for example, simply feel that the Observer would judge me. Being observed *changes* my behaviour. Since I act differently when observed, I lack liberty if there is no space in which I can be unobserved.

##### 4.3.2. The threat of active surveillance

When we can be punished after-the-fact based on evidence gathered, our actions are more likely to be affected by the observation. Some actions will be more costly due to the fact that I know that I will be punished. I do not take issue with liberty and the law, and take the view that liberty consists in living in accordance with a limited set of laws that are necessary to keep order. This is akin to Bastiat's [28]; p. 25) view that, for an individual, (proper) laws are not a violation of 'his personality, his liberty, nor his property. They safeguard all of these'.

Consider now my freedom to perform *immoral* acts – acts that people frown upon – without them being illegal. I would probably feel pressure to abstain from those as well. This is an issue Tocqueville [29] notes in his examination of American democracy – the tyranny of the majority. The majority can create a set of opinions and actions that are accepted, while others are met with social sanctions without being illegal. In America, Tocqueville noted, this set was so limited, and the sanctions so harsh, that people lacked both spiritual independence and *real* freedom of speech [29]; p. 293). It is easy to envisage freedom of action suffering as a result of the same mechanisms as freedom of discussion.

##### 4.3.3. The threat of surveillance proper

An interesting aspect of surveillance proper is that it leads to people being arrested for planning crimes not yet committed. Conspiring to do such things has been declared a crime, so a criminal act has been committed just by *planning* the actions, and acts of this kind are hard to uncover without surveillance of some sort. Thus, we have arrived at the most common justification for surveillance.

If we follow the argument of political philosophers like Thomas

Hobbes, we accept that people will, by necessity, award *some* rights of surveillance to the sovereign power in order to preserve what is most important: safety, order and the survival of the political community [19]. While Hobbes states that the government should have no more such rights than *necessary*, he is not comfortable about erecting solid barriers the authorities may never pass. More liberal theorists, such as John Locke, do not have such qualms [30]; p. 184). Either way, we probably cannot both claim *absolute* rights against government surveillance *and* say that we want the government to ensure order. In order to use the concept of liberty in a meaningful sense, we must be able to consider ourselves free, even in society. This is a case where utility clearly trumps absolute liberty. But can we sacrifice liberty for others purposes than safety? This is the age-old question of political theory and the legitimacy of the state. According to Hobbes [19], *security* and *survival* are the only things men can universally agree upon as goods. Thus, the state can legitimately limit our liberty through the use of surveillance aimed at promoting order, although this logic does *not* allow surveillance in order to promote other goods that might be seen as luxuries.

#### 4.3.4. Danger of abuse

Finally, I briefly consider more traditional arguments against surveillance, such as a) the possibility that the information will be used in other ways than we are led to believe, b) the fact that information, being stored, may come into the wrong (or just *other*) hands later on, and c) the possibility that the information will be used against us in new and novel ways in future that we cannot now foresee.

The first option involves either deception or simply a lack of understanding on the part of users. When people create their accounts on Facebook, they *assume* that the information they provide will not be used to target them politically, for example in order to influence how they vote. One might argue that they *should* be aware of such risks. If sufficiently many do *not* understand the risks, government regulation might be necessary in order to prevent the exploitation of individuals' trust. This is partly because of a general desire to preserve privacy and liberty, but also partly because of the near mandatory nature of such services in modern society.

The second option involves factors such as the chance of human error, the sale and transfer of information between corporations, organisations and government, and theft of data. While criminal exploitation of data, identity theft, hacking etc. are certainly possible, a full examination of the degree of risk each of the above possibilities entails is beyond the scope of this article.

The third option is of great importance, since it suggests that we should adopt a precautionary stance towards privacy regulation. While providing data may not pose a risk *today*, we have no guarantee that it will not be used for malign (from our perspective) purposes *tomorrow*. What if new regulations allow such data to be shared and used for purposes such as pricing insurance, granting travel visas, gaining access to public services etc.?

In addition to the threats of abuse, Big Data poses a threat in itself, so I might not even *need* to consider abuse in order to construct a liberal defence of privacy. When the foregoing points are combined with the possibility of abuse, however, we see the contours of an even greater threat to liberty.

#### 4.4. The third proposition

The above considerations lead to the third proposition:

Surveillance and the lack of privacy are a threat to freedom, because a) the information gathered can be abused, b) people have a right not to be observed (even if the surveillance is completely benign), and c) being observed is an intervention that can affect the observed person.

Not having privacy is a threat to freedom for three reasons. The first

P1: Big data threatens privacy  
P2: Lack of alternatives to a life under the gaze of Big Brother  
P3: Liberty requires privacy

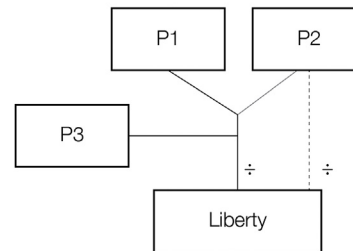


Fig. 2. The premises and their effect on liberty.

is based on a precautionary principle, which implies that surveillance and observation are wrong simply because they are *risky* – not because they are wrong in themselves. However, the second reason is that we can legitimately view it as wrong in principle to deprive people of a right to privacy. Thirdly, regardless of rights, surveillance is an intervention that changes my behaviour and makes it costlier to perform actions that I would prefer to be unobserved. Some might say that someone who has nothing to hide should have no objection to surveillance, but this is a flawed argument. The costs created by surveillance apply to actions that are not illegal or constitute ‘something to hide’ in the judicial sense.

## 5. Freedom under the gaze of Big Brother

### 5.1. Introduction

With these three premises established, it is time to see what conclusions follow. The premises in short form are as follows, but please refer to their full statement for more detail and precision. See Fig. 2 for the premises and their relationship with liberty.

There are two main conclusions that follow from the premises presented. They are 1) that Big Data poses a threat to both positive *and* negative liberty, but perhaps *especially* to the concept of liberty as non-domination described by Pettit [18]; and 2) individuals' liberty may be under threat even if the individuals themselves do not divulge information. Privacy may in fact be a public good.

### 5.2. Big Data is a threat to positive and negative liberty

#### 5.2.1. The threat to positive liberty

The premises lead to the conclusion that positive liberty is under threat. As P1 is combined with P3, we see that a lack of privacy and being under surveillance threaten liberty both because of the risk of abuse of information and because the fact of being observed is a violation of a person's right to have a private sphere in which he will be neither observed nor disturbed.

While a negative conception of liberty may allow us to disregard many factors that *influence* a person because they are inimical to liberty, the positive conception does not. If I am to be my own master, I must have the privacy required to act as if unobstructed. Being observed is an obstruction insofar as it imposes various costs on actions that a person may have a desire to perform. If I am observed, and thus act differently than I would otherwise want to, my actions are not the actions of a positively free person.

It is possible to argue that, if I am truly my own *master*, I should be strong enough to withstand the pressure of expectation, and withstand the possibility of social sanctions. In my opinion, human traits such as modesty and shame must be accepted instead of wished away. This means that it is problematic to legislate on the assumption that people are, or *should be*, free from such influences, and that we should instead legislate in ways that remove the possibility of making people less free

by not taking things such as modesty into consideration. We might wish that our spouses, and others, had no problem with surveillance at home, so that the government could protect everyone even better, but since that is not the case, such a policy cannot be accepted.

Positive liberty requires that I be given space to both *become* and *act* as my own master, and surveillance can prevent both these things from happening. Berlin imagines an autonomous person 'not acted upon by external nature or by other men as if I were a thing, or an animal, or a slave incapable or playing a human role, that is, of conceiving goals and policies of my own and realising them' [4]; p. 178). This, I argue, is not a person under surveillance.

### 5.2.2. The threat to negative liberty

For negative liberty, we can make a somewhat weaker – but still strong – argument for the case that Big Data is a threat. With the third premise, we may only need the first part, which concerns the risk of abuse, in order to argue that surveillance and lack of privacy are inimical to liberty. If so we would be constructing an argument that resembles Pettit's [18] liberty as *non-domination*. I will argue that a practical doctrine aimed at protecting liberty in the negative sense also requires *safeguards* against future interference, and I have shown that this will most likely involve restricting what sort of data can be gathered, or *at least* what information can be stored and transferred, and how it can be used – now *and* in the future.

It can also be argued that being deprived of the right to privacy is in itself a violation of negative liberty, due to the combination of the first and second premises. Berlin discusses *non-interference* when discussing negative liberty [4]. While being observed constitutes a violation of the space required to be positively free, I argue that it can also be interpreted as a form of *interference*.

Say that I, when at home alone, have a desire to watch movies that most people consider morally disgusting. If I can get a hold of such movies without anyone observing it, I would do so. However, if I know that others *are* registering and taking note of the movies I acquire, I might abstain. The introduction of observation is interference, and, if I cannot choose to not be observed, negative liberty is violated. I would argue that this was the case because a) someone could use this information against me in the future, b) I have a *right* to privacy with regard to my choice of movies, and c) I dare not watch the movies I want to watch when I am being watched, so this observation interferes with my ability to perform lawful actions that hurt no-one. I could say that I am 'coerced, or it may be, enslaved' because my inability to do what I desire is caused by the conscious and intentional actions of other men [4]; p. 169).

### 5.3. Privacy is a public good

An argument against the individualised approach to privacy regulation is that privacy might actually be a common good [31]. Public goods are usually considered to be non-excludable and non-rival, and the general preservation of privacy fits well with such a description. In the terminology of Barrett [32]; I consider this to be a public good in the category *aggregate effort*, as it requires the participation of *most* in order to be provided.

The fact that some people choose to bargain away their privacy has negative effects on the people around them. When enough people *like* me bargain away their privacy, data exist that can then be used to target *me*, even if I should turn down every opportunity to bargain away my privacy in return for online services etc. The profiles of people who share my main characteristics and willingly share their information might be sufficient to enable actors to violate my liberty in various ways. Had I been able to hide *all* information about myself, I would not be at risk, but that is an impossible scenario. Since *some* information about me exists, those who wish to target me will superimpose this information on the vast amounts of information they have about others, and thereby know much more than I would have wanted.

Others' attitude to privacy will also have more direct ramifications for me, in that their sharing of information will, by necessity, also include some information on their various relations and social life. Secondary data on me is then gathered, and services may even create secret 'shadow profiles' on *me* in which to store all this information, even if I actively choose not to have anything to do with the service. See, for example, the article *One plus one makes three (for social networks)* [33] for information about how the information supplied by members is used to obtain information about *non-members*. See also McMillan [34] for more about how social networks create privacy problems for non-members. I am unable to deal fully with this issue here, and merely conclude that this point is very important when considering what is the best approach to regulating privacy and the use of Big Data.

## 6. Conclusion: Big Data is a threat to liberty

Big Data can be seen as constituting a form of surveillance. This surveillance is problematic, and I argue that freedom is threatened under the gaze of Big Brother. It is important to note that the *technology* of Big Data is neutral, and that it is the way we apply it that is threatening.

The three premises I have presented lead to the conclusion that liberty, both positive and negative, is threatened, and that privacy is a *public* good. There are therefore several reasons for adherents of liberalism to be wary of the effects of Big Data and how we currently regulate (or do *not* regulate) it.

It could be argued that liberalism is concerned with freedom, and that this freedom means that businesses and government must be free to innovate and use new technology to gather data. As long as this is based on voluntary actions, many liberals would not object, and some would even claim that the *economic* benefits of how we use Big Data today more than outweigh the negative effects on privacy and other forms of liberty. In the areas of science and business, there are many examples of how the advent of Big Data has resulted in great benefits. I fully accept these benefits, but that does not alter the fact that it poses a threat to liberty. We must make a trade-off, and that means that we must consider how highly we value liberty.

I argue that liberty requires privacy, and that the individual's right to a sphere which no one can enter without express agreement is fundamental, and more so than businesses' freedom to innovate and observe others. This is particularly important since I also argue that agreeing to the collection of personal data is close to *compulsory* in today's society, and that privacy is a common good. The regime of *notice and choice* is therefore not sufficient to constitute informed consent, and we must move from individualised regulation of privacy to government regulation. The government has a role in providing common goods, and the area of privacy is a prime candidate for government intervention. How this can be achieved, particularly since this is a deeply problematic issue due to its digital and international nature, is one of the most pressing issues in modern society. Big Brother's gaze must be averted, if people are to be fully free. To be their own masters, if you wish, or simply to ensure that people are not 'coerced, and enslaved', to use the words of Isaiah Berlin [4].

## References

- [1] D. Boyd, K. Crawford, Critical questions for Big Data: provocations for a cultural, technological, and scholarly phenomenon, *Inf. Commun. Soc.* 15 (5) (2012) 662–679.
- [2] H. Chen, R.H. Chiang, V.C. Storey, Business intelligence and analytics: from Big Data to big impact, *MIS Q.* (2012) 1165–1188.
- [3] U. Sivarajah, M.M. Kamal, Z. Irani, V. Weerakkody, Critical analysis of Big Data challenges and analytical methods, *J. Bus. Res.* 70 (2017) 263–286.
- [4] I. Berlin, Two concepts of liberty, in: H. Hardy (Ed.), *Liberty*, Oxford University Press, Oxford, 2002.
- [5] C. Griffy-Brown, B.D. Earp, O. Rosas, Technology and the good society, *Technol. Soc.* 52 (2018) 1–3.

- [6] D. Laney, 3D data management: controlling data volume, velocity and variety, *META Group Res. Note* 6 (70) (2001).
- [7] A. Gandomi, M. Haider, Beyond the hype: big data concepts, methods, and analytics, *Int. J. Inf. Manag.* 35 (2) (2015) 137–144.
- [8] G. Bello-Organ, J.J. Jung, D. Camacho, Social big data: recent achievements and new challenges, *Inf. Fusion* 28 (2016) 45–59.
- [9] H.S. Sætra, Science as a vocation in the era of big data: the philosophy of science behind big data and humanity's continued part in science, *Integr. Psychol. Behav. Sci.* (2018) 1–15.
- [10] M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, H. Anderson, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, (2018) arXiv preprint arXiv:1802.07228.
- [11] K.D. Haggerty, R.V. Ericson, The surveillant assemblage, *Br. J. Sociol.* 51 (4) (2000) 605–622.
- [12] J.E. Cohen, What privacy is for, *Harv. Law Rev.* 126 (2013) 1904–1933.
- [13] G. Deleuze, F. Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, Bloomsbury Publishing, 1988.
- [14] R. Böhme, S. Köpsell, Trained to accept?: a field experiment on consent dialogs, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2010, April, pp. 2403–2406.
- [15] P. Greenfield, *The Cambridge Analytica Files: the Story So Far*, *The Guardian*, 2018, March 26th Retrieved from <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far>.
- [16] A. Picchi, *Facebook: Your Personal Info for Sale*, (2018, March 21) Retrieved from <https://www.cbsnews.com/news/facebook-your-personal-info-for-sale/>.
- [17] I. Carter, *A Measure of Freedom*, Oxford University Press, 1999.
- [18] P. Pettit, *Republicanism: a Theory of Freedom and Government*, Oxford University Press, 1997.
- [19] T. Hobbes, *Leviathan*, Basil Blackwell, London, 1946.
- [20] Taylor Charles, *Philosophy and the Human Sciences: Philosophical Papers 2*, Cambridge University Press, Cambridge, 1985.
- [21] G.C. MacCallum, Negative and positive freedom, *Phil. Rev.* 76 (3) (1967) 312–334.
- [22] Q. Skinner, A third concept of liberty, *Proceedings of the British Academy*, vol. 117, Oxford University Press, Oxford, 2002, pp. 237–268.
- [23] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, Quid Pro Books, New Orleans, 2010.
- [24] L. Baruh, M. Popescu, Big data analytics and the limits of privacy self-management, *New Media Soc.* 19 (4) (2017) 579–596.
- [25] J. Lanier, *Ten Arguments for Deleting Your Social Media Accounts Right Now*, The Bodley Head, London, 2018.
- [26] S. Zuboff, *The Age of Surveillance Capitalism: the Fight for the Future at the New Frontier of Power*, Profile Books, 2019.
- [27] Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Hafen Ernst, Michael Hagner, Yvonne Hofstetter, Jeroen Van Den Hoven, Roberto V. Zicari, Andrej Zwitter, *Will democracy survive Big Data and artificial intelligence?* in: Dirk Helbing (Ed.), *Towards Digital Enlightenment*, Springer, Cham, 2019.
- [28] F. Bastiat, *The Law*, Foundation for Economic Education, Irvington-on-Hudson, 1998.
- [29] A. Tocqueville, *Democracy in America*, The Library of America, New York, 2004.
- [30] J. Locke, *Two Treatises of Government*, Hafner Publishing Company, New York, 1969.
- [31] P.M. Regan, Privacy as a common good in the digital world, *Inf. Commun. Soc.* 5 (3) (2002) 382–405.
- [32] S. Barrett, *Why Cooperate? the Incentive to Supply Global Public Goods*, Oxford University Press, 2007.
- [33] 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.
- [34] R. McMillan, *Not on a Social Network? You've Still Got a Privacy Problem*, (2018, January 15) Retrieved from <https://www.wired.com/2014/10/privacy-friendster/>.
- [35] George Orwell, *Harcourt inc*, New York, 1949, p. 1984.
- [37] A.F. Westin, *Privacy and Freedom*, Athenum, New York, 1967.
- [38] M. Coeckelbergh, *Technology and the good society: A polemical essay on social ontology, political principles, and responsibility for technology*, *Technol. Soc.* 52 (2018) 4–9.