Technology in Society 68 (2022) 101854

Contents lists available at ScienceDirect

Technology in Society

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

The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security

Henrik Skaug Sætra

Østfold University College, Remmen, 1757, Halden, Norway

ARTICLE INFO

Keywords:
Privacy
Liberty
Freedom
Security
Social contract
Utilitarianism

ABSTRACT

A recurring question in political philosophy is how to understand and analyse the trade-off between security and liberty. With modern technology, however, it is possible to argue that the former trade-off can be exchanged with the trade-off between security and privacy. I focus on the ethical considerations involved in the trade-off between privacy and security in relation to policy formation. Firstly, different conceptions of liberty entail different functions of privacy. Secondly, privacy and liberty form a complex and interdependent relationship with security. Some security is required for privacy and liberty to have value, but attempting to increase security beyond the required level will erode the value of both, and in turn threaten security. There is no simple balance between any of the concepts, as all three must be considered, and their relationships are complex. This necessitates a pluralistic theoretical approach in order to evaluate policymaking related to the proposed trade of privacy for security.

1. Introduction

A recurring question in political philosophy is how to understand and analyse the trade-off between security and liberty [1–4]. With modern technology, however, it is possible to argue that the former trade-off can to a certain extent be exchanged with the trade-off between security and *privacy* [5,6].[1] One way of doing so is to argue that surveillance-based technology allows us to combat phenomena such as terrorism and disease without necessarily sacrificing liberty. I will challenge this conception by examining a variety of connections between liberty and privacy. The focus of the article is to highlight the ethical considerations involved in the trade-off between privacy and security, as these are highly relevant for policy formation in modern liberal democracies. A particular emphasis is placed on how this trade-off is connected to the traditional trade-off between liberty and security.[2]

I begin by examining two examples of how privacy can be sacrificed in order to gain security: Counter-terrorism based on widespread surveillance and contact tracing used to fight a virus. However, privacy is a rather abstract term, often misunderstood, and the arguments in favour of trading it for innovation, effectiveness, and *security*, are often both easier to state and to sell to the public than arguments for preserving privacy [10]. Therefore, we must first establish privacy as a concept, and explain its connection to surveillance.

The next step is an examination of the relationship between privacy and liberty. Like privacy, liberty is also a concept which is somewhat difficult to define, and a wide set of conceptions of liberty have historically been, and are still, employed – often with insufficiently established definitions [11–13]. By focusing on three main conceptions of liberty – negative, positive, and republican – I show how privacy performs different functions depending on what conception of liberty one adheres to [11,14]. By examining these functions, I further establish that only a somewhat caricatured version of negative liberty – often labelled *neoliberal* – actually supports the idea that privacy can be sacrificed without a non-trivial loss of liberty.

Lastly, the various functions of liberty are considered in light of a set of political theoretical perspectives in order to highlight the ethical implications of sacrificing privacy for security. These are the social contract, value pluralism, and utilitarianism. By examining the issue at

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

[1] Modern technologies are not new, as suggested by references to works released in 1967 and 1982. The mechanisms involved in modern information technology have partially been understood and analysed for a long time, but the availability and spread of these technologies in today's society make the issues even more pressing than before [7].

[2] A key related question which is beyond the scope of this article is the question of how to limit and control a government provided with broader executive powers, and the problems associated with such powers [3,8,9].

https://doi.org/10.1016/j.techsoc.2021.101854
Received 2 December 2020; Received in revised form 6 December 2021; Accepted 30 December 2021
Available online 4 January 2022

hand through these theoretical lenses and the previously established relationship between liberty and privacy, I argue that the relationship between the three concepts is non-linear and complex. The examination suggests that, up to a certain level, security promotes and is a precondition for effective liberty, and that too little liberty *or* privacy can reduce security. Furthermore, liberty requires a certain amount of privacy, and too much privacy *or* liberty also involves a risk of reducing security. These considerations are established by adhering to a pluralistic approach to privacy, liberty, *and* other social values, and this article thus constitutes the foundation of a framework for evaluating the ethical implications of new technologies promising to provide security by a reduction of privacy.

2. Using privacy as a currency to purchase security

First, I will examine how technology can increase security by reducing privacy, and I limit my discussion in two ways. Firstly, I focus on security as the absence of physical or biological threats, in particular the degree to which I am not subject to the violence of others, or to the dangers of disease.[3] Secondly, I examine technology that leverages personal information to increase security, without involving the direct use of physical or legal interference with individual's actions. These delimitations are imposed in order to highlight a particular kind of technology which is especially relevant in modern society, and which enables us to understand the ethical implications involved in trading privacy for security.

I use two stylised examples to illustrate the kinds of technologies I consider. Firstly, the use of contact tracing apps to combat the spread of disease. Secondly, the use of surveillance to combat terrorism. I will develop these two examples in an idealised manner which highlights how technologies can effectively increase security by reducing privacy, and why their implications for liberty are not straight forward. However, before establishing the mechanisms involved in trading privacy for security, it is necessary to establish an understanding of privacy as a concept.

2.1. Surveillance and the many facets of privacy

As privacy is considered the price paid for security, privacy must be defined, along with the closely related concept of surveillance. My starting point is an admission that privacy is difficult to define, and, in a sense, a "concept in disarray" [5,10,15]. Some mainstream conceptions of privacy are *the rights to be let alone, limited access to the self, secrecy, control over personal information, personhood,* and *intimacy* [16]. Focusing on the security technologies outlined below, the most relevant conceptions are related to privacy as a) a space in which one can be unobserved, and b) control of information about oneself [17]. The first relates to privacy as *boundaries*, as highlighted by Scanlon [18]. The second is less concerned with the act of observation, but emphasises individuals' abilities to *control* who does what with their personal information. This understanding is related to the claim of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others" [5,6]. It is also related to Allen's [19] conception of privacy as consisting partly of *proprietary* privacy, as it concerns information about our private property, which includes ourselves just as much as our material belongings.

Privacy in the following will refer to some form of withdrawal from the public – inaccessibility – and is characterised by being voluntary and temporary [5,19]. Both being able to restrict observation and the control of information if observation occurs is considered relevant.[4] Privacy can also increase or decrease gradually, which means that you can have, or sacrifice, a little privacy.

One could, like Warren and Brandeis [22], give privacy the status of a right. This is called normative privacy [17]. I will, however, initially follow Scanlon [18] and Thomson [23] in not regarding privacy as a right per se, but as something which is valuable because of its consequences. The value of privacy, particularly as it impacts liberty, will be the focus of section 3 of this article, and privacy as such will until then be considered a neutral concept without intrinsic value. This enables me first to examine the instrumental value of privacy, before I in section 4 proceed to also consider privacy's possible value as a right, and privacy as potentially intrinsically valuable.

2.2. Contact tracing and personal movement data in a pandemic

An infectious and serious disease is a potential threat to security. In a society with uncontrolled infection, people feel exposed and experience a lack of security in public if they experience a non-trivial risk of being infected with a disease and falling ill. COVID-19 is a ready example, in that it is both highly contagious and involves a risk of serious physical debilitation. While the chances of young people falling seriously ill is not great, the odds are considered to be non-trivial. If we also consider the risk of transmitting the disease to family members and others with a higher risk profile, it seems uncontroversial to consider the possibility of being infected to be a seriously undesirable outcome. Furthermore, research on the various long-term effects of the virus, often referred to as "long covid", also highlight the need for a precautionary approach and an acknowledgement that we do not fully understand the full risk of being exposed to COVID-19 [24].

During the COVID-19 pandemic, mobile applications (apps) with contact tracing functionality have been released and become the object of controversy in a number of countries [25]. Norway's "Smittestopp", Ireland's "COVID tracker", and Singapore's "TrackTogether" are just three examples [26–28]. As the principle of gaining security by a sacrifice of privacy is the focal point of the current undertaking, we will consider a hypothetical app which represents a generalised example of such apps.

Assume that the app is based on the idea of contact tracing and anonymised collection of movement data for disease control research purposes. Let us furthermore assume that the app runs on mobile phones, and that installing and using it is made mandatory. This latter assumption is introduced in order to consider an extreme case of the technology, which more easily enables us to see the implications for both liberty and security.[5] With this assumption, the trade-off between privacy and security is not an individual choice, and since the app is mandatory it will be maximally effective in providing security.

The main function of the app is contact tracing. By using a sensor (preferably) in each phone, all our devices will be capable of registering accurately whenever someone is closer than, for example, 1 meter, over a duration of, say, 30 seconds or more. This will be defined as "contact", and each contact will be stored for 14 days. Contact information is only stored locally on the user's phone and we here assume that it is not accessible by the government.[6] Whenever a person tests positive for the disease, everyone who has registered contact with this person will be notified through the application that they are at risk, and will be

[3] This is an intentional and necessary simplification of what the term *security* might entail, as discussed in detail by Waldron [4]. I mainly adhere to what he calls the "pure safety conception" of security, while extending it somewhat in terms of breadth in order to include both objective threats and subjective fear of assumed threats [4].

[4] There is also a tension between the two, which will not be discussed in detail. People may, for example, have an expectancy of being able to control information about acts performed in public [20,21].

[5] Israel, for example, introduced law that enabled the government to retrieve phone data from people suspected of being infected [29].

[6] This is a decentralised app, and the choice between centralised and decentralised apps has become a central question in debates about how to most effectively combat COVID-19 with contact tracing apps [25].

encouraged to schedule a test. In addition, the app sends anonymous location data to the government. This is done to facilitate effective research on movement patterns and the spread of the disease, in order to inform policy making and to evaluate the effectiveness of current and potential restrictions.

If we assume that the app is maximally effective, infections will be tracked, and uncontrolled infection will be substantially limited. Sick, and potentially sick, people will be tested and quarantined more effectively, and the location data will also support government efforts to introduce effective and minimally intrusive restrictions on behaviour and activity. The benefits and assumptions made are conceivable, but they are also controversial, and certainly debatable [25]. *If* these assumptions are accepted, the app could help reduce the spread of the virus. This, in turn, would increase security.

According to the preceding definition, however, people's privacy would also be reduced. They will be under a form of surveillance, and will not be able to restrict observation or make themselves fully inaccessible. This applies mainly to privacy from the authorities, and potential "snoopers" [28]. The observation would, however, be strictly limited to location data and contacts. The only information transmitted from their devices would be anonymised movement data, and thus not personal information of which control is relevant to privacy. We will also assume that reverse identification will be prevented by appropriate measures of anonymisation. This app clearly shows why the two characteristics of privacy are both necessary to capture the breadth of the concept. If our only concern was control of personal information, an app such as the one described would not reduce privacy at all if the information was fully anonymised, properly secured, and if contact information was only handled locally on the device, and anonymously between devices. Only the user of the app would get notified if one of their contacts tested positive.

Tavani and Moor [17] criticise notions of privacy that only focus on control, and this is one example of why one might raise such objections. The user of the app *is* observed, but as long as no one can make use of that information without the user's control, privacy is intact according to the control-based view. A related idea is the suggestion that the determining aspect of whether or not privacy is breached is determining if there is human judgement involved in handling the data collected [6,20]. Solove [20], for example, argues that surveillance is only associated with the negative effects of "conformity, inhibition, and self-censorship" when human judgement is involved. Such a view implies that it is the *effects* of observation that matter, and not some right, or disinterested desire, not to be unobserved.

If we see privacy as the boundary that stops others from observing us, privacy is lost with the app in question, no matter how the information is used – or not used. The simple fact that I cannot escape observation reduces my privacy. One reason to hold such a view is that the effects of surveillance are not necessarily the result of who observes. I have previously argued that that what matters is the results that occur in the one being observed, and that inhibitions and restraint may easily be the result of merely being observed, regardless of who – or what – watches [30]. I proposed the argument that observation, due to the fact that deliberate surveillance breaches the boundary that is privacy, changes behaviour and involves the exertion of a kind of power. These kinds of effects are shown in how, for example, the mere presence of a *poster* with a pair of eyes will reduce anti-social behaviour, and these negative effects are often referred to as chilling effects [6,31]. Observation can thus be construed as undue interference, a concept to which we will return in section 3 [30].

2.3. Surveillance and counter-terrorism

A different, and far broader, mechanism for trading privacy for security involves counter terrorism and comprehensive surveillance. Surveillance can be defined as purposeful "focused, systematic and routine" attention [32–35]. This is called *strategic* surveillance, as it involves a clear goal [32–34]. Both of the examples discussed in this article involve technologies and strategic surveillance aimed at achieving a clear purpose – less disease and less terror. Less focused forms of surveillance, such as those encompassed by Macnish's [32] surveillance as simply "sustained monitoring of a person or people", will not be considered specifically here. Furthermore, surveillance can be focused on particular persons, or it can be undirected and general. The first is *direct* surveillance and the latter is *indirect* [5].

Massive amounts of data are today collected, analysed, and used to gain insight into various aspects of human affairs, and this is one reason why many name our current age the era of Big Data [36–38]. The example of counter terrorism involves leveraging Big Data to prevent and combat terrorism in general and terrorist attacks in particular [37]. Terrorist attacks create insecurity, and terrorism is often discussed in relation to the trade-off between security and liberty in the aftermath of terrorist attacks. For example, in relation to 9/11 in the US, or the terrorist attack perpetrated July 22nd' 2011 in Norway [8,9,13,37,39,40]. Firstly, fear is instilled merely by contemplating the possibility of terrorist attacks, and this is often assumed to be the main goal of terrorists [4,39,40]. Secondly, the possibility of terrorist attacks also constitutes an actual risk of physical violence. It represents what has motivated Hobbes [1] and others to justify government, namely the "continual fear, and danger of violent death".

As in the case of a pandemic, I employ a generalised and somewhat extreme example of the use of technology to gain security. It is not a fictitious example, however, as we can consider the US Department of Defense program *Total Information Awareness,* revealed by the media in 2002 [10]. Solove [10] describes the program as based on massive data mining. The government collects extensive personal information (financial, educational, health, etc.) in order to analyse this data for insight into behaviour patterns that let them understand and identify terrorists. When uncovered, the program caused massive protests, and was subsequently defunded. However, various aspects are continued in a less unitary form by a set of government agencies [10].

The logic behind the program was that enough information gives us access to deep patterns of behaviour, and by understanding past patterns, we can predict and prevent future undesirable acts. I [30] differentiate between three forms of observation, namely *passive observation*, *active observation,* and *surveillance proper*. While passive observation is observation that cannot subsequently be used in any way, *active* observation enables the surveillant agent to use the data gathered retroactively, for example as proof in a criminal case. The surveillance discussed in the example of counter terrorism, however, involves the *pro*active use of information in order to avert or prevent attacks perceived as likely to occur in lieu of intervention. This is called surveillance *proper* [30]. Counter terrorism post 9/11 is often associated with this form of surveillance, with the increased emphasis on pre-emptive rationales in the aftermath of the attacks [8,9].

We will assume that the surveillance employed is indirect, in that the government gathers information on everyone – not just those who give rise to suspicion [6]. The kind of information gathered is much more extensive than the information gathered by the contact tracing app. We might assume here that all sorts of personal data are stored and available for inspection when the need is perceived to arise. The upside, however, is that we will also assume that this surveillance will be effective – at least to some non-trivial degree. We will assume that such surveillance will help government agencies to uncover certain forms of terrorist planning. With wide ranging authority to collect, and parse information about those involved – their persons, relations, and communication – surveillance proper enables the prevention of that which gave purpose to the program itself: Terrorism. Security could in theory be gained, by sacrificing privacy.

This example involves a clear-cut reduction of privacy, as all will be observed, *and* none will retain full control over how this information is subsequently handled and used. All are potentially observed, at all times. Even if a person has nothing to hide, their information will be

collected, and it may be employed in various ways, by chance, by random checks, or by the fact that the information is perceived as relevant because it in some way relates to data about *other* persons of interest.

3. Liberty and the function of privacy

Having established that privacy can be used as a currency by which we can purchase security, the next question is how this relates to *liberty*.[7] As will become clear, this requires us to define liberty and explain how it relates to privacy. However, instead of seeking a universal and ideal definition of liberty, I work from a position where multiple valid understandings of liberty are recognised. I will first briefly establish a set of mainstream conceptions of liberty, before proceeding to consider the various functions privacy holds according to these different conceptions.

3.1. The many shades of liberty

The discussion of liberty is partly based on Isiah Berlin's seminal lecture, "Two Concepts of Liberty" from 1958, along with the introduction he added to it as he updated it in 1969 [41,42]. His division of liberty into two distinct forms has been widely debated in the years that followed its publication, as philosophers have both come to Berlin's support and sought to correct the mistakes they believe he made [12].[8] In addition to Berlin's two original concepts, I will examine other influential forms of liberty argued to be neither negative nor positive, notably by considering contributions from Pettit [14], Raz [45] and List and Valentini [13]. As the main purpose of this analysis is to elucidate the relationship between liberty and privacy, it is not a full consideration of what liberty is, but an examination of liberty as far as it relates to privacy.

Value pluralism is an important part of Berlin's philosophy, and one which I will also base my analysis on [42,46]. Despite Berlin himself having rather clear perceptions about which form of liberty he preferred – or considered least dangerous – he also explicitly states that the two forms of liberty represent different facets of liberty, and that they are both legitimate and valuable. I follow this approach, in order to allow for different views of what liberty is, and thus of what the value of privacy is, to be considered in the examination of policy making implications. This pluralist approach is distinct from, for example, the one of List and Valentini [13], who argue in favour of finding the "right" approach to liberty. While the analysis is restricted to policy making in liberal democratic societies, this still allows for a broad range of ethical theories, values, and perspectives to be considered.[9]

Negative liberty is determined by "the degree to which no man or body of men interferes with my activity" [41]. It involves a consideration of the extent to which a person might *act* unobstructed and without interference, and is explicitly devoted to seeing as obstructions and interference only that which can be traced back to other persons. It is found by answering Berlin's question of what area a person has to act without interference by others, and to do the things they could do if no person hindered them [41].

If we ask a different question, aimed at discovering *what*, or *who* "is the source of control or interference" that determines what a person can do – or *be* – we are in the realm of positive liberty [41]. Positive liberty entails an emphasis of self-mastery, and instead of focusing only on external obstacles and interference, it turns the spotlight to internal obstacles, processes, and control [41,49].[10] While Berlin notoriously excluded a consideration of the conditions of liberty when considering how much negative liberty a person has, the notion of *effective* liberty is an integral part of positive liberty [46]. Positive liberty does not merely consider what sort of interference I am free from, but emphasises both what options and alternatives I have and whether or not I have the power to make use of them [46]. In other words, what I am free *to* do, as opposed to merely what I am free *from*. As the notion of self-mastery suggests, positive liberty entails a consideration of a person's internal processes and autonomy, and not only the person's physical and procedural liberty to act.

While these two conceptions are clearly different, there is some overlap between them, as Berlin also recognises [41]. Still, the two concepts have left certain things to be desired, and several philosophers have proposed positions that are argued to be situated *between* other concepts of liberty. One is republican liberty, often associated with Pettit [14] and Skinner [51]. Next is liberty as independence [13]. Lastly I will briefly mention liberty as autonomy [45]. The theories are chosen according to their usefulness in highlighting the aspects of liberty that are especially relevant to elucidate the functions of privacy.

Republican liberty is examined through Pettit's [14] liberty as *non-domination*. He explicitly states that he sees this form of liberty as an intermediary position between positive and negative liberty. It is negative by emphasising non-interference, but it is more than this, by emphasising that it is not only actual interference that matters, but whether or not individuals are protected from *potential* interference [14]. If someone has the power to arbitrarily obstruct and interfere with you, but for a time chooses not to, you are still in a state of domination according to this theory. This is a crucial point with regard to the need to be wary of surveillance and a lack of privacy – not just due to a scepticism of the motives of those in power, but because it generates the conditions of domination and unfreedom. This is similar to Hobbes's reason to object to the state of nature, where the *possibility* of war, and not constant acts of war and violence, is considered the main problem [1]. This line of thinking is also employed in the area of security, as Waldron [4], for example, emphasises the assurance of security.

Closely related to republican liberty is liberty as independence, which is stated to be positioned between Berlin's negative liberty and Pettit's republican liberty [13]. While agreeing with Pettit that we need protection from potential interference, List and Valentini disagree with proponents of republican liberty in the latter's emphasis on freedom from *arbitrary* domination. In order to better capture a) all situations of liberty reduction in need of justification, and b) common language usage of the word freedom, they believe that also any nonarbitrary liberty reduction must be seen as a loss of liberty [13]. A prisoner justly imprisoned will thus be deprived of liberty according to liberty as independence, but not, List and Valentini [13] argue, necessarily according to republican liberty. Liberty as independence is thus a non-moralised conception of liberty (as Berlin's negative liberty), and as I work from a pluralist position, this theory allows us to evaluate all sorts of liberty, and not just the liberty that has already been deemed desirable.

Finally, there is the idea that liberty is intimately connected to autonomy. In Joseph Raz's [45] *The Morality of Freedom*, we see that liberty can be understood as dependent on *autonomy*. This requires that a

[7] Liberty and freedom are used interchangeably throughout the article.

[8] Two early notable critiques of Berlin's dichotomy are provided by Maccallum [43] and Taylor [44].

[9] On the other hand, a lot of nuances and different conceptions of liberty will not be addressed specifically, such as the contextualisation of Berlin's liberty, "ancient" liberty and freedom, liberty as democratic self-rule, etc. [47,48].

[10] Berlin's positive liberty has been heavily criticised, amongst other reasons for conflating different ideas in a way that reduces the usefulness of the concept [50]. However, I use the term in Berlin's general meaning, and will mainly use it to show one important function of privacy, and not in order to condemn a broad array of social theories (as it could be argued that Berlin did).

person is "part author" of their own life, and that we do not only care about what a person and their lives are right now, but also about "the way it became what it is" [45]. This is related to Berlin's division between an empirical and authentic self. The first entails whatever a person is, whereas the latter involves a consideration of what a person *could* be [41]. Conceptions of liberty that include considerations of the authentic self are usually considered to be varieties of positive liberty, and the reason for singling out Raz's theory is his development of the *conditions of autonomy*, which are "appropriate mental abilities, an adequate range of options, and independence" [45]. The first condition will not be discussed here, and the second is discussed below in relation to negative liberty. The third condition is relevant to the value of privacy, as independence might require a certain level of privacy. Independence in this sense, which must be distinguished from the independence of List and Valentini [13], requires the freedom "from coercion and manipulation by others" (Raz, 1986, p. 373).

3.2. The function of privacy

With these preliminary conceptualisations of liberty in place, we can begin our examination of the function of privacy. I will first consider negative liberty and how this conception may, but need not, be considered as distinct from privacy. Moving on to positive liberty, I highlight how privacy can be considered a key precondition for liberty, and thus part of what we will call effective liberty. Lastly, privacy's function as a safeguard against domination and bulwark against encroachments on autonomy and independence is considered.

3.2.1. Privacy as distinct from liberty

Negative liberty can be argued not to be negatively affected by changes in privacy. With a minimalist interpretation of negative liberty, only human interference that changes the alternatives of action available to a person will be considered liberty reducing. By this account, the mere fact of being observed has little consequence for liberty. This implies that it is important to distinguish between objective and subjective privacy, as the one might make me unfree under surveillance, whereas the other might not. Berlin [41] famously emphasised, as did Bishop Butler, that "everything is what it is", and not something else [4]. He insists that liberty must not be conflated with justice, equity, or the conditions of liberty in general. We could add that it must not be confused with *privacy*. This allows for a position where surveillance reduces *privacy*, while leaving liberty untouched, as I am as free to act as I was without surveillance.

While this is a fairly traditional account of negative liberty, it is too simple. I have previously argued [30] that observation can *change* and *interfere with* our actions, and that it can thus be construed as a form of interference when performed by other humans. Conformity, inhibition, and self-censorship, as mentioned by Solove [10], are phenomena that occur in the person observed, and if they are caused by other people and change our actions, this might be considered as interference. Another way in which a reduction of privacy might reduce negative liberty is if it is positively harmful. Warren and Brandeis [22] argue that privacy incursions can cause pain and distress "far greater than could be inflicted by mere bodily injury". If this is accepted, it would be reasonable to argue that such harm caused by others is a form of interference and liberty reducing if intended to change our actions. It seems unlikely, however, that all forms of surveillance are this problematic, and few have reported, for example, such degrees of pain and distress from using contact tracing apps.

Furthermore, whenever surveillance is mandatory, or covert, it is liberty reducing by being forced upon us [30]. Even if surveillance is not made mandatory by law, it can be so pervasive that opting out becomes prohibitively costly, and not a real alternative [25,30]. If privacy is construed as a right, surveillance can be a violation of this right. But even if privacy is not a right, forced observation reduces a person's freedom of choice, and thus liberty. The latter account is, however, somewhat problematic. It requires us to be willing to evaluate the worth of available alternatives, and thus take a *perfectionist* position on liberty which involves that some liberties are worth more than others. Carter [49], for example, proposes a non-perfectionist theory where what he calls overall liberty is simply the number of available actions divided by available *plus* unavailable actions. Under forced surveillance, I lose the alternative of acting unobserved, but I gain the option of acting under surveillance. If we refuse to value the former higher than the latter, liberty is untouched by such a swap [30].

In sum, negative liberty shows that if liberty is exclusively focused on action, being observed might not have an effect of liberty. This is particularly true if the person being observed is unaware of the observation. In such a case, no self-censorship or similar phenomena would occur, and the person's actions would not change as a result of the observation. The person would feel as free as if under no surveillance, and would thus *be* free in this sense. This paradox, where surveillance seems *more* amicable to liberty if covert, is only resolved when we later discuss liberty as non-domination. However, we have seen that overt and mandatory observation and surveillance could be argued to have negative effects also on negative liberty. The contact tracing app might be liberty reducing in being mandatory, and the privacy lost by being observed by the app *could* be argued to constitute a form of interference by how it changes my actions. It might, for example, prevent me from seeing people or visiting places that I was particularly worried that others might observe, even if others do not in reality have the means to observe, judge, or use the results of the observation. Widespread surveillance carries the same risk, to a higher degree, as it entails that all will be aware that their every movement, action, and communication might be observed.

3.2.2. Privacy as a precondition for liberty

One central aspect of Berlin's negative liberty is that he separates it from the conditions of liberty [42]. This move has been heavily criticised by a range of authors, who argue that it makes little sense to speak of liberty without an eye to what is often called effective liberty [46]. Effective liberty combines the alternatives available to us with our power to actually make use of these alternatives. For example, me having the formal rights to purchase the food I need is inconsequential if I have no means to actually make these purchases [46]. Under negative liberty I would have, formally, the freedom to buy food, but effective liberty, which is introduced in positive liberty, requires that I also have the power to make use of these actions if they are to be considered as liberties.

Self-mastery is related to autonomy, and autonomy, according to Raz [45], requires, for example "appropriate mental abilities". This again can be related to what Berlin [41] describes as the "minimum area" of liberty required to develop faculties and skills required to live our lives in an autonomous manner. Nissenbaum [52] similarly states that privacy is required for providing the "necessary conditions for formulating goals, values, conceptions of self, and principles of action". Privacy, in other words, is a part of the preconditions of liberty, in that it is an integral part of societies "which support social forms which … leave enough room for individual choice" [45]. With the positive conception of liberty, we can argue that privacy has a key function as a precondition for developing a self that has the capacities required to be described as *free*.

It is also worthy of note that positive and negative liberty can be seen as a difference in perception of liberty arising from fundamentally different ways of understanding individualism, and the self. Privacy as a concept is something that depends on being able to see an individual as separated from its social setting, and Berlin [41] notes that negative and individual liberty is what has given privacy the meaning and value it now holds. This, then, could imply that seeing the individual as a deeply social being, and the self as socially constructed and individuals as socially situated, involves stripping privacy of any value. Raz [45] and Julie Cohen [33] are amongst those that reject pure individualism, but

they certainly do not deny privacy's value.

In "What privacy is for", Cohen [33] provides a strong argument for the value of privacy based on a non-individualist account of the self. She argues that negative liberty and a neoliberal conception of the self is incapable of showing the true function of privacy, which according to her is that it "enables individuals both to maintain relational ties and to develop critical perspectives on the world around them" and it allows for the development of subjectivity [33,53]. It is, however, worth noting that she never argues that observation *in itself* is a problem, and privacy is thus mostly important because of the role it plays in creating a particular kind of safe place in which to develop. A situated and social self will always be observed, and it depends fundamentally on both seeing others and being seen and recognised. However, some space must be preserved even between what she labels a "post liberal self" and those around it. One reason for this appears to be quite utilitarian, in that the subjectivity that is developed under privacy helps "ensure that the development of subjectivity and the development of communal values do not proceed in lockstep" [53]. Wachter and Mittelstadt [54] and Zarsky [55] similarly point to the role privacy plays in protecting individual personality, and that data driven inferences based on a lack of privacy threaten identity and self-determination.

The main function of privacy under positive liberty, then, could be described as a precondition for developing a capacity for self-determination and self-development – both which can be argued to be required for self-mastery [33]. While positive liberty in general is often associated with political rationalism and paternalism, the function of privacy as it is presented here can be seen as a *barrier* to the more problematic varieties of positive liberty. Berlin [41] feared the proponents of positive liberty, such as Rousseau [56], who argued that a person could be "forced to be free", by coercing them to pursue the goals of their authentic rather than their empirical selves. A form of positive liberty that conceives of self-rule as rule based on being able to develop in private is, however, distinct from this position.

While observation in itself is not perceived as problematic with a positive conception of liberty, it becomes deeply problematic if it penetrates too deeply, or into the core areas in which a person develops. Preventing individuals from being unduly affected by society, then, requires us to restrict certain forms of observation, and the overall surveillance pressure a person experiences. It seems likely that contact tracing apps would raise relatively few objections from proponents of such a view, while deep surveillance could be perceived as highly problematic. The latter would penetrate deeply into all areas of a person's life, and would not leave individuals with that minimum area most seem to agree on as a requirement for being free in the positive sense of the concept. A key difference between negative and positive liberty is that positive liberty enables us to make a clear distinction between the threat of personal data consisting of rich psychological data and, for example, simple recordings of our movements.

3.2.3. Independence and privacy as a safeguard against domination

The final function of privacy is to provide a bulwark against domination. Liberty as non-domination solves a problem sometimes connected to negative liberty, which is that liberty under a liberal and benevolent dictator could be said to be characterised by high levels of negative liberty. The case of the "free" slave with a benevolent master is another frequently used objection [13]. This problem is rectified when we introduce Pettit's [14] requirement that the liberty we have is also safeguarded.

Privacy is a safeguard in several respects, and I focus on three main varieties here, which will subsequently be elaborated. Firstly, privacy makes it easier to hide certain aspects of our lives and movements, which in turn makes it harder to exercise precise physical authority over us. Secondly, privacy prevents others from collecting information about our mental lives, which would in turn enable them to exercise psychological force over us. Thirdly, privacy prevents the collection of personal data, and thus simultaneously reduces the amount of personal data in existence, which in turn reduces the risks of personal data changing hands, being stolen, etc. [6,30]. These aspects of privacy are highlighted by Véliz [57], who discusses privacy as a form of power. When we have privacy, we have power; when we don't, others have power over us.

Traditionally, the threat of surveillance has been connected to government and its monopoly on the use of physical force in a society, while modern surveillance is usually considered a phenomenon involving government *and* private companies – often in cooperation [25,30,33]. I restrict my analysis to government surveillance, as this most clearly relates to the examples in question, and allows for a necessary delimitation of the article.

Liberal theory is premised on the notion that we cannot and should not trust government, but rather make sure to create institutional barriers that limit the government's chances of infringing upon the rights of individuals. Following such an approach, a refusal to trust government entails a scepticism of surveillance and the need to protect privacy, as we would otherwise be left more vulnerable to the abuse of power. Many modern societies are, however, characterised by rather high levels of trust between citizens and the government, and the Nordic countries are examples of how such trust can facilitate less scepticism towards government efforts to use, for example, personal health data to promote the public good. However, it may be precisely when we *do* trust government that we should be most wary [40]. The main idea behind republican liberty is the "escape from the arbitrary", and not being subject to the "capricious will" of others [14]. List and Valentini [13] point out the problematic nature of focusing on arbitrary power, and suggest that we focus on liberty as the absence of both arbitrary and nonarbitrary sources of domination. This would include seeing a legitimate government as liberty reducing, and Carter and Shnayderman [58] have criticised the theory for making unfreedom ubiquitous and consequently the concept of freedom useless. The shared focus on a robust protection against potential abuse of power unite the two theories, and is also the most relevant insight in this context. While privacy in itself will not solve the problem of potential abuse of power, it denies those with the potential to dominate us access to our personal information. This deprives them of some power, and it also enables more effective resistance against their power, as it will be easier to organise opposition with a certain level of privacy [57]. Lack of privacy has a chilling effect on "social and political mechanisms of change", and thus leaves those in opposition with fewer legitimate and non-violent means to explore their opposition [3,9].

Secondly, I have argued [59] that detailed personal information can be used to manipulate and coerce in ways that are inimical to liberty. By surreptitiously using in-depth knowledge about a person's psychological weaknesses and proclivities, it is hypothetically possible to coerce a person into acting in certain ways without them being aware of this, and such coercion is construed as interference by use of psychological instead of physical force [59]. Privacy prevents others from collecting the information required to exercise such force, and thus constitutes a barrier against domination [57].

Finally, the mere existence of personal data constitutes a risk. While we may trust our current government, power may change hands. While we might trust a certain company, they may sell the data, or be subject to a merger or hostile takeover [57]. Also, data could quite simply be stolen, and end up in the hands of someone with either the physical or psychological power to dominate us [6]. Privacy serves as a safeguard against all such forms of domination by reducing the amount of personal data in existence. Finally, while personal data does not constitute a risk today, it is in principle lasting, and we have no guarantee that new and objectionable ways of using, or abusing, the data we voluntary give away today will not be invented tomorrow. As such, privacy is also a safeguard against unknown future forms of domination [30]. This latter point can be explained with the concept of modal robustness. List and Valentini [13] argue that a modally robust conception of freedom emphasises that liberty must be protected not only in the actual world, but also in a "range of nearby possible worlds", one of which might have a

different head of government, different boards of major companies, and even new technologies.

3.3. Key relationships between privacy and liberty

The preceding considerations have uncovered several key connections between the concepts of privacy and liberty. Negative liberty lets us see that privacy could be considered to be a possible choice or a right, and that liberty is reduced by forcefully removing it. It is also possible to see observation and lack of privacy in itself as a form of interference that affects individuals' actions. The positive conception of liberty lets us see that liberty might be required for providing people with a minimally large area in which to develop their fundamental faculties as human beings – their selves – in order to become beings capable of autonomy and liberty. Lastly, liberty as non-domination shows that privacy performs key functions related to safeguarding individual liberty, and preventing others from having power to arbitrarily dominate us – regardless of their actual intent or plans to do so.

4. Framing the trade-off between liberty and security

Having established that security can be bought with privacy, and that privacy has various functions related to liberty, it is time to consider the ethics of trading privacy for security. As the focus of this article is on the ethical considerations related to policy formation, the question is examined in light of three key theories from political theory. Firstly, the social contract with its perennial focus on trading liberty for security. Secondly, pluralism, liberalism and democracy as key factors in the examination of whether, or how much, privacy can be traded, and how to answer these questions. Thirdly, utilitarianism and the consideration of consequences.

4.1. The social contract and the danger of absolutes

The first step is to decide if we can ever use the desire for security as a reason to ask people to sacrifice other values, such as liberty or privacy. This is the foundational question of political legitimacy, and the social contract tradition provides one possible answer to this question.

According to Thomas Hobbes [1], individuals have by nature been provided with absolute liberty. Our *natural rights* and liberties are limitless, and in what he refers to as the statue of nature, people have absolute freedom in the sense that they have the right to everything. This, he states, leads to major problems because of three phenomena. First, many important goods are scarce goods (competition). Second, we tend to be uncertain regarding the motivations of other people and thus fear what they might do (diffidence). Third, we have a desire for other people to value us as highly as we value ourselves (glory). The latter is a problem because they *will* not generally value us as highly, and this will, along with the other two factors, lead to conflict [1]. With absolute liberty, life is, according to Hobbes, plagued by "continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short" [1]. As none of us desire such a situation, Hobbes argues that we should, and would, all agree to trade our absolute liberty for *security*. If related to terrorism, we are united by the fact that "nobody wants to be blown up" [4]. We would erect government, and transfer our rights and liberties to it in order for it to protect us [1]. One way of seeing this trade-off is to see security as a means to obtain liberty [4].

The problem, however, is how to control this government. For, just as absolute liberty is misery, others, as Andrew Hamilton in 1735, argue that "without liberty, life is misery", and that the "loss of Liberty to a generous Mind, is worse than Death" [60]. Other social contract theorists, without going to such extremes, have proposed social contract theories in which liberty *is* sacrificed for security, but in which individuals take great care to retain a great deal of liberty, and the opportunity to rebel against abusive government. John Locke [61] did so not long after Hobbes, and Robert Nozick [2] presents a similar and more modern theory. While Hobbes, Locke, and Nozick might all to a certain degree be considered proponents of a negative view of liberty, Rousseau [56] is a social contract theorist known, as we have seen, as a proponent of positive liberty.

The preceding considerations suggest that it is at times legitimate to trade other values for a basic level of security required to escape continual fear and danger of violent death [9]. Berlin [41] himself also stated that such a minimum of "contraction" of liberty was inevitable. Anything *beyond* the minimum, however, is not simply slightly undesirable, but would leave us "coerced, or it may be, enslaved" [41].

4.2. Pluralism and liberal democracy

Building on a basic social contract, it remains to determine how to prioritise all *other* values than the avoidance of death or fear of it. Privacy and liberty are two potential values, and as we have seen, the definitions of these concepts are not easily agreed upon. Instead of attempting to choose which versions of these concepts are best, most appropriate, or should be given priority, I propose basing the evaluation of the trade-off between security and privacy on Berlin's [41] value pluralism. This involves considering different values, priorities, and, for example, conceptions of liberty, as incommensurable values all valid for political consideration.

In addition to letting us consider different perspectives, it involves certain requirements for our political societies. If we consider value pluralism to be a valid representation of the nature of values, society should be organised in a manner that allows different people to pursue different values. This implies that all forms of political rationalism are viewed with great scepticism [62]. While positive liberty is accepted as a potential individual value, this implies that we should not make positive liberty a *political* goal, in so far as this would entail paternalistic policy and an adherence to a goal of actively helping, or forcing, citizens to achieve their "true" or "authentic" selves [48,62]. Pluralism is also compatible with Hobbes's [1] basic political philosophy, which explicitly states that any use of government coercion beyond that which is required for securing peace, is illegitimate.

This implies that coercion to protect privacy could be perceived as illegitimate. Nissenbaum [52] argues strongly in favour of freedom and individual autonomy. While she believes the lack of privacy constitutes "injustice and even tyranny", privacy must be the result of individual choice [52]. Allen [19], on the other hand, suggests that coercion *is* necessary for securing a sufficient level of general privacy in society. According to this view, privacy is a public good, which is susceptible to be underprovided if left to individual choice [19,57,63,64,70].

Also related to pluralism is the importance of context. Different societies can have very different ideas about the value of privacy, liberty, and security, and they will also be categorised by different levels of trust, both between citizens and between citizens and government [6,39]. This implies that any answer to the question of whether a certain danger justifies prioritising security over privacy will to a certain degree be contextually dependent.

4.3. Utilitarianism and the political calculus of trade-offs

Having accepted a pluralism of values, the question of how to balance and prioritise the various values citizens adhere to remains. One possible avenue for answering it is through utilitarianism and the evaluation of the consequences of various policies. With the general framework of the social contract and value pluralism, utilitarianism provides a practical approach to policy making when evaluating incompatible policies and trade-offs are required. Without entering the details of political calculus, problems of defining utility, inter-personal utility comparisons, I simply use utilitarianism to show how and why privacy might be considered to have social value. As such, this provides a starting point for weighing privacy against various measures to increase security. In combination with the social contract, and with a clear

focus on evaluating the positive consequences of individual rights, such consequentialism need not be as problematic as Donohue [3] assumes when she argues that it will "fail to give sufficient weight to the place and complexity of individual rights".

On an individual level, people might experience privacy itself and being able to have an area of their own as valuable. In addition, some will consider privacy to be a right, and they will also perceive rights being respected as valuable [3]. Individuals might also appreciate being able to privately perform actions that others would condemn had they seen them, and this could include both legal but unpopular and unlawful actions. Similarly, privacy might have negative effects for individuals, for example, by hindering the free exploration of our curiosity about others, and by promoting an individualist culture when some prefer tighter social bonds and collectivism. Mill [65] names three principal liberties of central importance: Liberty of thought and opinion, liberty of tastes, pursuits, and planning our lives, and liberty of associating with like-minded individuals. While privacy might be considered conducive for all these liberties, the trade-off is greatly complicated by the fact that both contact tracing apps and surveillance might in fact increase liberty to associate and to act and move about freely. Seeing privacy and liberty separately allows us to avoid conflating measures with quite different implications.

These liberties might be beneficial for individuals, but they also have positive effects for society. For example, individualism and the absence of a majority that wields moral power to encourage conformity and homogeneity might lead to both innovation, growth, and happiness. This moral power, and the associated majority tyranny greatly worried thinkers such as Mill [65] and Tocqueville [66], partly because of individual rights and liberties, but also because of the beneficial effects individualism and liberty have for society [3]. Privacy, as we have seen, is important in providing and securing this. Privacy and choice, Allen [19] argues, is "beneficial to individuals and society", if our goal is to promote "free, democratic, and reasonably efficient forms of life". Waldron [4] also emphasises the importance of securing people's modes of life, and he suggests that this is included in the definition of security.

In addition, privacy can be considered a key condition for promoting the public good and a "certain public culture" considered valuable [45]. This connects fundamentally to the existence of a liberal and democratic society, on which extensive surveillance and lack of privacy have negative effects [3,9,33]. While innovation and liberty might give rise to wealth, a lack of privacy might also be argued to be the cause of economic growth. Zuboff [7] labels capitalism of today *surveillance capitalism*, and emphasises how today's largest companies are based on extracting value from data – *personal* data in particular. In addition, Big Data and artificial intelligence has led to advances in health and, as is the focus of this article, security. By prioritising privacy, we would restrict the possibilities of further gain in these areas. Opposed to these benefit of less privacy is the argument that a lack of privacy and data protection might make businesses wary of operating in such settings [6].

The value of privacy is often not sufficiently recognised, according to Solove [10]. Part of this stems from the fact that privacy has social value, which exceeds the value perceived when we examine privacy exclusively from an individual perspective [9,10]. As the value of privacy is properly recognised, it becomes easier to see how it provides a counterweight to the arguments for sacrificing privacy in order to facilitate innovation, foster economic development, or provide security [10]. As emphasised by Banks [8], we must also calculate the cost of increased executive powers and less oversight, as these will be significant for liberal democracies committed to transparency, checks on power, and the rule of law.

The preceding considerations mainly serve to show that the value of privacy is a highly complicated question, and making the trade-off with security is further complicated by the complex interrelationship between the two concepts. A key point is that while privacy reducing technology can reduce liberty due to liberty's dependence on privacy, it may simultaneously *increase* liberty. The contact tracing app might let the government avoid imposing a lockdown that would dramatically reduce people's liberty in a wide range of areas. Deep surveillance may similarly reduce liberty by a loss of privacy, but not taking advantage of the benefits of surveillance might necessitate other forms of restrictions in order to achieve similar levels of security. We have also noted that privacy is related to a range of other values, and while surveillance capitalism might be liberty reducing by way of reducing privacy, it could also be said to be liberty promoting by fostering innovation and wealth which provides us with new avenues of actions and liberties.

4.4. *Three framings of the trade-off and a unification of the various perspectives*

Thus far, we have seen that there are three seemingly contradictory, but all conceptually valid, ways of framing the trade-off between security and privacy, and the associated effects on liberty. Firstly, we could argue that by trading privacy for security, we increase liberty, as a liberty that we can safely use and enjoy requires security [1,4]. Secondly, some could argue that security can be increased by sacrificing privacy, without liberty being neither reduced nor increased. This could be argued to be possible with regard to a simple interpretation of negative liberty [41]. Thirdly, while security might be increased by reducing privacy, when privacy is reduced, so is liberty. This is shown both by the emphasis on a space in which to develop autonomy and by considering liberty as non-domination [14,33]. While seemingly contradictory, the three perspectives on the relationship between the three concepts are in fact reconcilable.

Following Berlin, we consider both negative and positive liberty to be of some value, and we will similarly assume that a basic level of security is required for liberty to be meaningful. This might imply discussing the conditions of liberty, and effective liberty, or it might simply involve acknowledging that in human society a minimum of contraction of liberty is quite simply unavoidable for life to be both possible and meaningful [4,41]. As reflected in more recent literature on freedom, the lack of it is associated with problems of upholding order, as "in some areas it is *only* through freedom that the security of civilians in a state can be obtained" [3]. We need not assume that this is an objective fact, but could also rely on a psychological theory akin to that of Maslow, where security is considered a basic need that must to a certain degree be fulfilled before we attach value to and become preoccupied with liberty [4,67,68].

However, the relationship between security and liberty is not so simple as to be described as linearly positively correlated. After the initial positive relationship, negative liberty will increasingly come under pressure with efforts to gain more and more security. This implies that a consequentialist approach to security, liberty, and privacy cannot involve maximising security in isolation, as doing so would actually *reduce* security once the effects of privacy and liberty are factored in [9]. Absolute security is considered neither possible nor desirable, as it would involve severe restrictions on individual action. As neither absolute liberty nor absolute security is feasible, the trade-off between security and privacy, and then liberty, requires us to properly understand the relationship between the three.

The argument made in this article suggests that it would be misguided to attempt to maximise any of the three concepts we examine in isolation, as their interrelationships indicate that they are preconditions of each other and are characterised by complex dependencies. The need to account for all concepts at once is shown in Fig. 1, which suggests that whenever we seek too much of one concept, we necessarily get too little of another. While the relationships between the three concepts are not as simple as they might appear by just looking at the figure, the figure shows that while certain positions might be hypothetically realisable, only the grey areas are feasible and realisable when one considers how, for example, security requires both liberty and privacy.

Many discuss this in terms of finding a *balance* between, for example,

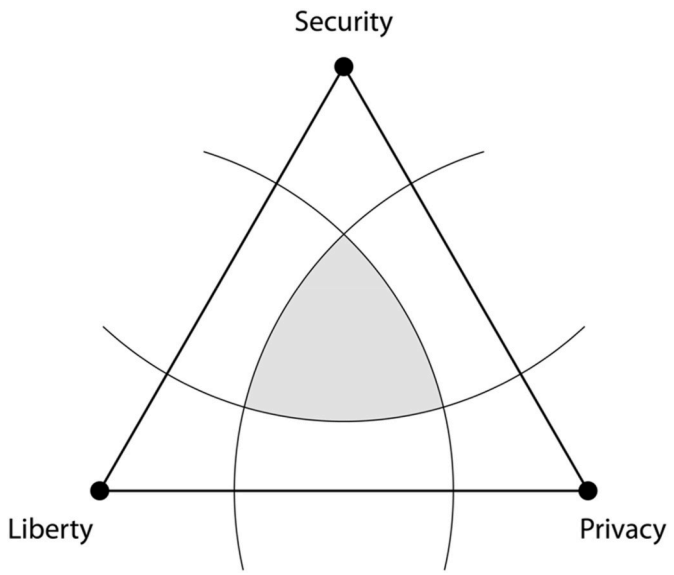

Fig. 1. The realisable area in which sufficient levels of security, liberty, and privacy are provided simultaneously.

public safety and private liberty [6,8]. However, the trade-off between liberty and security is often criticised as being a false choice, or for excessively simplifying a highly complex relationship between the two concepts [3,4,9,39,40]. One reason is that increasing security by reducing liberty involves long term negative effects from infringing on individual rights, such as direct experienced loss from loss of rights, and blocking paths to legitimate opposition to government, which may, for example, lead to increased insecurity through civil unrest and terrorism [3,9]. This will naturally be less applicable to the threat of disease than to the threat of terror, as disease has no intentions and will not be assumed capable of being provoked by anti-disease measures. Another reason to be wary of the idea of a trade-off is that it shifts the balance between state power and the rights of individuals, and creates potentially dangerous precedents [3].

I have shown that this criticism is correct, when aimed at the use of "balance" and a "trade-off" that implies a simple linear relationship which suggests that an increase in the one is followed by a decrease in the other. Furthermore, I have suggested that separating privacy and liberty, but taking account of both, enables us to see the mechanisms involved in a more complex trade-off between security and other values. Donohue [3] has argued that the debates about security and freedom often miss the larger picture. I agree, and support her call for these debates to account for "broad and ongoing liberal, democratic dialogue" [3].

Positive liberty, as we have seen, is less susceptible to be reduced by sacrificing privacy related to information about movement and physical actions. It is, however, like negative liberty, dependent on a certain level of space in which to live and act independently and in ways that will involve *some* degree of public risk. If we consider the potential of liberty as safeguards against any form of domination, far stricter requirements for preserving privacy emerge. While it is possible to trade privacy for security without necessarily sacrificing much negative liberty, and to a certain degree not necessarily infringing on positive liberty, a reduction of privacy rapidly creates threats to liberty as non-domination. As soon as more information about both our physical and psychological states are known to others, we become more susceptible to their power [57].

5. Conclusion

This article has examined the concepts of liberty, privacy, and security – three concepts of vital importance for anyone interested in the constitution of the good society and the role of technology [69]. While the three concepts are all crucially important, I have shown that one cannot approach these concepts in isolation, and that any attempt to maximise these concepts without analysing how they are interrelated entails grave dangers.

While security is, and must be, a key consideration for government, there are clear limits to how far we can pursue security before we lose both privacy and liberty. While such losses would be disastrous by themselves, I have further argued that whenever privacy and liberty *are* lost, there can be no security. Privacy and liberty are in fact conditions of security, so whenever someone discusses the trade-off between security and privacy or liberty, it is important to note that such a trade-off is far more complicated than it might first appear. The two examples examined have highlighted some of the complex nature of these relationships.

Privacy reducing technologies are not all alike, and each must be considered separately in light of the preceding considerations. Contact tracing apps have the potential to reduce liberty by reducing privacy, but it will also let us *increase* the kinds of liberty that are dependent on a certain level of security. By reducing the risk of disease, such an app will allow us to move about more freely, associate more freely, and society in general might avoid detrimental effects related to both the economy and health which could in turn lead to a reduction of liberty. Counter terrorism involves the same kinds of considerations, but it is also different on two key points. In most modern societies, the danger of terrorism often feels less prevalent than a dangerous virus does in times of a pandemic, and the required reduction of privacy is much more serious. The scale of a terrorist incident is, however, great, and will lead many to accept the trade-off between privacy and security. While legitimate, it is worth noting the warning of Cohen [33], who states that a "society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy". Security might be gained, but both privacy and liberty will be the price paid.

The answer to the question of whether or not pivotal events and new technologies justify reducing privacy in order to bolster security also relies on context. In a situation where insecurity creates fundamental challenges for exercising liberties of any kind, security increasing technologies will be more likely to promote liberty than in societies in which we already have relatively high levels of security. The answer to the question of whether or not a particular trade-off or technology is legitimate consequently depends on an analysis of the current status of security, privacy, and liberty in the examined context. Accepting a privacy-reducing technology should thus have a far higher threshold in countries in which we are already secure, or in which privacy is already at a minimal level.

Security is fundamentally valuable, but at a certain point the loss of privacy leads to a serious loss of liberty and privacy. It turns out that too much of a good thing is not that good at all.

Author statement

Henrik Skaug Sætra: Conceptualization, Data curation, Investigation, Methodology, Visualization, Writing - original draft, Writing - review and editing.

References

[1] T. Hobbes, Leviathan, Basil Blackwell, London, 1946, p. 1651.
[2] R. Nozick, Anarchy, State, and Utopia, Basic Books, New York, 1974.
[3] L.K. Donohue, Security and freedom on the fulcrum, Terrorism Polit. Violence 17 (1–2) (2005) 69–87.
[4] J. Waldron, Safety and security, Nebr. Law Rev. 85 (2006) 454.
[5] A.F. Westin, Privacy and Freedom, IG Publishing, New York, 1967.
[6] A. Cawkell, Privacy, security, and freedom in the information society, J. Inf. Sci. 4 (1) (1982) 3–8.
[7] 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, PublicAffairs, New York, 2019.
[8] C.P. Banks, Security and freedom after September 11: the institutional limits and ethical costs of terrorism prosecutions, Public Integr. 13 (1) (2010) 5–24.

[9] T. Dragu, Is there a trade-off between security and liberty? Executive bias, privacy protections, and terrorism prevention, Am. Polit. Sci. Rev. 105 (1) (2011) 64–78.
[10] D.J. Solove, Understanding Privacy, Harvard University Press, Cambridge, 2008.
[11] I. Berlin, Liberty, Oxford University Press, Oxford, 2002.
[12] B. Baum, R. Nichols, Isaiah Berlin and the Politics of Freedom: 'Two Concepts of Liberty' 50 Years Later, Routledge, New York, 2013.
[13] C. List, L. Valentini, Freedom as independence, Ethics 126 (4) (2016) 1043–1074, https://doi.org/10.1086/686006.
[14] P. Pettit, Republicanism: a Theory of Freedom and Government, Clarendon Press, 1997.
[15] D.J. Solove, A taxonomy of privacy, U. Pa. L. Rev. 154 (2005) 477.
[16] D.J. Solove, Conceptualizing privacy, Calif. Law Rev. 90 (2002) 1087.
[17] H.T. Tavani, J.H. Moor, Privacy protection, control of information, and privacy-enhancing technologies, Comput. Soc. 31 (1) (2001) 6–11.
[18] T. Scanlon, Thomson on Privacy, Philosophy & Public Affairs, 1975, pp. 315–322.
[19] A.L. Allen, Coercing privacy, Wm. & Mary L. Rev. 40 (1998) 723.
[20] D.J. Solove, The Digital Person: Technology and Privacy in the Information Age, NyU Press, 2004.
[21] H. Nissenbaum, Protecting Privacy in an Information Age: the Problem of Privacy in Public,", Law and philosophy, 1998, pp. 559–596.
[22] S.D. Warren, L.D. Brandeis, The right to privacy, Harv. Law Rev. (1890) 193–220.
[23] J.J. Thomson, The Right to Privacy, Philosophy & Public Affairs, 1975, pp. 295–314.
[24] F. Callard, E. Perego, How and why patients made Long Covid, Soc. Sci. Med. 268 (2021) 113426.
[25] C. Véliz, Privacy during the pandemic and beyond, Philosopher's Mag. 90 (2020) 111–117.
[26] Helsenorge, Together we can fight coronavirus – smittestopp temporarily deactivated. https://helsenorge.no/coronavirus/smittestopp. (Accessed 1 September 2020).
[27] NearForm, Building the gold-standard COVID-19 contact tracing app within 3 months. https://www.nearform.com/work/covid-app-development/, 9, 1.
[28] H. Cho, D. Ippolito, Y.W. Yu, Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-Offs, 2020 arXiv preprint arXiv:2003.11511.
[29] J. Tidy, Coronavirus: Israel enables emergency spy powers, in: BBC News, 2020.
[30] 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.
[31] K. Dear, K. Dutton, E. Fox, Do 'watching eyes' influence antisocial behavior? A systematic review & meta-analysis, Evol. Hum. Behav. 40 (3) (2019) 269–280.
[32] K. Macnish, The Ethics of Surveillance: an Introduction, Routledge, Oxon, 2018.
[33] J.E. Cohen, What privacy is for, Harv. Law Rev. 126 (2012) 1904.
[34] D.M. Wood, K. Ball, D. Lyon, C. Norris, C. Raab, A Report on the Surveillance Society, Surveillance Studies Network, UK, 2006.
[35] D. Lyon, Surveillance Studies: an Overview, 2007. Polity.
[36] 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, https://doi.org/10.1080/1369118X.2012.678878.
[37] H. Chen, R.H. Chiang, V.C. Storey, Business intelligence and analytics: from big data to big impact, MIS Q. (2012) 1165–1188, https://doi.org/10.2307/41703503.
[38] 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.
[39] A.L. Fimreite, P. Lango, P. Lægreid, L.H. Rykkja, After Oslo and Utøya: a shift in the balance between security and liberty in Norway? Stud. Conflict Terrorism 36 (10) (2013) 839–856.
[40] C.W. Lewis, The clash between security and liberty in the US response to terror, Publ. Adm. Rev. 65 (1) (2005) 18–30.
[41] I. Berlin, in: H. Hardy Liberty (Ed.), Two Concepts of Liberty, Oxford University Press, Oxford, 2002.
[42] I. Berlin, in: H. Hardy Liberty (Ed.), Introduction, Oxford University Press, Oxford, 2002.
[43] G.C. MacCallum, Negative and positive freedom, Phil. Rev. 76 (3) (1967) 312–334.
[44] C. Taylor, Philosophy and the Human Sciences: Philosophical Papers 2, Cambridge University Press, Cambridge, 1985.
[45] J. Raz, The Morality of Freedom, Clarendon Press, Oxford, 1986.
[46] 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.
[47] J. Tully, "Two concepts of liberty" in context, 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. 23–51, ch. 1.
[48] E. Myers, Berlin and democracy, 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. 129–142, ch. 7.
[49] I. Carter, A Measure of Freedom, Oxford University Press, Oxford, 1999.
[50] C.B. MacPherson, Berlin's division of liberty, in: C.B. MacPherson (Ed.), Democratic Theory: Essays in Retrieval, Clarendon Press, Oxford, 1973, pp. 95–96.
[51] Q. Skinner, A third concept of liberty, Proc. Br. Acad. 117 (2002) 237–268.
[52] H. Nissenbaum, Privacy as contextual integrity, Wash. Law Rev. 79 (2004) 119.
[53] J.E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press, 2012.
[54] S. Wachter, B. Mittelstadt, A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI, Columbia Bus. Law Rev. (2019) 494.
[55] T.Z. Zarsky, Mine Your Own Business: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion, vol. 5, Yale JL & Tech., 2002, p. 1.
[56] J.-J. Rousseau, Rousseau, The Social Contract and Other Later Political Writings, Cambridge University Press, Cambridge, 1997, p. 1762.
[57] C. Véliz, September 2nd. Privacy Is Power, AEON, 2020.
[58] I. Carter, R. Shnayderman, The impossibility of "freedom as independence", Polit. Stud. Rev. 17 (2) (2019) 136–146, https://doi.org/10.1177/1478929918771452.
[59] H.S. Sætra, When nudge comes to shove: liberty and nudging in the era of big data, Technol. Soc. 59 (2019) 101130, https://doi.org/10.1016/j.techsoc.2019.04.006.
[60] J. Alexander, J.P. Zenger, A. Hamilton, A Brief Narrative of the Case and Trial of John Peter Zenger, Printer of the New-York Weekly-Journal, W. Dunlap, New York, 1736.
[61] J. Locke, Two Treatises of Government, Hafner Publishing Company, New York, 1969, p. 1690.
[62] M.A. Orlie, Making sense og negative liberty: Berlin's antidote to political rationalism, 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. 143–154, ch. 8.
[63] P.M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill: University of North Carolina Press, 1995.
[64] J.P. Choi, D.-S. Jeon, B.-C. Kim, Privacy and personal data collection with information externalities, J. Publ. Econ. 173 (2019) 113–124.
[65] J.S. Mill, On Liberty, Penguin books, London, 1985, p. 1859.
[66] A.D. Tocqueville, Democracy in america, The University of Chicago, Chicago, 2000, pp. 1835–1840.
[67] A.H. Maslow, Motivation and Personality, Pearson Education, Delhi, 1987.
[68] H.S. Sætra, Toward a Hobbesian Liberal Democracy through a Maslowian Hierarchy of Needs, The Humanistic Psychologist, 2020.
[69] C. Griffy-Brown, B.D. Earp, O. Rosas, Technology and the good society, Technol. Soc. 52 (2018) 1–3.
[70] Henrik Skaug Sætra, Privacy as an aggregate public good, Technol. Soc. 63 (101422) (2020). https://doi.org/10.1016/j.techsoc.2020.101422.