A neo-republican critique of transparency

The chilling effects of publicizing power

Matthew Hall

Introduction

Democratic legitimacy of some kind has been produced by the transparency regulations brought in to oversee state surveillance in the wake of Edward Snowden's revelations about the secret and often unlawful practices of the NSA in the United States and GCHQ in the UK. Granting citizens knowledge over the scope of the rules governing surveillance, providing opportunities to identify abuses of power, and highlighting unfair or unjust uses of surveillance all go some way toward repairing what is considered to be one of the key harms produced by Edward Snowden's denunciation: a breach of the public's trust.

Viewing the harm of surveillance practices and transparency regulations instead through a perspective of *freedom as nondomination* – the neo-republican conception of freedom – however, illuminates something missing from the debate, which is this: making state surveillance practices more transparent may in fact compound surveillance's harmful effects on freedom. This is because publicizing surveillance power through transparency regulations amplifies surveillance's "chilling effects" on individuals already susceptible to being targeted by surveillance.

From the liberal perspective, publicizing surveillance's existence and its parameters makes it less harmful and more legitimate. This justification, however, fails to account for the arbitrary capacities inherent to surveillance and the effects this produces in those subject to it. My argument, instead, is that for it to be legitimate we would need to be able to contest *why* surveillance is conducted – explicitly, contesting the reasons behind the justifications for using surveillance over certain populations – not merely be informed about *how* surveillance is being conducted. Such an ability would also reduce the harmful effects produced by surveillance in certain populations, effects which are exacerbated by transparency as it is commonly understood.

The chapter will unfold as follows. I will firstly sketch what appears to be the primary justification for embedding practices of transparency into law – repairing public trust – focusing on the UK example by discussing the

Investigatory Powers Act (IPA) passed in 2016 by the British government. I will argue in the next section that the real problem concerning surveillance and transparency is the harm being done to our freedom as nondomination. This is the core of my argument, showing from a neo-republican perspective – a perspective within political theory which maintains that liberty is being free from domination – how surveillance and the transparency practices overseeing it impact our liberty as nondomination. I will diagnose existing proposals as instances of what I will call “hierarchical transparency,” which a republican framework reveals to be inadequate. This will provide an analytical framework for demonstrating that the characteristic problem with the version of transparency on offer is not an issue of information or openness, but rather one of the power represented by surveillance practices. I will then distinguish between the “demos” and the “demoi” to show that “the public” from whom transparency practices are seeking approval is not the same constituency as the one being harmed by surveillance. Finally, I will offer a route out of these problems by offering my own conceptual innovation to the debate on transparency, the concept of “horizontal transparency” – an analytical framing and political proposal at the same time.

Snowden’s “denunciation,” transparency proposals, and public trust

While security services by their nature need to act secretly, the discovery that they were operating not only secretly but also in a way that appeared to be unrestrained, excessive, and unregulated, as the public learned from Edward Snowden’s revelations (Bauman et al. 2014), brought the legitimacy of these types of surveillance practices into question. Characterizing the problem as a breach of trust between citizen and government led to a recognition that, to rebuild trust, maintain public confidence in institutions, and guarantee continued consent for security agencies, some kind of increased transparency was needed. Despite welcome democratic by-products of transparency proposals – such as norms of openness and procedures to limit the uses of surveillance, which can act as a benchmark and mechanism for holding abuses of power to account – foregrounding public trust as the justifying principle for surveillance regulations contributes to the hierarchical structure of transparency, which reproduces dominating effects on certain groups, as I will show.

In the aftermath of the Snowden revelations John Naughton, Emeritus Professor of The Public Understanding of Technology at the Open University and prominent journalist of technology and surveillance in the UK, was invited to contribute to the inquiry led by the UK’s Intelligence and Security Committee of Parliament and stated:

What it comes down to in the end is essentially a proposition “trust us,” and in the past two or three years we have seen a number of startling

examples of where serious British public institutions have demonstrated vividly that they are not worthy of trust.

(Intelligence and Security Committee of Parliament 2015, 108)

The then Shadow Home Secretary, Yvette Cooper MP, argued that the work of the Agencies

depends on the framework of consent, and that depends on there being a level of knowledge and understanding as well. I think if we try to keep everything behind closed doors, the danger is that we will undermine the trust that we need for the Agencies to be able to do their work.

(*ibid.*, 107)

The report into the inquiry concluded that “the Government acknowledged the requirement for greater transparency and openness ... placed great value in public confidence, recognising that without the public’s support they cannot fulfil their functions” (*ibid.*, 107).

While increased clarity with which to restore public confidence was deemed important, the fact that this is inherently partial was concurrently recognized, with the report stating that

[i]t could also be argued that it may be beneficial for adversaries to be “kept guessing” about the range and scale of the Agencies’ capabilities: terrorists’ behaviour may be constrained if they believe that the Agencies have more access than they do.

(*ibid.*, 108)

This demonstrates a recognition that unclear yet present surveillance has the power to cause effects in subjects whether they are under surveillance or whether they are not. When those subjects are deemed to be “criminal,” this is classed as deterrence; “chilling” begins when lawful behavior is affected (Stoycheff et al. 2019). However, the line between what is deemed to be “criminal” by the security services, and what is not, and therefore who as a result is considered to be “deterred” and who is “chilled” cannot be so clearly drawn.

The assumption underpinning transparency practices and regulations is that citizens now know what the security agencies are doing (to a certain extent), know that surveillance and data collection are regulated, and know that legally underpinned guidance with penalties is attached to the use of citizens’ data. Citizens can therefore trust the surveillance practices more fully, because we can trust that surveillance is being conducted in a way that is clearly defined for reasons we, the public, find acceptable.

What the republican perspective brings to light, however, is that greater trust does not necessarily equal greater democratic legitimacy. Social trust is something like a recognition of vulnerability that is accepted on the basis of

assumed good faith on the part of the other party. Placing such good faith in a relationship implies we believe that the other party will be “trustworthy” toward us (Hardin 2006). For authorities, trust has been described as “the invisible institution” that grants legitimacy to other institutions and government actions. Rebuilding trust is, in a sense, a way to rebuild the legitimacy of institutions that may have lost it (Rosanvallon 2008). Trust also has a relationship to risk. Trust anticipates and has expectations of the future. Risk is wary of it and seeks to reduce probabilities that the future will not be like we do not want it to be. Transparency, in an important sense, is the act of making the practices and operations of power visible and reducing an aspect of *unknowability*, thus inviting those subject to state power to trust it on the basis that the consequences of trusting it are now more knowable. In this way a relationship between transparency and risk is apparent, and reducing a perceived risk that institutions will behave badly increases public trust in, and hence the democratic legitimacy of, those institutions.

Yet, *distrust*, rather than trust, is in fact a vital component of maintaining *liberty* in democracies. Surveillance itself as a concept was not always understood as something that authorities and organizations did to citizens and individuals, but rather, surveillance, invigilation, and denunciation are historical methods for citizens to “oversee democracy.” Benjamin Constant, a republican thinker, spoke in 1819 of conducting “surveillance in hatred” when asserting that “[e]very [good] constitution is an act of distrust” (Rosanvallon 2008, 7), grounding the principle of liberty in the reality that power needs invigilating because office holders cannot be trusted with that power, putting our liberty is at risk.

Desirable political arrangements from a neo-republican perspective are not to ensure that goodwill and good faith flourish in order to buttress social trust in institutions. Rather, the motivation is to ensure that citizens and their liberty are *not* dependent on the goodwill and good faith of political actors and institutions. Being distrustful of the potential consequences of relying on another’s power to treat you in the way you wish to be treated is healthy for democratic freedom. The key point for republicans is to *secure* against the possibility of interference by other actors, not trust that they will behave in good faith toward you and your interests. The desire is to have some kind of control and input so that your life is not subject to the whims of officials, authorities, or rules which you have no say over and no possibility to contest.

Of course, a complete lack of trust is dangerous for democracy as it erodes the preconditions for negotiating a shared life. The antivaccination movement, for example, tries to persuade parents to refuse inoculations for their children, premised on skepticism of authority figures such as doctors and medical professionals and denying the credibility of science. This type of distrust is unpolitical in the sense that it offers no shared grounds for cooperatively resolving such a conflict of competing beliefs. Republican distrust, on the other hand, can be characterized as a healthy guardedness against

political power and authority, not a distrust that seeks to eradicate all faith in an authority.

Rather than responding to the breach of trust by state surveillance agencies revealed by Edward Snowden by trying to rebuild faith and confidence that security agencies are now doing what it is we want them to – to mend the distrust – we can instead use this breach of trust to ask deeper questions about surveillance's effects on those subject to it. For example, we can ask questions about surveillance's purposes, to generate a healthy distrust of state surveillance activities with more depth and breadth. My contention is that, when interpreting the harm of both surveillance and transparency regulations through the concept of freedom as nondomination, *embedding distrust* toward power in a politically constructive way like this seems a more realistic approach.

In order to make this argument, it is first necessary to explain the concept of freedom as nondomination and how we can use it to understand some of the harms of mass surveillance which the mainstream debate occludes.

Surveillance and freedom as nondomination

Freedom as nondomination differs conceptually from negative liberty in a number of important ways. The conception of negative liberty tells us we are free to the extent that we are not interfered with by humanly imposed external obstacles to our choices, classically demonstrated through laws or physical coercion. For republicans, on the other hand, it matters not only whether we are interfered with in this way but also whether we *could* be interfered with in some way, and whether the ability to shape or prevent that interference is beyond our control.

The classic example used in the literature to demonstrate this is the figure of the Roman slave who is relatively free on a day-to-day basis if they happen to have a benign master. In this context the slave may be able to freely socialize, visit the market, have free time throughout the day to be in town, and so on. However, the extent of their unfettered free choices comes at the grace and favor of their master. At any time, the ability to freely act can be removed if the master's mood changes, or if the master simply decides to restrict the slave's freedom in some way. This is a status of domination, no matter the amount of day-to-day negative liberty this slave enjoys. Not only is this a status of unfreedom, but it also engenders *freedom-reducing* behavioral and psychological impacts. Not knowing what behaviors may bring censure from the arbitrary power held over you, embodied in the master, or what the limits to your free behavior are, and having no control over those limits or when they could be imposed, induces effects such as self-censorship, toadying to authority, deference, second-guessing, anxiety, and fear (Skinner 1998). These effects then further limit the capacity to act freely within the space of the free choices that the dominated agent, represented in the figure of the slave, apparently enjoys.

This accurately characterizes part of the problem with mass state surveillance. The key factor for republicans is not whether surveillance constitutes a violation of privacy, nor whether it directly coerces your choices or is used by someone to directly interfere in your life in some way, although this is important. It is the very *possibility* that “arbitrary” interference in your life could occur, due to the gathering of information about you, that is the offense to liberty. In this scenario, all surveillance can be liberty-reducing in certain ways if we cannot know for sure what surveillance is conducted and why, have no meaningful control over the rules governing its practice now or in the future, have no meaningful control over what may be done with our data at some future point, and have no resources to contest surveillance practices.

Importantly, these types of “arbitrary” capacities to use our data or interfere in our choices may produce the freedom-reducing impacts documented in republican literature. These types of effects are demonstrated today in the “chilling effects” caused by surveillance (Stoycheff et al. 2019). Those who suspect they are subject to surveillance may engage in avoidance strategies designed to offset potential or perceived consequences.

In the context of post-Snowden security surveillance, the limits of free inquiry on the internet, for example, are unknown, but it *is* known that you are watched and monitored in some way. If it is unclear what types of communication are definitely allowed or disallowed, or what would be of interest or not of interest to authorities, but *it is known* that searching for these (currently unknowable or unclear) things online may produce a response from authorities of some kind, then this can be interpreted as a situation of domination parallel to that of the controlled Roman slave, and a range of chilling effects may be likely. Chilling effects are well documented, but republican conceptions of freedom as nondomination bring a hitherto missing dimension to explain *why* it is that our free activities are “chilled.”

More broadly, if you know that there is the capacity to use the data you generate through your day-to-day internet activity and that that data can be used in ways that are opaque or unclear, it seems plausible that this may also cause some of the impacts observed by republicans when individuals are exposed to power of this type. The machine learning and algorithmically driven Big Data processes that are not directly interfering in your choices now but are building a potential capacity to interfere in your choices at some future point by accumulating knowledge about you represent another version of this type of potential harm. That surveillance and data are so often used for reasons other than those originally justified means that reassurances about data use remain unconvincing in the face of justified skepticism about the future reliability of those reassurances because of the lack of meaningful control over both why and how surveillance is deployed and data is collected. This type of power, for republicans, is considered to be arbitrary power.

Arbitrariness and chilling effects

I will now lay out precisely what arbitrariness means in this context, and why we have reason to be concerned that increases in transparency alone will be insufficient to curtail the arbitrary power that state surveillance represents. Arbitrary means something quite specific in political theory, beyond simply signifying random or unpredictable. Power can be procedurally arbitrary, meaning that the limits and aims of that power are not effectively stipulated, restrained, and fixed and are not made common knowledge to all parties potentially affected by that power (Lovett 2010). Substantive arbitrariness is a power that does not suitably track or, more specifically, is not “forced to track” the welfare and world-view of agents affected (Pettit 1997, Lovett 2010).

Procedural arbitrariness can be offset if sufficient democratic oversight is applied to the scope of the rules governing surveillance, and this is made common knowledge to all. The important aspect of state surveillance considered here, however, is that it produces *effects* distinct from the procedural basis of its justification. These “chilling effects” are produced regardless of whether democratic oversight is sufficiently applied. This demonstrates that a substantively arbitrary aspect to surveillance remains – that which potentially acts against the interests of the subject under surveillance – even if the rules governing it are common knowledge and clearly stipulated. Keeping in mind these distinctions between procedural and substantive arbitrariness is relevant for understanding the distinct approaches to transparency I will unpick below and the solutions I believe can be offered to offset the domination produced by them.

Firstly, a type of transparency that addresses the legal basis and scope of rules to which surveillance practices must adhere mirrors the version of securing “procedural non-domination” espoused by the republican theorist Frank Lovett in his influential book, *A General Theory of Domination and Justice* (2010). He claims that completely eradicating “procedural arbitrariness” – making the rules that govern power absolutely clear, stringently regulated, and common knowledge to all subject to that power – eliminates or radically reduces domination, diminishing uncertainty and other freedom-reducing impacts (Lovett 2010). In such a scenario, he claims, individuals with full and detailed knowledge of the rules of power could then “plan around” those rules and navigate an authority with power over them, because they now know what precisely is proscribed, and what is not. This, it is claimed, increases freedom of the individual by granting them the capacity to avoid knowable consequences (ibid.). This type of procedural nonarbitrariness requires the rules restraining that power to be effective, external, and common knowledge.

Criticisms of this approach have noted a problem, however. This type of procedural transparency could mean that a fully rationalized and well-publicized system of *oppressive surveillance* could, in principle, be acceptable

and nonoffending to freedom. An example used to make this point is the “pass laws” that existed in apartheid-era South Africa. There was a well-defined and strict monitoring system that dictated where black citizens could or could not go at certain times of day. Procedural nonarbitrariness, or procedural transparency, would mean that individuals in this scenario are *not* dominated. Knowing precisely what is allowed, by whom and at what times, eliminates uncertainty and unknowability. However, publicizing the rules of power clearly, making them common knowledge to all, does not in and of itself reduce the harm of that power, simply because its operation becomes transparent and clearly defined. Lovett swallows these criticisms, asserting instead that not everything that is bad about power means that it is dominating. The situation in apartheid-era South Africa could be described as unjust and oppressive, but that does not mean it is dominating in the republican framework he is offering, he claims. For my case, while a clear distinction can be drawn between the oppressive enforcement of rules in apartheid-era South Africa and state surveillance of citizens in liberal democracies, the same procedural issue is relevant.

In the example of internet activity, if it is clear and transparent that very specific and perhaps illegal internet activity would be monitored by security agencies, such as activities for aiding and abetting terrorism, and security agencies were strictly limited to that task alone, then this would seem to produce more areas of activity in which we could operate free from uncertainty, reducing domination and its freedom-limiting effects.

Since the time of the Snowden revelations, and the resulting legal oversight and transparency, the chilling effects have in fact expanded, however. Jon Penney has studied search traffic to what he terms “privacy sensitive” Wikipedia articles, and he found that they experienced statistically significant declines. These declines were not only apparent in the immediate aftermath of the Snowden revelations in 2013, but also demonstrated a downward trend over the long term, up to and including the same year that the IPA was passed into law, 2016 (Penney 2016). Longer-term trends will be interesting to study, but the processes since the Snowden revelations – public awareness, consultation on security activities, and, finally, legally embedded transparency practices – have evidentially generated further chilling-type effects.

Paradoxically, then, Snowden’s denunciation has in fact reduced the liberty of citizens in an important way. Prior to Snowden’s revelations and the increased transparency they created, citizens at large were exposed to arbitrary power but without their knowledge. This means that “free” action, such as searching at will for privacy-sensitive articles online, was less hindered than it is now. Such activity was conducted without the clear knowledge that state agencies were gathering and collecting information on what one was searching for – knowledge that now exists. To use the omnipotence metaphor, to a certain extent the public was in the panopticon prior to Snowden’s denunciation but was not aware that the guard tower watching over them was a guard tower

at all. Those subject to state surveillance without their knowledge prior to the Snowden revelations would not have felt as compelled to limit their own freedom of choice, as they had less knowledge of the capacity of the state to watch over them.

This is a status recognizable to republicans, and even with the apparently increased freedom to act and make choices that comes with the ignorance of a power watching you, you cannot be considered free under the conception of freedom as nondomination. This situation is what Philip Pettit calls “alien control” (Pettit 2008). Alien control is the condition in which you are exposed to a power with an arbitrary capacity to interfere in your life, but you are unaware of that capacity. As such, you operate as if you are not being watched or controlled. Limits to your free action, based on the preferences that a power has over what you choose to do, mean that you are unfree, however. In many ways alien control is more conducive to negative liberty, as described, insofar as your liberty is not limited by your knowledge of any power with an arbitrary capacity to interfere in your life. Chilling and self-censorship are absent. However, unknown to you, there are still limits to your choices, the boundaries of which you may one day bump up against, producing consequences from the surveilling power of which, until that point, you were unaware. With security surveillance in the shadows, unconstrained and unregulated, citizens at large were previously dominated in this way because of these unknown yet present consequences attached to certain behaviors and choices, yet they more “freely” made their choices about how to behave under the surveillance of which they were unaware.

Bringing state surveillance practices into the light, then, through surveillance practices that are now more publicized, can produce *more* chilling effects. Now enlightened to the knowledge that you are exposed to a power with an arbitrary capacity to interfere in your life in some way, avoidance strategies, self-censorship, and second-guessing pertain.

Hierarchical transparency

The problem with this type of transparency offered in Western liberal democracies is that it is *hierarchical transparency*. By this I mean, firstly, that the imbalance of power represented by surveillance is made clear to those subject to it through practices and processes of transparency, producing the chilling effects discussed above, and secondly, what is made knowable to the public, or which rules are given clarity and why surveillance is used, and over whom, is still decided by the surveilling power, not those subject to it.

The amplification of chilling effects produced by transparency practices can be explained if we consider these practices to be only “partial transparency.” It may be that it is still not quite clear enough to the public, activists, and journalists what definitely is and what definitely is not allowed. What is “criminal,” what is “extremism,” what is “radicalism,” who are “enemies,”

and what is considered a “threat to the state” by security agencies all remain ambiguous. Is it *really* true that a journalist’s sources will not be tracked down in some way if they release sensitive information? Is the line between what is considered “sensitive” and what is a “threat to state security” really clear? Are political organizations, curious citizens, journalists, and certain minority groups susceptible to state surveillance *really* clear about what may be of interest to state agencies that may produce unwelcome attention for those groups? It seems that *publicizing* the scope of the rules by which the public are being monitored on a mass scale, for reasons now apparently clear but importantly open to interpretation, provides only enough knowledge to generate uncertainty among those who feel they may be subject to surveillance. Becoming aware of a power held over you, but without a full knowledge and understanding of its operation and the consequences for certain types of your own behavior, is to realize you live in a status of domination. Procedural transparency of this type cannot completely eliminate the uncertainty associated with surveillance practices that produce chilling effects.

Of course, total transparency cannot eliminate uncertainty either. If *everything* state security agencies did could, in principle, be made public, it might well encourage the opposite of what is sought by calls for transparency. For state surveillance agencies to remain effective, they would be compelled to engage in something like a massaging of the truth, deliberate ambiguity of surveillance aims, or bland descriptions of operations. These types of evasions or half-truths are the symptoms of a hierarchical transparency that must protect the operative capacities of whatever authority is being transparent (O’Neill 2002, 64).

Philip Pettit develops the conception of freedom as nondomination further in a way that is helpful for understanding hierarchical transparency. Pettit describes the difference between negative liberty on the one hand, and freedom as nondomination on the other, as the difference between freedom and free rein (Pettit 2014). When a horse is given free rein, the rider allows it to go where it wills. It may turn left, right, slow down, and speed up, apparently free as the reins hang loose. However, those reins are still held by a rider, and the reason the horse has free rein is not due to the horse’s preference, but the preference of the rider. While running freely may *feel* like freedom, someone is still in the saddle. True freedom is not free rein, in which you have a wide range of choices to enact; true freedom is *unbridled freedom*, with no one in the saddle granting you license to have free rein (Pettit 2014).

To be free in this unbridled way we must be able to choose the options that we prefer, despite the preference of others over us. This has three component parts. Firstly, we can choose freely if we have the capacity to choose an option and choose it without the interference of others. Secondly, we must have the room and resources to choose what it is we *prefer to choose*, not just the choices available. For example, a prisoner cannot liberate herself by choosing not to want to walk in the park and therefore “choosing” to stay in

her cell. Altering your preferences to fit the options offered by others is no freedom. Finally, you must be able to be free to choose despite the preferences of others. For example, ingratiating yourself with a prison guard in order to be allowed license to walk in the park – even though this is *your* preference this time – is still no freedom because it depends on the will of another (Pettit 2014, 28–54).

This conception of freedom as nondomination, as may be clear by now, is constitutively linked to how nondomination is secured. In other words, in order to be free to choose a range of preferred options you must have the room and resources to *secure* that range of options for yourself. This requires the power to do so, despite the attitude of the more powerful toward you. In republican terms this is secured through “anti-powers”: public laws, norms, and the capacities of citizens to participate in governing, and to contest, impede, and block arbitrary uses of political power in order to enforce those democratically determined laws and norms. This driving principle does not identify clear, unambiguous cases of freedom but rather offers a roadmap to liberate individuals from harmful forms of dependence on others, based on the security of norms, laws, and antipowers with which to defend their liberty.

In this context, then, hierarchical transparency, a process which sets the scope of the rules and the purposes behind those rules and then publicizes them, making them common knowledge to all subject to that power, *demonstrates* the limits of our freedom. Transparency regulations allow us to “liberate” ourselves by *choosing new options* on the basis of the newly available information. However, choosing new options because our preferred options may prove too risky (because we are not sure about what is surveilled and for what reason, or what may be done with our data) is no freedom at all, as we have just seen above. Unless we have the political resources to exercise choices beyond the preferences of the surveilling authorities, set out in the transparency regulations determining the scope of the rules, we remain dominated. Hierarchical transparency regulations simply set out more clearly the boundaries to the free choices we have; they set out the extent to which our free rein runs.

Defending the “demos,” dominating the “demoi”

In response to my argument above, it might be objected that existing democratic procedures can counteract the dominating tendencies of publicized surveillance. If the *demos* is considered to fully participate in the rulemaking of the state, then the power represented by state surveillance counts as *authorized interference* and is therefore nondominating. If we can consider the UK as democratic to a certain extent, then this could be considered sufficient to prevent us from being dominated. The rules are governed by a recognizably democratic mechanism in this version, and it could be claimed that we have

sufficient rights to defend ourselves from undue intrusion by state surveillance authorities.

Surveillance scholars have long noted a particular problem with surveillance, however, one that is relevant for claims such as this: namely, the differential treatment under surveillance between individuals and groups, a tendency most famously espoused as “social sorting” (Lyon 2003). This problem reasserts itself in the question of who the demos is – to whom justifications about surveillance are given. Surveillance is engaged in sorting *within* the demos; it does not monitor and defend a homogenous demos in order to keep it free and safe from the private domination of *others*.

In doing so, state surveillance is in fact monitoring the *demos*. The term “*demos*” is used in other republican theories to discuss the delineation that can be drawn *within* political entities between different *peoples*. For example, the European Union is discussed in republican terms as a *demosi-cracy*, which is to say, different peoples engaged with one political authority in a way that grants that authority political legitimacy (Bellamy 2019). Applying this thinking to surveillance reveals the inherently differential nature of the effects produced by surveillance.

A relationship of power involving surveillance of a different type can demonstrate the problem that surveillance represents for the *demos*. Consider the case of police body cameras, or “bodycams.” The filming of encounters between police and citizens, it is claimed, increases trust in officers by making those encounters transparent and concomitantly produces up to 93% reductions in complaints about the police from the public (Ariel et al. 2016). The implication in transparency claims of this type is that either the dishonesty on behalf of some of “the public” is addressed – they now no longer make complaints they know are spurious – or that the police now behave in a manner more befitting their role, now that they know they are being monitored. However, what may look like a way of making the police more accountable doubles as a means to use surveillance over groups already subjected to more intensive policing and surveillance practices – those groups and classes in society likely to encounter the police.

This brings into question whether the declared purpose behind police bodycams – improving the accountability of the police – is the true motivation and outcome of this type of surveillance encounter. Transparency in this instance is not only for the population who are subject to more surveillance but is also used to build trust with a public not involved in the encounter but whose confidence is required to secure the trust that maintains the legitimacy of the police.

The questions here from a republican perspective would be: do the transparent practices now overseeing encounters between the public and police through police body cameras in fact represent domination of the individual being filmed? And is the reduced volume of complaints and contestation of police practices premised not on the rebuilding of trust and honesty, which

seems to underpin those claims, but rather a result of surveillance *producing* conforming behaviors among those subject to surveillance in those interactions, through domination, fear, self-censorship, and anxiety?¹

Surveilling more of the *demoi* in this way does produce transparency, but not necessarily for “the public” (or *demoi*) upon which the police directs its surveillance cameras. Instead, encounters between the police and surveilled subjects are made transparent to another “public” not susceptible to the potential conformity produced by being under surveillance: the *demos* that is not involved in the encounter, but on whose trust the police rely.

Up until now I have offered a critique of the transparency of surveillance practices, showing how it compounds the core harm of surveillance, which I interpret as domination. In what follows I will return to questions of trust and liberty in order to develop my horizontal transparency proposals, which, while necessarily incomplete, are driven by a principle of constructive *mistrust* of the purposes of surveillance and the harmful effects it has on those it monitors.

Horizontal transparency

Horizontal transparency is a way of fleshing out what meaningful control might look like, which we could build toward in the present. My notion of horizontal transparency is premised on the reality of state surveillance and transparency argued for thus far, namely the fact that even democratically authorized surveillance with regimes of transparency and oversight dominate individuals in ways that are *prima facie* unjustifiable – as demonstrated by the chilling effects they produce. It is not sufficient to transparently expose the scope of rules governing surveillance practices; the justification of the purposes for which surveillance is used must be transparent as well, in order for them to be challenged.

To address this reality, constitutionally embedded *mechanisms of mistrust* can secure our liberty under surveillance (Rosanvallon 2008). In practice, this could mean an array of citizen invigilation mechanisms and organizational forms that act as “editorial” rights (Bellamy 2013) and “anti-powers” to impede power *that has already been democratically authorized*.

There are two aspects of state surveillance that can be impeded with invigilation mechanisms: the harmful effects of surveillance, even when democratically authorized – the “chilling effects” – and the purposes for which surveillance is conducted. Such an alternative framework of demands requires not just more regulatory proposals but normative resources with which those subject to the most intensive state surveillance practices can challenge the basis on which they are under surveillance and the chilling effects produced.

The key to horizontal transparency is a recognition that substantive inequalities produce differentiated harms under surveillance. This is demonstrated by the sociological and economical fact of the *demoi*. While equality as a

desirable end state is beyond the discussion held here, there are strategies we can discern from societies that were both chronically antiegalitarian yet profoundly pro-liberty, such as the Florentine republics in which republican political philosophy was born. If we accept that surveillance's character is to identify and distinguish between unequal sections of society (to sort them) we can draw on strategies that pull back the veil of formal equality to reveal the class structure of society to combat the sorting inherent in surveillance's logic.

Thanks to Snowden, an opportunity to challenge the imperatives by which mass state surveillance is driven presents itself. This goes significantly further than simply regulating and publicizing already existing surveillance practices. Snowden's denunciation could be considered a first step in an activity of democratic mistrust that could engineer a basis for holding security agencies and government institutions to account for the justifications they offer for putting certain groups and individuals under surveillance, not only their legal basis for doing so. Horizontal transparency not only *looks through* to the purpose of surveillance but also seeks to *see the effects* surveillance produces in the populations it monitors, even when democratically authorized.

The difference between democratic oversight that legitimizes surveillance practices (which may be harmful) and republican nondomination is the difference between "authorial" and "editorial" rulemaking (Bellamy 2013). This distinguishes my approach from participatory, deliberative, and liberal approaches. The capacity to impede and block political power that has been democratically authorized but turns out to be dominating (like state surveillance) is a prerequisite for freedom in the view I am articulating here: freedom as antipower, in Pettit's term (Pettit 1996). This constitutes a bottom-up, "monitorial" (Schudson 1999) and "contestatory" (Pettit 1999) approach, in order to challenge the legitimate limits of what can and should be watched, even if democratically authorized. Horizontal transparency, unlike hierarchical transparency, constitutes "editorial" rights over the political power that is expressed by surveillance, following its authorization, rather than "authorial" rights concerning its legal basis, no matter the harm it presents for certain groups and members. In manifestly and profoundly unequal societies, there needs to be a normative basis for contesting things that have passed through existing "democratic" procedures (even leaving aside the question of how "democratic" these are, given how many are excluded from the rulemaking procedures). This is the point of the "editorial" control requirement.

Transparency implies "looking through" or "seeing through." Making this line of sight nonhierarchical is to enable people to see through to *the purposes* behind the surveillance, and to *see clearly* the consequences and harmful effects that are produced. Doing this holds not only the rules and legal basis of surveillance to account – as is currently the case – but furthermore holds the purposes and effects of state security surveillance to account. This more widespread and comprehensive vision of surveillance – inward to its purposes, and outward to the chilling effects it produces – is the key to horizontal

transparency. Mass state surveillance would need to be not only transparent in its proclaimed aims but also transparent in the *effects* it produces in certain populations and activities, and in why those effects are produced.

What these types of proposals require, to widen lines of vision of political power and the antipowers to then contest political power, is not the separation of powers at an institutional level, as is common to liberal democracies, but the separation of *political power* at the ground level. Such an approach focused on ground-level political power accepts that enforcing formal equality in an environment of substantive inequalities does not reduce the harm generated by unequally applied surveillance. To both recognize the dominating impact of democratically authorized surveillance, while simultaneously being able to act against it, necessitates a series of antipowers; antipowers such as independently constituted invigilation task forces (Hoye and Monaghan 2018), community panels with political oversight of police practices, tribunals, and the right to block, impede, and challenge surveillance.

In the context of security surveillance specifically, avenues for citizen contestation into the actual categories, classifications, and descriptions of surveillance – of “radicals,” “threats,” and “extremists” – that surveillance’s “sorting” is premised on, can provide horizontal transparency. The recent “Spycop” scandal in the UK, where mass police infiltration was revealed to be taking place into a huge array of peaceful, noncriminal political organizations and civil society groups (Woodman 2018), seems to demonstrate that the state security agencies and police’s interpretation of what constitutes a “threat,” what is “radical,” “extreme,” or “criminal,” needs to be opened up to public debate, not left to the police and security services to define, classify, and then use to monitor those they deem fit that category.

Of course, democratic and liberal approaches could also reflect on the harm caused by surveillance practices and adjust accordingly. To promote republican freedom, however, it is necessary to equalize power imbalances among citizens in order to defend against dominating power. This requires the production of political arrangements to contest those surveillance practices and the antipowers necessary to defend oneself against surveillance.

Conclusion: freedom, self-government, and the eyeball test

The primary purpose of this chapter has been to argue that transparency practices may in fact produce new harms to the freedom of certain groups and individuals under surveillance, demonstrated by chilling effects and articulated through freedom as nondomination. I have also begun to make suggestions as to how this could be countered, with a new line of vision and contestation: horizontal transparency.

This is underpinned by a republican account of power and freedom, and one final crucial point to consider with horizontal transparency needs

reemphasizing. Being able to participate in the way described above, and enact antipowers successfully, is premised on having more or less equal power to do so, whereas those most susceptible to harm by surveillance are often precisely those with less societal and political power. Some type of political equality is a precondition for freedom from a republican perspective. While a full account of political equality is beyond the scope of this chapter, I will end by sketching what I take to be a key republican insight into what substantive, as opposed to merely formal, equality requires.

Social sorting points to the fact of a chronically unequal society being one reason why surveillance is necessary from the state's point of view. The "eye-ball test," however, describes the basis of self-government as premised on equalizing power as far as is possible so that citizens can look one another and the government "in the eye" without deference, fear, or favor (Pettit 2012). Enacting horizontal transparency without first doing something about the power imbalances that produce much surveillance over certain individuals, groups, and communities in society in the first place would be insufficient.

To do so would require taking seriously the ability of those in the demo subject to liberty-reducing surveillance and domination to defend themselves. And this requires the political capacities to normatively contest their condition. For example, opening up public contestation only to ask the question "who is it that ought to be watched by police body cameras and why?" may not provide the desired result. Would it be the case that "we," the public (the demos), would decide we are in fact happy with the people the police are currently monitoring, compounding the problem? In a society of unequal resources, classes, and groups, the logic of the state to categorize and monitor these groups – to sort them (Lyon 2003) – produces surveillance, even if it is to treat those groups in a formally equal way. Opening up participatory avenues to contest state surveillance needs to ensure that those who come forward to participate do not embed the problem being addressed; imbalances of power ricochet through institutional proposals designed to overcome imbalances of power.

To reduce domination by surveillance, actual economic and political power *external* to surveillance practices needs to be equalized to lessen the divisions between citizens that drive much surveillance and to grant those citizens who are subject to surveillance the political capacities necessary to challenge the justifications for the surveillance to which they are subjected. Such societal and historical realities are obviously beyond the reach of this conclusion, but they should not be beyond the considerations of how state surveillance and transparency are deployed, and the domination and chilling effects they produce.

What my argument does show, however, is that transparency practices as they are currently constituted – as hierarchical flows of information – exacerbate the chilling effects experienced by certain groups exposed to surveillance. To secure liberty under surveillance, meaningful participation in the

production of society's information, which produces the justifications for surveillance, is necessary. I have tried to show how the concept of horizontal transparency could contribute to this project.

Note

- 1 Rachel Hall promotes a similar idea in her excellent work on the “transparent traveler” (2015), in which those subject to procedures such as airport security are forced into certain types of docile and submissive behaviors as they are compelled to be transparent *for* security officials. The same type of coerced submissiveness could be said to be at play here. However, whereas in the case of the transparent traveler it is the subject being forced to perform an “aesthetics of transparency” *for* authority, here the issue is the effects produced in the subject by an authority itself performing transparency.

References

- Ariel, Barak, Alex Sutherland, and Darren Henstock. 2016. “Contagious Accountability. A Global Multisite Randomized Controlled Trial on the Effect of Police Body-Worn Cameras on Citizens’ Complaints Against the Police.” *Criminal and Justice Behaviour* 44(2): 293–316.
- Bauman, Zygmunt, Didier Bigo, Paul Esteves, Elspeth Guid, Vivienne Jabri, David Lyon, and Rob B. J. Walker. 2014. “After Snowden: Rethinking the Impact of Surveillance.” *International Political Sociology* 8(2): 121–44.
- Bellamy, Richard. 2013. “Rights, Republicanism and Democracy.” In *Republican Democracy: Liberty, Law and Politics*, edited by Andreas Niederberger and Philipp Schink, 253–75. Edinburgh: Edinburgh University Press.
- Bellamy, Richard. 2019. *A Republican Europe of States*. Cambridge: Cambridge University Press.
- Hall, Rachel. 2015. *The Transparent Traveler: The Performance and Culture of Airport Security*. Durham, NC: Duke University Press.
- Hardin, Russell. 2006. *Trust*. Cambridge: Polity Press.
- Hoye, J. Matthew, and Jeffrey Monaghan. 2018. “Surveillance, Freedom and the Republic.” *European Journal of Political Theory* 17(3): 343–63.
- Intelligence and Security Committee of Parliament. 2015. *Privacy and Security: A Modern and Transparent Legal Framework*. 12 March 2015, HC 1075, House of Commons. London. United Kingdom.
- Lovett, Frank. 2010. *A General Theory of Domination and Justice*. Oxford: Oxford University Press.
- Lyon, David. 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Abingdon: Routledge.
- O’Neill, Onora. 2002. *A Question of Trust*. Cambridge: Cambridge University Press.
- Penney, Jonathon W. 2016. “Chilling Effects: Online Surveillance and Wikipedia Use.” *Berkeley Technology Law Journal* 31(1): 117–82.
- Pettit, Philip. 1996. “Freedom as Anti-Power.” *Ethics* 106(3): 576–604.
- Pettit, Philip. 1997. *Republicanism: A Theory of Freedom and Government*. Oxford: Clarendon Press.

- Pettit, Philip. 1999. "Republican Freedom and Contestatory Democratization." In *Democracy's Value*, edited by Ian Shapiro and Casiano Hacker-Cordon, 163–90. Cambridge: Cambridge University Press.
- Pettit, Philip. 2008. "Republican Liberty: Three Axioms, Four Theorems." In *Republicanism and Political Theory*, edited by Cecile Laborde and John Maynor, 102–30. Oxford: Blackwells.
- Pettit, Philip. 2012. *On the People's Terms: A Republican Theory and Model of Democracy*. Cambridge: Cambridge University Press.
- Pettit, Philip. 2014. *Just Freedom: A Moral Compass for a Complex World*. New York: Norton.
- Rosanvallon, Pierre. 2008. *Counter Democracy: Politics in an Age of Distrust*. Cambridge: Cambridge University Press.
- Schudson, Michael. 1999. *The Good Citizen: A History of American Civic Life*. New York: Harvard University Press.
- Skinner, Quentin. 1998. *Liberty before Liberalism*. Cambridge: Cambridge University Press.
- Stoycheff, Elizabeth, Juan Liu, Kai Xu, and Kunto Wibowo. 2019. "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects." *New Media & Society* 21(3): 602–19.
- Woodman, Connor. 2018. "Spycops in Context: Counter-Subversion, Deep Dissent and the Logic of Political Policing." Centre for Crime and Justice Studies, www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/Spycops%20in%20context%20-%20counter-subversion%2C%20deep%20dissent%20and%20the%20logic%20of%20political%20policing.pdf.