Philosophy & Technology (2022) 35: 8
https://doi.org/10.1007/s13347-022-00503-9

RESEARCH ARTICLE

Government Surveillance, Privacy, and Legitimacy

Peter Königs[1]

Received: 8 September 2021 / Accepted: 15 January 2022 / Published online: 5 February 2022

Abstract

The recent decades have seen established liberal democracies expand their surveillance capacities on a massive scale. This article explores what is problematic about government surveillance by democracies. It proceeds by distinguishing three potential sources of concern: (1) the concern that governments diminish citizens' privacy by collecting their data, (2) the concern that they diminish their privacy by accessing their data, and (3) the concern that the collected data may be used for objectionable purposes. Discussing the meaning and value of privacy, the article argues that only the latter two constitute compelling independent concerns. It then focuses particularly on the third concern, exploring the risk of government surveillance being used to enforce illegitimate laws. It discusses three legitimacy-related reasons why we should be worried about the expansion of surveillance capacities in established democracies: (1) Even established democracies might decay. There is a risk that surveillance capacities that are used for democratically legitimated purposes today will be used for poorly legitimated purposes in the future. (2) Surveillance may be used to enforce laws that lack legitimacy due to the disproportionate punishment attached to their violation. (3) The democratic procedures in established democracies fail to conform to the requirements formulated by mainstream theories of democratic legitimacy. Surveillance is thus used to enforce laws whose legitimacy is in doubt.

Keywords Surveillance · Privacy · Legitimacy · Democracy · Punishment

1 Introduction

For a long time, large-scale government surveillance was a hallmark of authoritarianism. Authoritarian states known for their extensive surveillance systems include the GDR, the People's Republic of China, the Soviet Union, and North

✉ Peter Königs

[1] Frankfurt School of Finance & Management, Frankfurt, Germany

Korea.[1] In the past few decades, however, established liberal democracies have been increasingly ready to monitor their citizens on a massive scale. One notorious surveillance program run by an alliance of democracies was uncovered by Edward Snowden. The current rise of large-scale government surveillance is widely viewed with great concern, if not outright horror. Critics fear the rise of Orwellian surveillance states and celebrate Edward Snowden as a paragon of civil disobedience.[2] Much of the criticism of government surveillance has revolved around privacy, its meaning and value, and how it is impacted by surveillance. Government surveillance and the erosion of privacy it is associated with are being discussed as a cause of distrust and feelings of vulnerability, as a potential source of discrimination and unjust domination, and as a threat to democracy and the integrity of the public sphere, to name but a few concerns. By many, existing government surveillance programs are also deemed disproportionate.[3]

At the same time, there remains some ambiguity about the acceptability of surveillance in democracies. For one thing, recent technological advances have made large-scale government surveillance not only feasible and cheap but also, in one sense, less intrusive. Modern government surveillance relies increasingly on technology rather than human spies and informers. Surveillance practices include, for instance, the monitoring of public spaces with CCTV cameras, the automatic interception and retention of Internet and telecommunication traffic, and the use of artificial intelligence to make sense of the huge amounts of data collected. As a result, modern surveillance is characterized by the rarity of actual human access to the large quantities of data collected. While the quantity of data collected is staggering, only a small proportion of them are ever accessed by a human person. Human access to collected surveillance data can be expected to further decrease as artificial intelligence becomes more sophisticated. This has led to a debate about whether modern surveillance even reduces the privacy of those subject to surveillance, with some arguing that modern surveillance, involving little human access to the collected data, tends to leave people's privacy intact.[4]

For another thing, surveillance operations by democracies seem much more acceptable than the kind of surveillance conducted by authoritarian regimes. Democracies are using surveillance mostly for seemingly innocuous purposes, such as combating terrorism and serious crime or, most recently, containing the spread of

[1] For an overview of policing and surveillance in twentieth-century dictatorships, refer to Dunnage (2016). Dunnage reports that it is estimated that, in the post-Stalinist Soviet Union, some 30 to 60% of the population were forced to work as informers for the KGB, and in the GDR, roughly every thirtieth citizen served as an informer for the regime. Nazi Germany may have relied less on surveillance and more on denunciations (pp. 122–123). On surveillance in China and North Korea, see Denyer (2018) and Lankov and In-ok (2011), respectively.

[2] See, e.g., Brownlee (2016) and Scheuermann (2014).

[3] Critical discussions of government surveillance include Goold (2009); Henschke (2017, ch. 9); Hoye and Monaghan (2018); Lever (2008); Nissenbaum (1998); Roberts (2015); Solove (2007); Smith (2020); Stahl (2016, 2020); and I. Taylor (2017). For two non-privacy-centered criticisms of government surveillance, see Macnish (2018, 2020) and Sorell (2018). A classic treatment of this topic is Foucault (1975). See also Zuboff (2019), though her focus is on "surveillance" by private companies.

[4] Most prominently Macnish (2018, 2020); see also Posner (2005) and Sorell (2018). For an argument that public video surveillance does not violate privacy rights, refer to Ryberg (2007).

a deadly virus. They are less inclined to use surveillance to crush legitimate political opposition or to persecute members of stigmatized groups, notable exceptions notwithstanding.[5] There is a significant moral difference, then, between, say, the NSA and the East German *Stasi*.[6]

In sum, when democratic governments conduct large-scale surveillance operations in the pursuit of seemingly innocuous goals, all while limiting human access to the collected data, the case against surveillance is at least not obvious. In fact, some philosophers have expressed wholehearted support for large-scale government surveillance. Noting that it is generally permissible for law enforcement agencies to secure information about past events, one advocate of government surveillance has suggested that "the State should place all of its citizens under surveillance at all times and in all places."[7] Others have invoked catastrophic risks, such as those posed by biological and nuclear weapons of mass destruction, to justify extensive government surveillance.[8] To be sure, such wholesale endorsements of government surveillance are the exception.[9] But they convey an idea of the ethical ambivalence of government surveillance.

My goal in this paper is to contribute a new perspective on what is ethically at stake when democratic governments monitor their citizens and to achieve a better understanding of what is pro tanto objectionable about it.[10] I will proceed by distinguishing three independent concerns that a critic of government surveillance may have. The first concern is that governments diminish citizens' privacy by collecting large amounts of data. This concern focuses on the loss of privacy brought about by the collection of data as such, that is, irrespective of whether the data will be accessed or used for objectionable purposes. The second concern is that the collected data may be accessed after all, again causing a loss of privacy, though of a different kind. The data may be accessed by government employees or exposed to the public through a hack or a leak. The third concern is that the collected data may be used for objectionable purposes (other than accessing the data).

Two of the above introduced concerns revolve around privacy. Zooming in on these two concerns, this paper seeks, first, to shed light on the significance of privacy in the context of surveillance. Engaging with the debate about the meaning of privacy, I will suggest that, whereas access to data is objectionable as such, the privacy loss brought about by the mere collection of data does not constitute an independent reason to object to government surveillance. Second, moving on to the third concern, the paper seeks to achieve a better understanding of problems associated with what surveillance can be used for. I will suggest that one serious and

[5] Exceptions include surveillance in the McCarthy era, the FBI's COINTELPRO (including the wiretapping of Martin Luther King), and undercover policing in the UK (see the ongoing Undercover Policing Inquiry). See also Goold (2009, p. 43).

[6] See Sorell (2011, pp. 12–14).

[7] J. S. Taylor (2005, p. 227).

[8] Persson and Savulescu (2012)

[9] Much more cautious defenses of surveillance have been advanced by Smith (2020) and I. Taylor (2017).

[10] In what follows, the "pro tanto" will usually be omitted, but I will return to it in the conclusion.

underappreciated problem with surveillance is related to the problem of political legitimacy. Surveillance can be used to enforce laws that lack legitimacy.

My discussions of privacy and legitimacy, though motivated by concerns about government surveillance, are, I hope, of more general relevance and thus of interest to scholars who have no particular interest in surveillance.

2 Surveillance and Privacy

I want to begin by examining the first concern about privacy, that is, the notion that there is something objectionable about government surveillance because the collection of massive amounts of data reduces people's privacy. By undermining people's privacy, government surveillance may be deemed objectionable irrespective of whether the data are accessed (second concern) or used for objectionable purposes (third concern). It is, in this sense, an *independent* concern about government surveillance.

There are four reasons why this concern is worth looking at. To begin with, it is a very natural thought that surveillance is objectionable simply on the grounds that the collection of people's data reduces their privacy. Privacy is a widely valued good, and the mere collection of data is thought by many (though not all) to undermine privacy. It is therefore natural to object to the collection of data simply on the grounds that this violates people's privacy — irrespective of whether the other two concerns apply.

Moreover, the extent to which increasingly automated surveillance practices really involve privacy losses is, as already noted, intensely discussed among privacy and surveillance scholars. An underlying assumption here seems to be that if the collection of citizens' data reduces their privacy, surveillance is ipso facto problematic, irrespective of whether the data will be accessed or used for malicious purposes. Why else think that it matters how we define privacy and whether it is undermined by surveillance? Surveillance may be thought to be problematic simply in virtue of the fact that it undermines people's privacy.

Yet another reason why the validity of the first concern matters is that some might question the force of the other two concerns. Human access to the collected data is very limited, and established liberal democracies may seem to use surveillance mainly for justifiable purposes. In light of this, some might question why we should object to large-scale government surveillance at all. If there is something objectionable about collecting large amounts of data as such (because of the privacy breaches associated with it), the critic of government surveillance has a ready answer to this question.[11]

Finally, discussing this first concern will contribute towards achieving the overarching goal of this paper, namely a better understanding of how surveillance and

[11] The observation that no access takes place when data are processed by intelligent algorithms might be challenged on the grounds that these algorithms are themselves "agents" of sorts, who "access" the data when processing them. Whether intelligent systems qualify as "agents" or not, I agree with Macnish (2020) that there is a significant difference between access by humans and access by entities that lack "semantic understanding," e.g., intelligent systems.

privacy concerns relate to each other and how the potential harm done by government surveillance should be characterized. I believe that the first concern is ill-founded in that it fails to constitute a compelling independent reason to object to government surveillance, over and above the other two concerns. Appreciating why this is so allows a better understanding of the problem of government surveillance and of what is at stake in debates about the meaning and value of privacy.

Notice first, then, that the idea that there is something objectionable about the collection of data as such, though natural, can be challenged by means of a thought experiment. Imagine an unrealistically benevolent, well-organized, and stable democratic state that engages in large-scale surveillance operations. The state is characterized by the following two features:

1) Thanks to excellent institutional safeguards and security measures, there is no risk that data is illicitly accessed by government employees, nor that data might be exposed to the public.
2) It uses the collected surveillance data to enforce laws in a legitimate and just manner. It never uses the surveillance capacities for objectionable purposes. It also boasts a set of unrealistically robust checks and balances, which completely remove any risk of the surveillance capacities being used for less benign purposes in the future.

Admittedly, such perfectly benign surveillance is difficult to imagine. But when we do imagine it, it is difficult to see what might be objectionable about it. Once we stipulate that there is no risk of illicit access to the collected data and that the surveillance capacities will only ever be used for good purposes, that is, once we stipulate that the other two concerns do not apply, there just seems little cause for concern. On the contrary, it is arguable that we should welcome such perfectly benign surveillance. It provides enhanced security without any obvious downsides. To object to such perfectly benign surveillance would, it seems to me, be quite irrational. To be sure, we may have a residual feeling of unease at the thought even of such benevolent large-scale government surveillance (I, for one, certainly feel uneasy at the thought of it). But this is probably because no surveillance system in the real world resembles this perfectly benign surveillance system. Our emotional responses have been trained on a data set of surveillance practices that invariably do not meet the above two criteria. Upon rational reflection, we should welcome surveillance of this sort.

This provides at least initial grounds for thinking that the first concern must be ill-founded. The collection of large amounts of data as such — divorced from the other two concerns — seems unobjectionable. But one might still find the above line of reasoning unconvincing as it entirely brackets the key issue of privacy. Indeed, I have made two seemingly conflicting claims. On the one hand, I have just suggested that there does not seem to be anything problematic about the collection of data as such, divorced from the other two concerns. On the other hand, I have suggested that the collection of large amounts of data may diminish citizens' privacy. This raises the question how the collection of large amounts of data could possibly diminish people's privacy without being in any way problematic as such. If it diminishes their privacy,

does this not show precisely that there is something objectionable about surveillance irrespective of whether the data are exposed or used for objectionable purposes?

To resolve this tension, and more generally to understand how surveillance and privacy relate, it is useful to briefly consider the debate about the meaning of privacy. One view in the literature is that privacy should be spelled out in terms of control. A person's privacy remains intact as long as this person retains control over her personal information.[12] Beate Rössler, for instance, proposes the following definition: "Something counts as private if one can oneself control the access to this 'something.'"[13] On this view, privacy is reduced as soon as one loses the relevant sort of control. A competing view holds that privacy is a matter of access, not of control. A person's privacy is intact to the extent that no one actually accesses her personal information. Mere loss of control over one's personal information is not enough for there to be a reduction of privacy. Kevin Macnish has made the case for the access account by appeal to the so-called threatened loss cases. Threatened loss cases are characterized by a loss of control over one's personal information in the absence of actual access to it. He invites us to consider the case of a person who left her diary on a table in a coffee shop. When she returns to the coffee shop to pick it up, it is handed back to her by a stranger in whose possession it was for the last 30 minutes. During this interval, the diary owner had lost control over her personal information in the diary. But if the stranger did not open the diary during this time, it seems plausible that the diary owner's privacy has not been comprised. Such threatened loss cases suggest that what matters is actual access rather than loss of control.[14]

An assumption underlying this debate is that there is a lot at stake in the dispute about the meaning of privacy. Recall that modern government surveillance, relying increasingly on technology rather than people, involves relatively little actual human access to the collected data. Depending, then, on how we define privacy, modern government surveillance involves either privacy erosions on a massive scale (control account) or hardly any privacy losses at all (access account), given that it involves loss of control over one's personal data but little actual human access to them.[15] This is why how we define privacy has been taken to matter a great deal.

Notwithstanding the many valuable insights this debate has generated, I do not believe that how we define privacy matters as much as is commonly thought. Little of substance depends on it. Whether we should think of government surveillance operations as reducing

[12] I am focusing on informational privacy, as this seems to be the relevant kind of privacy in the present context.

[13] Roessler (2005, p. 8). Other proponents of the control account include Fried (1984, p. 209); Menges (2020a); Moore (2003, 2008); Westin (1967, p. 7); and, tentatively, Mainz and Uhrenfeldt (2021) (the latter focus on the *right* to privacy, though). For an interesting exchange about its plausibility, see Lundgren (2020) and Menges (2020b).

[14] Macnish (2018); see also Macnish (2020) and Thomson (1975, pp. 304–305, n. 1). An argument strikingly similar to Macnish's (that even features a diary example) was independently developed by Tom Sorell (2018). For a subtle attempt by a control theorist to account for threatened loss cases, refer to Menges (2020a, forthcoming).

[15] Note, though, that Menges, although a control theorist, tries to capture the intuition that no privacy loss occurs in threatened loss cases and thus agrees with Macnish that modern government surveillance involves very little loss of privacy (2020a, 2020b, forthcoming).

privacy in the strict sense of the term or not is, at the end of day, not that relevant. Indeed, Macnish himself, who in the title of a paper asserts that "defining privacy matters," is (rightly, I think) adamant that government surveillance is problematic even if, technically, citizens' privacy is not diminished.[16] This begs the question why exactly it should matter which definition of privacy we opt for. I believe it does not matter all that much. What matters are the actual wrongs and dangers of surveillance, and their exploration does not require resolving the dispute between access theorists and control theorists.[17]

I therefore wish to sidestep this debate by engaging in an act of conceptual stipulation. I suggest that we distinguish *two* concepts of privacy: "access privacy" and "control privacy." Access privacy is the kind of privacy that requires nonaccess to one's personal information, whereas control privacy is reduced as soon as one loses control over one's personal information, whether accessed or not. Modern government surveillance, to the extent that it does not involve human access to the collected data, reduces control privacy while leaving access privacy mostly intact.[18] The suggested distinction is a technical stipulation. By making this stipulation, I am not suggesting that our everyday concept of privacy is fundamentally vague or ambiguous. Perhaps it is, but I am not committed to this view.[19] Nor do I mean it to discourage further inquiry into how to best analyze everyday privacy talk, which strikes me as an interesting undertaking in its own right. But introducing these two technical concepts by means of stipulation allows us to sidestep an intricate and unresolved debate, and it yields two technical concepts that are useful for analytical purposes. To be sure, the proposed terminological stipulation tells us little of substance about the significance of privacy in the context of government surveillance. But it helps us organize our thoughts and get more quickly to the heart of what is normatively at stake.[20]

[16] Macnish (2018, 2020). Menges concurs (2020a, pp. 46–47). A view similar to Macnish's has been defended by Sorell, who "den[ies] that bulk collection is seriously intrusive without denying that it is morally objectionable in other ways" (2018, p. 47).

[17] I am here concurring with Henschke (2017, p. 46), Solove (2007, p. 760; 2009, pp. 39–40), and van den Hoven (2008), who have warned against getting bogged down in conceptual debates.

[18] Henschke (2020), too, suggests distinguishing two concepts of privacy. His distinction differs from mine. In his 2017, he defends a pluralistic, "clustered" approach to privacy.

[19] For what it is worth, I share Macnish's linguistic intuition that privacy is only reduced in situations in which human access occurs.

[20] An anonymous reviewer has sensibly suggested that I clarify whether this approach commits me to the views that (1) defining privacy is not crucial to assessing the ethical permissibility of surveillance, and (2) intermediate moral principles such as "Do not diminish a person's privacy [or, for that matter, autonomy, freedom, etc.]" play little role in moral theory compared to more fundamental principles such as the categorical imperative or the utilitarian calculus. In response, I wish to state that I do believe that defining privacy matters, and I have offered two stipulative definitions of privacy. What I do not believe is that we necessarily need to determine which of several privacy definitions on offer (especially privacy as control and privacy as nonaccess) best capture everyday privacy talk before we can address the ethical issue at stake. We can proceed by exploring *both* the normative significance of reductions of control privacy and that of reductions of access privacy. This way, we can come to grips with the problem of surveillance without first having to identify which concept of privacy best captures everyday privacy talk. This is the approach I am taking in this essay. Relatedly, I am not committed to the view that intermediate principles do not matter for moral theorizing. Such principles as "Do not diminish a person's privacy" do play a role in moral theorizing, but again, we can work with different versions of such principles (e.g., "Do not diminish a person's control privacy," "Do not diminish a person's control privacy," etc.), and we need not first identify which privacy concept best captures everyday privacy talk.

With these clarifications in mind, we can return to the question at hand: How might the collection of data involve a reduction in privacy without being in any way problematic as such, that is, irrespective of whether the data may actually be accessed or used for objectionable purposes? My answer is not that we should simply reject the assumption that the mere collection of data even involves privacy losses, as adherents of the access account of privacy would do. I think both accounts of privacy are legitimate, and it is not obviously wrong to say that the mere collection of data reduces people's (control) privacy. Instead, the answer I want to propose is that the collecting of data may well be said to diminish people's (control) privacy, but that the value of this kind of privacy depends on the other two concerns, that is, on the risk of collected data being accessed or of them being used for objectionable purposes. In a, again unrealistic, world in which there is no risk of data access or misuse by the government, the value of control privacy would be unclear. Mere loss of control over one's personal data would be unproblematic, *if* we could rest assured that the data are not accessed and that nothing bad happens with these data. I want to state unequivocally that I am not suggesting that, in normal circumstances, there is no reason to value control privacy, or that we need not be concerned about governments reducing people's control privacy. In normal circumstances, the antecedent of the above conditional is not satisfied. The risk of our data being accessed or abused is real, and this is reason enough to be concerned about the mass collection of data. Rather, the point I wish to make is an analytical one: at least in the context of surveillance, the value of control privacy is closely tied to the other two concerns. We may plausibly define privacy in such a way that government surveillance can be said to diminish people's privacy, namely their control privacy.[21] But its diminution does not constitute an *independent* concern, over and above concerns about access to one's data (losses of access privacy) and about what these data are or might be used for.[22]

Turning now to the second concern about privacy, a loss of access privacy is different from a loss of control privacy. There seems to be something problematic about people accessing personal information as such, that is, irrespective of other concerns, especially of whether the accessed information will be used for objectionable purposes. Imagine that government agents monitor your behavior, eavesdrop on your conversations, read your mail or email, or reduce your access privacy in some other such way. These privacy breaches seem harmful even when there is no risk whatsoever that the collected information is used for bad purposes (or exposed to the public so that even more people access the information). Even if we stipulate that these agents are perfectly virtuous people who, somehow isolated from the rest of society, have not the slightest opportunity to pass on the information gleaned to others, there is, I think, a distinct sense that you are being harmed. I admit that I am here appealing to intuition and that it is not easy to spell out the nature of this harm

[21] At least according to the standard version of the control account. See again Menges (2020a, b, forthcoming) for a version of the control account that entails that government surveillance need not necessarily reduce people's privacy.

[22] Similarly, Henderson (2016, p. 962) observes that "assuming complete automation, the key privacy harm seems to occur only upon human viewing, or use.".

or provide further support for this view. Perhaps we are here reaching ethical rock-bottom. One way of going beyond brute intuition may be to observe that people who have had intimate information accessed by others often feel exposed, embarrassed, humiliated, or simply awkward, a response that does not appear fully reducible to fears about what the information gleaned may be used for. Maybe, as ethicists, we do well to take these responses at face value.[23] Thus, although the argument for it remains somewhat schematic, it is certainly plausible that breaches of access privacy are objectionable as such, irrespective of other concerns, in particular of what the accessed information will be used for.[24] There appears to exist a significant normative difference between whether some piece of personal information, which we had rather kept for ourselves, is actually in somebody else's mind or not — a distinction that certainly has some plausibility on its face. Admittedly, though, my argument for this asymmetry is not uncontestable, and it is open to critics to challenge it by either disputing that access as such is problematic or by pushing the intuition that loss of control as such is problematic too.

The claims I have made are substantive ethical claims, which are independent from definitional questions. They would remain true if we opted for some other definition of privacy, although this would necessitate reformulating them. The increasingly automated character of modern surveillance matters not for reasons related to the meaning of privacy. It matters *morally* because it means that there can be collecting and processing of large amounts of data without any access taking place. This is relevant because access as such is morally problematic. By contrast, the mere collecting of large amounts of data, though reducing control privacy, does not constitute a compelling independent concern about surveillance, independent, that is, from the other two concerns. To understand what is ultimately problematic about government surveillance, we must therefore focus on the concern about access and the concern about what surveillance is used for. The question regarding the meaning of privacy and whether surveillance should be said to reduce "privacy" is peripheral.

The concern about access is legitimate and important. There seems to be something objectionable about human access to surveillance data in its own right, irrespective of what the accessed data are used for. The force of this concern about modern government surveillance is difficult to gauge, though. There certainly is a non-negligible risk of access taking place, in spite of the increasingly automated nature of surveillance. For instance, there are reports that employees of the US's National Security Agency use surveillance tools to spy on their partners.[25] There is also the risk that data are hacked or leaked to the public, in which case they may be accessed by people other than government employees. Just as the extensive data collection efforts by private corporations is worrisome because the collected data are never perfectly secure, so is government surveillance.[26] Indeed, recent security

[23] A related line of research explores the connection between privacy and dignity (Bloustein, 1964; Floridi, 2016; Kleinig, 2009).

[24] This is not to deny that access to information may *additionally* be problematic for the reason that the accessed information may be used for objectionable purposes.

[25] Perez (2013)

[26] For criticisms of corporate "surveillance," see Zuboff (2019).

breaches of government and corporate databases have exposed data of 50 million Turks and 223 million Brazilians, respectively.[27] Still, the fact that surveillance today relies on modern surveillance technologies means that the amount of access taking place is relatively low, compared to "old-fashioned" large-scale surveillance operations. The collection of massive amounts of data does typically not translate to a massive erosion of people's access privacy. Security breaches such as the ones above are the exception, and even when they occur, only a small portion of the data made available is actually accessed. Technological and institutional safeguards may be put in place to further reduce the probability of data breaches, although they will never completely eliminate the risk.[28] Despite the recent massive expansion of government surveillance, it is arguable that today's government surveillance in, say, the US, the UK, or the EU causes fewer reductions in access privacy than, say, government surveillance in the GDR.[29] On the whole, the concern that data might be accessed should be taken seriously, and it is no doubt *part* of the explanation of why real-world mass surveillance is so worrisome. But it only goes some way towards explaining the fierce opposition or even horror that large-scale government surveillance tends to elicit.

Arguably, the most compelling concern about modern government surveillance is that it can be used for objectionable purposes. Mass surveillance is a powerful instrument for controlling people, and placing an instrument this powerful in the hands of already powerful governments raises legitimate fears about what it will be used for (other than potentially for accessing the data). It was mentioned in the introduction that surveillance scholars have already raised a number of concerns regarding large-scale government surveillance. Many of these concerns can be interpreted as being ultimately about how the surveillance data are or might be used. Adding another perspective to this discussion, I will, in the remainder of this paper, explore one problem associated with the use of surveillance that in my view constitutes one of the principal problems with government surveillance and that has so far received little attention.

3 Surveillance and Legitimacy

To appreciate this particular problem, we must consider that government surveillance is a means of enforcing laws. The primary purpose of government surveillance is to ensure that people comply with the law by enabling the legal prosecution of those

[27] Belli (2021); Hern (2016)

[28] See I. Taylor (2017, pp. 335–336).

[29] It is true, though, that the advent of new surveillance technologies has made it more likely that democracies engage in surveillance that might not have engaged in surveillance without these technologies. Thus, although surveillance operations relying on these technologies involve little data access, it may still be the case that the advent of these technologies has led to an *absolute* reduction of access privacy, given that even modern surveillance tends to be associated with *some* reductions in access privacy.

who fail to comply and by creating a climate of deterrence.[30] This section explores the idea that one fundamental problem with government surveillance is that it can be used to enforce laws (or, more broadly, government policies) that the government has no right to enforce. In his autobiography, Edward Snowden asserts that.

> a world of total automated enforcement – of, say, all pet-ownership laws, or all zoning laws regulating home businesses – would be intolerable. Extreme justice can turn out to be extreme injustice, not just in terms of the severity of the punishment for an infraction, but also in terms of how consistently and thoroughly the law is applied and prosecuted.[31]

This observation is, I think, important and to the point. One problem with extensive government surveillance is that we should not want all laws to be consistently and thoroughly applied and prosecuted. The problem of government surveillance is thus closely intertwined with the more general problem of political legitimacy. There is a sense in which a criticism of surveillance along these lines is not a criticism of surveillance per se. Surveillance is really just the tool for achieving that which is argued to be objectionable. This point is well taken. Indeed, I mentioned at the outset that I take my discussion to be of more general relevance and thus, hopefully, of interest to scholars who have no particular interest in surveillance. But it is also true that the rise of government surveillance renders concerns about legitimacy particularly salient and pertinent. It renders the "consistent and thorough application and prosecution of the law" possible in a way that until recently states could only dream of. This is why Snowden's above-quoted concern is not "off-topic" and why, I hope, the below discussion of issues related to legitimacy is fitting.

Political legitimacy refers to the moral right of a government to pass and enforce laws.[32] Understanding the ethical significance of government surveillance requires an understanding of the conditions that must be satisfied for coercive government action to be legitimate. Although most people, political theorists and laypeople alike, accept the legitimacy of democratic governments, it is worth making explicit why government action is in need of legitimation. Essentially, the problem of political legitimacy is that government action is coercive. Government commands are backed by punishments that one cannot defy, as one is literally forced to comply. One might refuse to pay a fine, decide not to turn up to a court hearing, or continue driving one's car after having had one's license revoked. But at the end of the chain

[30] This is not to deny that government surveillance may be used for other purposes that are not straightforwardly reducible to law enforcement or that the effects of government surveillance on those subjected to surveillance may go beyond mere compliance with the law (as scholars in the Foucauldian tradition might suggest).

[31] Snowden (2019, p. 196).

[32] See, e.g., Huemer (2013, p. 5), who defines political legitimacy as "the right, on the part of a government, to make certain laws and enforce them by coercion against the members of its society – in short the right to rule." Political legitimacy can be understood as one dimension of political authority, the other being citizens' obligation to obey laws.

of sanctions, there is (typically) imprisonment, and one is ultimately made to go there by physical force.

The fact that government ultimately rests on the threat of physical force and imprisonment is morally significant, as it constitutes a serious pro tanto wrong that stands in need of moral justification. Indeed, in nonpolitical settings, people are extremely reluctant to condone or personally resort to physical coercion to achieve even desirable aims. Most people would be aghast at the idea of private individuals using physical coercion to carry out the kind of policies that they take governments to be perfectly entitled to enforce. They would, for instance, be appalled if a private individual forcibly extracted money from her neighbor for charitable purposes by threatening to use physical force to lock her up in the basement.[33] Given then the widely acknowledged considerable pro tanto badness of physical coercion and imprisonment, there is a need to justify the use of coercive measures by the government. This need for justification carries over to government surveillance, which is a part of the coercive apparatus of the state. The primary purpose of government surveillance is to ensure compliance with the law and to facilitate the prosecution of those who fail to comply.

One group of people who should find government surveillance objectionable is libertarians and anarchists, who, emphasizing the badness of physical coercion, believe that the scope of legitimate government action is very limited or, indeed, zero.[34] They should approve of government surveillance only for the enforcement of the set of policies that governments may legitimately enforce, which, according to them, is either very small or empty. The observation that there is something objectionable from a libertarian or anarchist point of view with an institution that is an instrument of law enforcement borders on the trivial.[35] Also, libertarianism and anarchism are minority views that few interested in the ethics of government surveillance share. I will therefore put libertarian or anarchist objections to one side and focus on more mainstream conceptions of political legitimacy, which are more optimistic about the capacity of democratic procedures to generate legitimacy. From such as perspective, government surveillance, when carried out by established liberal democracies, may appear prima facie legitimate. When established liberal democracies — think the US, the UK, Germany, or France — rely on surveillance for law enforcement purposes, they are enforcing what appear to be democratically legitimated laws.

My project in this section is to explore why even those subscribing to more mainstream conceptions of political legitimacy have reason to be concerned about government surveillance on account of its forming part of the coercive apparatus of the state. I will identify and discuss three such reasons for concern.[36]

[33] See again Huemer (2013, p. 11). Huemer is a skeptic about political legitimacy, but his characterization should be common ground among optimists and skeptics about political authority alike.

[34] See, e.g., Huemer (2013), Nozick (1974), and Wolff (1970).

[35] Though see Pilon and Epstein (2013).

[36] For a different legitimacy-centered criticism of surveillance, inspired by Habermasian discourse theory, refer to Stahl (2020).

The first and perhaps most obvious reason is that there is always the risk of democratic decay. States that are functioning liberal democracies today might degenerate into severely defective democracies in the future. This risk is today more palpable than ever. It means that there is a risk that the surveillance infrastructure and the collected data that are used for democratically legitimated purposes today will be used for poorly legitimated purposes in the future. When democratic institutions decay, they will at some point fail to generate the legitimacy that is necessary for the enforcement of laws to be rightful. This problem carries over to surveillance. There is something deeply objectionable about government surveillance when it is used to enforce laws that are illegitimate. One risk, then, is that surveillance capacities are used in the future to enforce laws that have not been adequately legitimated. A fortiori, government surveillance is objectionable when a democracy has degenerated into an authoritarian tyranny that employs surveillance to infringe basic human rights. Surveillance can and has been used to stifle free speech, to restrict the freedom of assembly, to go after dissidents, and to oppress and persecute marginalized people, which is not only illegitimate but also substantively unjust.[37]

Second, most democratic theorists agree that there are limits to what can be democratically legitimated. While they regard democratic procedures as an effective way of legitimating coercion, they usually hold that some policies are illegitimate even if they have been passed in a proper democratic procedure. That is, they usually endorse at least some substantial criteria of political legitimacy, the violation of which defeats the legitimating force of democratic procedures. This proviso is typically thought to affect laws that violate basic political rights, the so-called liberties of the ancients. For instance, it is generally held that it is never legitimate to disenfranchise a certain group of people, to take away people's right to freedom of expression, or to severely curtail the freedom of the press. But most democratic theorists also take this proviso to protect nonpolitical human rights, including the liberties of the moderns such as liberty of conscience and the right to bodily integrity.[38]

Many surveillance operations serve to enforce laws against terrorism and serious crime. These are not plausible candidates for laws that involve legitimacy-defeating violations of basic liberties. In the wake of the Covid crisis, however, surveillance has also been used to enforce restrictions on people's basic liberties. Taiwan, South Korea, and Israel have been particularly resolute, relying on mandatory surveillance instruments to enforce quarantine regulations.[39] One newspaper article reports, for instance, that "the [Taiwanese] government worked with telecommunications companies to track quarantined residents' locations using their phone numbers. This

[37] See also Henschke on "Deliberative Information Harms" (2017, pp. 223–227). Note that, in addition, the ready availability of a surveillance infrastructure and of surveillance data might also facilitate the *transition* to an authoritarian regime. It is easier to establish an authoritarian tyranny and persecute its enemies when one already possesses or can readily acquire information about the political orientation and activities of one's subjects.

[38] See, e.g., Christiano (2008, ch. 7); Cohen (1997b); Estlund (2007, p. 110); Freeman (1990); Gutmann and Thompson (2004, ch. 3); Habermas (1996, ch. 3); and Rawls (1996, ch. 8).

[39] Altshuler and Hershkowitz (2020)

system, called a 'digital fence,' notifies authorities when anyone under mandatory quarantine goes outside their designated quarantine site."[40] Surveillance is effectively used to severely restrict citizens' liberty of movement, liberty of assembly, freedom of trade, and other basic liberties. Whether such restrictions constitute a morally justifiable response to the Covid pandemic is debatable and will not be discussed here. I mention them as they convey an idea of how readily surveillance may be used to enforce restrictions that do infringe on citizens' basic liberties.

There is, however, another route to arguing that government surveillance might end up being deployed to enforce democratically enacted yet illegitimate laws. This route — again anticipated by Snowden's remark on the "severity of the punishment for an infraction" — is in my view quite compelling but perhaps also somewhat non-obvious and contrarian. It concerns not the content of the laws that are enforced, for instance, whether they curtail basic liberties, but their mode of enforcement. David Estlund observes that among the democratically enacted laws that are illegitimate are not only those that undermine the proper functioning of democratic procedures but also laws that are morally abhorrent for other reasons. He asserts, convincingly, that a "law, passed by proper democratic procedures, that established, as a punishment for anything, being boiled in oil would be neither legitimate nor authoritative even though it has no real antidemocratic dimension to it."[41] The feature that renders this law illegitimate relates to the punishment attached to its violation, that is, to its mode of enforcement rather than to its content. While nobody is boiled in oil these days, excessively cruel punishments are by no means a thing of the past. Today, people are punished by being locked up in a prison cell, and it is arguable that this is an extremely inhumane punishment, too. As Chris Surprenant and Jason Brennan observe, "[d]epriving someone of freedom, subjecting them to extended risk of physical and sexual abuse, forcing them to remain locked in a small space, and in some cases, keeping them isolated and without entertainment for extended period[s] [is] barbaric."[42] Incarceration also causes considerable collateral damage by negatively affecting people who are personally close to the incarcerated person and may depend on his or her support, such as family members, partners, and friends. Surprenant and Brennan imagine that an outsider might offer the following account of incarceration as a punishment:

> You […] enslave your convicts, place them under constant surveillance, remove their privacy, dehumanize them, bore them, psychologically torture them, and subject them to near constant threats of capricious physical and sexual abuse. You *ruin* their lives, and you make it so that these people provide nothing of value to society, either. And you do this all at tremendous monetary expense. […] [Y]ou punish criminality with prolonged dehumanization punctuated by capricious, unexpected brutality.[43]

[40] Lee, McCauley, and Abadi (2020).
[41] Estlund (2007, p. 111).
[42] Surprenant and Brennan (2019, pp. 70–71); see also Huemer (2018).
[43] Surprenant and Brennan (2019, p. 72).

Now consider again the example of death by boiling in oil. Assume, for the sake of argument, that drug offenses, theft, or tax evasion were punished by boiling the delinquent in oil. It is plausible that even if we assume that the laws that criminalize these practices and specify the punishment were democratically passed, democratic theorists should dismiss them as illegitimate on account of the disproportionate cruelty of the punishment attached to their violation. The punishment is profoundly inhumane, and its inhumanity nullifies whatever democratic legitimation the laws may have received. It would evidently be wrong to enforce these laws and to boil in oil the drug user or dealer, the thief, or the tax evader. While incarceration is certainly less inhumane than boiling in oil, it is, I submit, still sufficiently inhumane and excessive as to defeat the legitimacy of some laws that result in people being incarcerated. I am not saying that incarceration is never justified. Some wrongdoers, such as serial killers, rapists, and terrorists, ought to be locked away so as to prevent them from causing further harm.[44] But incarceration as a punishment for nonviolent crime is unjustifiably inhumane. Thus, many instances of incarceration, especially but not exclusively in the USA, are so inhumane that we should question the legitimacy of the laws responsible for them.[45]

What I am suggesting, then, is that government surveillance is problematic when it is used to enforce laws that are illegitimate because of the inhumanity of the punishment attached to their violation. That is, there is a considerable risk that government surveillance is abused to enforce laws that are illegitimate because of their mode of enforcement. Although most democratic theorists focus on the content of laws rather than their mode of enforcement (Estlund being an exception), I take this concern about government surveillance to be consonant with the spirit of much of democratic theorizing, which acknowledges that grossly inhumane legislation is illegitimate irrespective of the democratic legitimation it may have received.[46]

Third, the use of surveillance to enforce laws may be objectionable because the democratic institutions of established liberal democracies are *already* defective. So far, my argument assumed that the democratic procedures in established liberal democracies are by and large doing a good job at generating democratic legitimacy, although it was acknowledged that they might decay (first problem) or on occasion produce illegitimate laws by violating procedure-independent standards (second problem). The third problem arises from the observation that the democratic procedures of established liberal democracies are *already* defective and may thus fail to secure the legitimacy of the laws that surveillance is used to enforce. They are defective by the standards of at least a number of influential mainstream theories of political legitimacy.

[44] See again Surprenant and Brennan (2019, p. 85).

[45] Similarly, Surprenant and Brennan encourage juries to make use of their right to nullify the law (2019, pp. 140–141).

[46] To be sure, at least Brennan is a libertarian, but while his and Surprenant's critique of incarceration might be *characteristically* libertarian, it is by no means *exclusively* libertarian.

For instance, many proponents of deliberative accounts of political legitimacy hold that policies are legitimate only if they emanate from ideal political deliberation. Seyla Benhabib asserts "that legitimacy in complex modern democratic societies must be thought to result from the free and unconstrained public deliberation of all about matters of common concern."[47] But, as many have observed, actual political deliberation does not at all conform to this ideal.[48] Or consider how John Rawls conceives of legitimacy:

> [T]he idea of political legitimacy based on the criterion of reciprocity says: Our exercise of political power is proper only when we sincerely believe that the reasons we would offer for our political actions – were we to state them as government officials – are sufficient, and we also reasonably think that other citizens might also reasonably accept those reasons.[49]

Often, however, the exercise of political power is not justified by public reasons in the way envisaged by Rawls and his followers in the public reason tradition. Estlund, defending an epistemic theory of democratic legitimacy, holds that "[d]emocratic legitimacy requires that the procedure can be held, in terms acceptable to all qualified points of view, to be epistemically the best (or close to it) among those that are better than random."[50] But it is fair to say that actual democratic procedures in established liberal democracies, however, worthy of respect and protection, are not close to being the epistemically best among those that are better than random. Estlund himself, acknowledging the problem of voter ignorance, notes that he is unsure whether the requirements of epistemic proceduralism will ever be met.[51] The neo-republican approach ties legitimacy to the concept of non-domination and to popular control over government. Philip Pettit, who has offered the most comprehensive account of neo-republicanism, states: "[A] state will be legitimate just insofar as it gives each citizen an equal share in a system of popular control over government."[52] Again, due to existing inequalities between citizens, virtually no democracy conforms to this ideal, as Pettit himself observes.[53]

I cannot and need not here review all theories of political legitimacy. This selective review suffices to illustrate that at least *several* prominent theories of political legitimacy formulate standards of legitimacy that established liberal democracies do not meet. Perhaps, this is unsurprising. Democratic theorists are in the business of

[47] Benhabib (1994, p. 26). According to John Dryzek, the core claim of deliberative democracy is "that outcomes are legitimate to the extent they receive reflective assent through participation in authentic deliberation by all those subject to the decision in question" (2001, p. 651). Some theories of deliberative democracy are ambiguous as to whether legitimacy requires actual or hypothetical deliberation (e.g., Cohen, 1997a; Habermas, 1996). Whether, according to these theories, legitimacy is damaged by the defects of actual deliberative procedures is somewhat unclear. The letter of these theories seems to say "no," but their spirit suggests "yes.".

[48] See, e.g., Huemer (2013, pp. 61–64).

[49] Rawls (1997, p. 771).

[50] Estlund (2007, p. 98).

[51] Estlund (2007, p. 14).

[52] Pettit (2014, p. 22).

[53] Pettit (2014, pp. 136–140).

outlining to-be-emulated political ideals. They do not seek to provide descriptively adequate accounts of the imperfect status quo. But it means that if we take these theories at face value, the legitimacy of most policies enforced in established liberal democracies is in doubt. This problem has, to my knowledge, hardly been addressed in the literature, and its precise implications remain to be explored.[54] At this point, I want to cautiously point out that, by the standards of several notable theories of legitimacy, many laws seem to lack legitimacy and that there may be something problematic about enforcing such laws. To the extent that government surveillance is used to enforce such imperfectly legitimated laws, government surveillance is problematic, too.

Note that the problem of defective legitimacy affects not only laws that are enforced with the help of government surveillance but also government surveillance as a policy itself. If existing democratic procedures do not meet the requirements necessary for democratic legitimation, the actual decision-making processes that lead to the introduction of surveillance programs may fail to ensure their legitimacy. Indeed, given the secretive nature of many surveillance operations and the importance of transparency for political legitimacy, the problem may be particularly acute for surveillance policies.[55]

To summarize, the three subproblems are as follows: (1) even if established liberal democracies are, by and large, legitimated to enforce laws today, their democratic institutions may decay in the future. Existing surveillance data and infrastructure might then be used for illegitimate purposes. (2) Even if established liberal democracies possess the procedural institutions that generate democratic legitimacy, there are procedure-independent standards that may defeat the legitimacy of laws decided by these institutions. The inhumanity of incarceration may be such a defeater. Government surveillance is objectionable if it is used to enforce such laws. (3) It is unclear to what extent established liberal democracies really possess the procedural institutions that generate democratic legitimacy, if judged by the standards of several prominent theories of political legitimacy. It is arguable that government surveillance is problematic when it is used to enforce laws whose legitimacy is in doubt.

To be sure, the established liberal democracies I have considered are, as of today, not authoritarian tyrannies (trivially). Also, some of the most salient mass surveillance operations, such as those uncovered by Snowden, serve to fight terrorism and similarly serious crime. One might argue that if any laws are legitimate, it is laws against terrorism and serious crime. They ought to be enforced even when they have resulted from imperfect democratic processes, and incarceration may be a morally justified response to the violation of these laws. Arguably, people who plot terrorist attacks ought to be put behind bars. However, democratic institutions are increasingly under threat, with many experts fearing an authoritarian backlash.[56] And as

[54] Kirshner (2018) and Pettit (2014, pp. 136–140) discuss the related problem of whether citizens have a duty to obey the law in defective democracies.

[55] On the transparency requirement, see, e.g., Pettit (2014, p. 215). I owe this observation to Irina Schumski.

[56] See, e.g., Applebaum (2020), Levitsky and Ziblatt (2018), and Snyder (2018).

surveillance technologies become more sophisticated and citizens more desensitized to being monitored, it is likely that government surveillance will progressively expand beyond the purpose of counterterrorism and the like.[57] Indeed, already today, surveillance is used to enforce rather questionable legislation. One of the most extensive surveillance operations, said by some to eclipse that of the National Security Agency, is run by the US Drug Enforcement Agency (DEA). Through the "Hemisphere Project," the DEA has access to a vast database of phone data, provided by telecommunication company AT&T, to prosecute the "war on drugs," one of the US's most questionable policy programs.[58] Another controversial surveillance operation is carried out by the US's Immigration and Customs Enforcement (ICE). It uses facial recognition to scan millions of driver's licence photos, possibly in an effort to track down undocumented immigrants.[59] To such surveillance programs, the above legitimacy concerns seem readily applicable. These programs also demonstrate that government surveillance is expanding rapidly and often in an unchecked manner — the DEA's surveillance was secret until accidentally uncovered, and the ICE proceeds without seeking state or court approval, let alone approval of the driver's licences' owners — giving a foretaste of what is to come. Surveillance is thus likely to continue expanding beyond the prevention of terrorism and serious crime. The more government surveillance is leading to the "total enforcement" of the law, the more applicable the above concerns about legitimacy become.

4 Conclusion

Having distinguished three potential reasons for concern, I have argued that, ultimately, we ought to be concerned about whether collected surveillance data may be accessed and about what the data are used for. The mere collecting of surveillance data, though involving privacy losses of sorts, does not constitute a compelling reason for concern in its own right, over and above the other two concerns. Debates about the meaning of privacy, though insightful, need not be settled for the ethical assessment of government surveillance. One chief problem with government surveillance in democracies is that it may be used to enforce laws that ought not to be enforced — a problem that will become increasingly acute as government surveillance expands.

I conclude with a caveat regarding the implications of my argument. The aim of this essay was to get a better grip on what is pro tanto objectionable about modern government surveillance in established liberal democracies. I have made no attempt

[57] Besides, the risk of this happening has repercussions in the present. If there is a risk that surveillance data are used for illegitimate purposes in the future, citizens' freedom and autonomy is curtailed in the present as they will adjust their behavior in anticipation of these risks. For related discussions on the "chilling effects" of surveillance, see, e.g., Macnish (2018, p. 428), Solove (2006), Stahl (2020, p. 85), and Thomsen (2020b, p. 381).

[58] Shane and Moynihan (2013)

[59] Harwell (2019); Harwell and Cox (2020)

to provide an all-things-considered judgment of its ethical acceptability. Nothing I have said entails that government surveillance is never justified. To call for an end to all government surveillance on the basis of the above concerns, perhaps by appeal to the precautionary principle, would be to ignore the opportunity costs that forgoing government surveillance may involve.[60] As mentioned in the introduction, some scholars have defended government surveillance as a useful instrument for preventing terrorist attacks of a catastrophic scale. An all-things-considered judgment that accounts for these and other potential opportunity costs, which would also require assessing the actual effectiveness of surveillance, cannot be provided within the scope of one article.[61] Indeed, it is doubtful that any such general assessment can be provided, as the moral costs and benefits of each surveillance technique or operation must be judged on its own terms.[62] What I do hope to have achieved is to contribute a new perspective on whether and why we should be concerned about government surveillance and on how the problem of government surveillance relates to questions of privacy and legitimacy.

Acknowledgements The author would like to thank Saskia Nagel, Niël Conradie, Jan-Christoph Heilinger, and Hendrik Kempt for their helpful comments. He is a member of the project group "Regulatory theories of Artificial Intelligence" within the "Centre Responsible Digitality" (ZEVEDI).

Author Contribution Not applicable (single authored).

Funding Open Access funding enabled and organized by Projekt DEAL. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy — EXC-2023 Internet of Production — 390621612.

Declarations

Conflict of Interest The author declares no competing interests.

[60] See Sunstein (2005).

[61] On the questionable effectiveness of the NSA's surveillance program, see Greenwald (2014, pp. 202–205). Refer to Macnish (2015), Rønn and Lippert-Rasmussen (2020), and Thomsen (2020b) for discussions of government surveillance and proportionality, which may be helpful for reaching more comprehensive judgments.

[62] For one moral assessment of a specific surveillance practice, see Thomsen (2020a).

References

Altshuler, T. S., & Hershkowitz, R. A. (2020). How Israel's COVID-19 mass surveillance operation works. Retrieved from https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/. Accessed 03/02/2022

Applebaum, A. (2020). *Twilight of Democracy: The Seductive Lure of Authoritarianism*. Penguin.

Belli, L. (2021). The largest personal data leakage in Brazilian history: Why the rest of the world should be worried, and think hard about how to create a data protection culture. Retrieved from https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/. Accessed 03/02/2022

Benhabib, S. (1994). Deliberative rationality and models of democratic legitimacy. *Constellations, 1*(1), 26–52.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *New York University Law Review, 39*(6), 962–1007.

Brownlee, K. (2016). The civil disobedience of Edward Snowden: A reply to William Scheuermann. *Philosophy and Social Criticism, 42*(10), 965–970.

Christiano, T. (2008). *The Constitution of Equality: Democratic Authority and its Limits*. Oxford University Press.

Cohen, J. (1997a). Deliberation and democratic legitimacy. In J. Bohman & W. Rehg (Eds.), *Deliberative Democracy* (pp. 67–92). MIT Press.

Cohen, J. (1997b). Procedure and substance in deliberative democracy. In J. Bohman & W. Rehg (Eds.), *Deliberative Democracy* (pp. 407–438). MIT Press.

Denyer, S. (2018). China's watchful eye. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/. Accessed 03/02/2022

Dryzek, J. (2001). Legitimacy and economy in deliberative democracy. *Political Theory, 29*(5), 651–669.

Dunnage, J. (2016). Policing and surveillance. In P. Corner & J.-H. Lim (Eds.), *The Palgrave Handbook of Mass Dictatorship* (pp. 119–130). Palgrave Macmillian.

Estlund, D. (2007). *Democratic authority: A philosophical framework*. Princeton University Press.

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy and Technology, 29*(4), 307–312.

Foucault, M. (1975). *Surveiller et Punir: Naissance de la Prison*. Gallimard.

Freeman, S. (1990). Constitutional democracy and the legitimacy of judicial review. *Law and Philosophy, 9*(4), 327–370.

Fried, C. (1984). Privacy: A moral analysis. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 203–222). Cambridge University Press.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Goold, B. (2009). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In D. W. Schartum (Ed.), *Overvakning I en Rettstaat* (pp. 38–48). Bergen: Fagbokforlaget.

Gutmann, A., & Thompson, D. (2004). *Why Deliberative Democracy?* Princeton University Press.

Habermas, J. (1996). *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. MIT Press.

Harwell, D. (2019). FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/. Accessed 03/02/2022

Harwell, D., & Cox, E. (2020). ICE has run facial-recognition searches on millions of Maryland drivers. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/. Accessed 03/02/2022

Henderson, S. E. (2016). Fourth amendment time machines (and what they might say about police body cameras). *University of Pennsylvania Journal of Constitutional Law, 18*(3), 933–973.

Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge University Press.

Henschke, A. (2020). Privacy, the Internet of things, and state surveillance: Handling personal information within an inhuman system. *Moral Philosophy and Politics, 7*(1), 123–149.

Hern, A. (2016). Database allegedly containing ID numbers of 50m Turks posted online. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/apr/04/database-allegedly-containing-id-numbers-of-50m-turks-posted-online. Accessed 03/02/2022
Hoye, J. M., & Monaghan, J. (2018). Surveillance, freedom and the republic. *European Journal of Political Theory, 17*(3), 343–363.
Huemer, M. (2013). *The Problem of Political Authority: An Examination of the Right to Coerce and the Duty to Obey*. Palgrave Macmillan.
Huemer, M. (2018). Unconscionable punishment. In C. W. Surprenant (Ed.), *Rethinking Punishment in the Era of Mass Incarceration* (pp. 34–48). Routledge.
Kirshner, A. S. (2018). Nonideal democratic authority: The case of undemocratic elections. *Politics, Philosophy & Economics, 17*(3), 357–376.
Kleinig, J. (2009). The ethical perils of knowledge acquisition. *Criminal Justice Ethics, 28*(2), 201–222.
Lankov, A., & In-ok, K. (2011). The decline of the North Korean surveillance state. *North Korean Review, 7*(2), 6–21.
Lee, W.-Y., McCauley, E., & Abadi, M. (2020). Taiwan used police surveillance, government tracking, and $33,000 fines to contain its coronavirus outbreak. Retrieved from https://www.businessinsider.com/taiwan-coronavirus-surveillance-masks-china-2020-6/. Accessed 03/02/2022
Lever, A. (2008). Mrs. Aremac and the camera: A response to Ryberg. *Res Publica, 14*(1), 35–42.
Levitsky, S., & Ziblatt, D. (2018). *How Democracies Die*. Broadway Books.
Lundgren, B. (2020). A dilemma for privacy as control. *The Journal of Ethics, 24*(2), 165–175.
Macnish, K. (2015). An eye for an eye: Proportionality and surveillance. *Ethical Theory and Moral Practice, 18*(3), 529–548.
Macnish, K. (2018). Government surveillance and why defining privacy matters in a post-Snowden world. *Journal of Applied Philosophy, 35*(2), 417–432.
Macnish, K. (2020). Mass surveillance: A private affair? *Moral Philosophy and Politics, 7*(1), 9–28.
Mainz, J. T., & Uhrenfeldt, R. (2021). Too much info: Data surveillance and reasons to favor the control account of the right to privacy. *Res Publica, 27*(2), 287–302.
Menges, L. (2020a). Did the NSA and GCHQ diminish our privacy? What the control account should say. *Moral Philosophy and Politics, 7*(1), 29–48.
Menges, L. (2020b). A defense of privacy as control. *The Journal of Ethics, 25*(3), 385–402.
Menges, L. (forthcoming). Three control views on privacy. *Social Theory and Practice*
Moore, A. (2003). Privacy: Its meaning and value. *American Philosophical Quarterly, 40*(3), 215–227.
Moore, A. (2008). Defining privacy. *Journal of Social Philosophy, 39*(3), 411–428.
Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy, 17*(5/6), 559–596.
Nozick, R. (1974). *Anarchy, State, and Utopia*. Basic Books.
Perez, E. (2013). NSA: Some used spying power to snoop on lovers. Retrieved from https://edition.cnn.com/2013/09/27/politics/nsa-snooping/index.html. Accessed 03/02/2022
Persson, I., & Savulescu, J. (2012). *Unfit for the Future*. Oxford University Press.
Pettit, P. (2014). *On the People's Terms: A Republican Theory and Model of Democracy*. Cambridge University Press.
Pilon, R., & Epstein, R. A. (2013). NSA surveillance in perspective. *Chicago Tribune* (12.06.2013)
Posner, R. A. (2005). Our domestic intelligence crisis. *The Washington Post* (21.12.2005).
Rawls, J. (1996). *Political Liberalism*. Columbia University Press.
Rawls, J. (1997). The idea of public reason revisited. *The University of Chicago Law Review, 64*(3), 765–807.
Roberts, A. (2015). A republican account of the value of privacy. *European Journal of Political Theory, 14*(4), 320–344.
Roessler, B. (2005). *The Value of Privacy*. Polity Press.
Rønn, K. V., & Lippert-Rasmussen, K. (2020). Out of proportion? On surveillance and the proportionality requirement. *Ethical Theory and Moral Practice, 23*(1), 181–199.
Ryberg, J. (2007). Privacy rights, crime prevention, CCTV, and the life of Mrs Aremac. *Res Publica, 13*(2), 127–143.
Scheuermann, W. E. (2014). Whistleblowing as civil disobedience: The case of Edward Snowden. *Philosophy and Social Criticism, 40*(7), 609–628.
Shane, S., & Moynihan, C. (2013). Drug agents use vast phone trove, eclipsing N.S.A.'s. *The New York Times*. Retrieved from https://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html. Accessed 03/02/2022

Smith, P. T. (2020). A neo-republican account of just state surveillance. *Moral Philosophy and Politics, 7*(1), 49–71.
Snowden, E. (2019). *Permanent Record*. Metropolitan Books.
Snyder, T. (2018). *The Road to Unfreedom: Russia, Europe, America*. Tim Duggan Books.
Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.
Solove, D. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review, 44*, 745–772.
Sorell, T. (2011). Preventive policing, surveillance, and the European counter-terrorism. *Criminal Justice Ethics, 30*(81), 1–22.
Sorell, T. (2018). Bulk collection, intrusion and domination. In A. I. Cohen (Ed.), *Philosophy and Public Policy* (pp. 39–60). Rowman & Littlefield.
Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology, 18*(1), 33–39.
Stahl, T. (2020). Privacy in public: A democratic defense. *Moral Philosophy and Politics, 7*(1), 73–96.
Sunstein, C. R. (2005). *Laws of Fear: Beyond the Precautionary Principle*. Cambridge University Press.
Surprenant, C. W., & Brennan, J. (2019). *Injustice for All: How Financial Incentives Corrupted and Can Fix the US Criminal Justice System*. Routledge.
Taylor, I. (2017). Data collection, counterterrorism and the right to privacy. *Politics, Philosophy & Economics, 16*(3), 326–346.
Taylor, J. S. (2005). In praise of big brother: Why we should learn to stop worrying and love government surveillance. *Public Affairs Quarterly, 19*(3), 227–246.
Thomsen, F. (2020a). The ethics of police body-worn cameras. *Moral Philosophy and Politics, 7*(1), 97–122.
Thomsen, F. (2020b). The teleological account of proportional surveillance. *Res Publica, 26*(3), 373–401.
Thomson, J. J. (1975). The Right to privacy. *Philosophy and Public Affairs, 4*(4), 295–314.
van den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 301–321). Cambridge University Press.
Westin, A. (1967). *Privacy and Freedom*. Atheneum.
Wolff, R. P. (1970). *In Defense of Anarchism*. Harper & Row.
Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.