

Privacy, Democracy and Surveillance

Annabelle Lever

University of Geneva

annabelle.lever@unige.ch

Sept. 2 2013

Forthcoming in *The Philosopher's Magazine*, autumn 2013

<http://philosophypress.co.uk/>

It is especially hard, at present, to read the newspapers without emitting a howl of anguish and outrage. Philosophy can heal some wounds but, in this case, political action may prove a better remedy than philosophy. It can therefore feel odd trying to think philosophically about surveillance at a time like this, rather than joining with like-minded people to protest the erosion of our civil liberties, the duplicity of our governments, and the failings in our political institutions - including our political parties – revealed by the succession of leaks which have dripped away this the summer. Still, philosophy can help us to think about we should do, not merely what we should believe. Thus, in what follows I draw on my previous work on privacy, democracy and security, in order to highlight aspects of recent events which – or so I hope – may prove useful both for political thought and action.

Not all forms of surveillance are alike in their implications for people's civil and political liberties. So even when we think that some form of surveillance or monitoring of people's behaviour, movements and communications is warranted, there are important distinctions to be made over how this monitoring should take place. This is an aspect of debates on surveillance and security which is often overlooked, because people are primarily concerned to ask *when* surveillance is justified – assuming that we know *what* forms of surveillance we are concerned with, and *the range of alternatives* that we need to consider. Comparing racial profiling, random searches and universal searches, however, shows that there are very considerable moral and political differences in the way we can scrutinise and monitor each other, even if you disagree with me that racial profiling is particularly hard to justify, because it places the burdens of collective security primarily upon a disadvantaged social group, and is likely, as well, to exacerbate unjustified prejudices and hostility.

Likewise, the differences between a uniformed police presence, CCTV and a bus conductor or bathroom attendant are important to the justification of security in public places, and the justification of the one does not automatically mean that we should accept the others. The disadvantage of CCTV relative to a visible, uniformed police presence, for example, is that it provides no one who can come to our aid and, depending on how likely we are to forget that it is there, and how impetuous we are, it may do little to prevent crime. The prime uses of CCTV, therefore, are likely to be in the post-hoc identification of criminals, whereas deterrence as well as solidarity may be better fostered by the presence of identifiable people who are able to provide some oversight of public areas, even if they are also engaged in other tasks.

People have privacy interests in public which we can provisionally define as interests in anonymity, seclusion, confidentiality and solitude. These are morally and politically important, even though it is unreasonable to demand the same degree of protection for our privacy in public places, to which all have access, as in areas where we are entitled to exclude others. Privacy in public places, such as parks, streets, museums, cinemas, pubs matters because many of us live in such crowded conditions that public space provides some of our best chances for peace and quiet, for a heart-to-heart with friends, or for relaxation and fun.

It is a mistake, therefore, to suppose that people lack legitimate interests in privacy once they leave their houses, or to suppose that privacy on public transport, the park or, even, at work, is a contradiction in terms simply because these are all areas in which others may see us, overhear what we say, or bump into us without violating our moral or legal claims to privacy. After all, being snooped on and overheard by a passer-by are not the same, nor does groping on the tube seem any more morally acceptable than at a cocktail party. It is therefore important, when thinking about security, to consider the differences between our privacy interests in public – our interests in anonymity, seclusion, confidentiality and intimacy, for example – and their implications for the different forms of surveillance, if any, which may be justified.

A few years ago, for instance, some police forces in the UK attempted to force pubs to install CCTV on their premises, as a condition for getting or retaining their entitlement to

serve alcohol. (<http://www.theguardian.com/uk/2009/mar/12/cctv-pubs-privacy-ico>; <http://www.theguardian.com/uk/2009/mar/16/pubs-police-cctv-in-bars> ; and, more generally, <http://www.theguardian.com/uk> search 'CCTV+pubs'). Now alcohol clearly exacerbates tendencies to violence and aggression, and may make it easier for people to steal other people's property, and to deceive or coerce them. But to insist on treating all pubs as though they are the same is to ignore the differences for both privacy and security of small pubs, where people regularly meet and know each other, and the large, anonymous drinking places increasingly found in bigger cities. The threats to security posed by the former are very much smaller than the latter, and the intrusion on privacy created by CCTV may well be much greater, because of the greater degree of intimacy and informality characteristic of such settings. In short, the costs to privacy of surveillance are likely to vary even within spaces that are characteristically thought of as public.

We should therefore be wary of ignoring people's interests in privacy on the internet, including in areas of the web which are open to all, rather than 'closed' or part of recognisably private conversations. Clearly the web, like the street, the park or the cinema, cannot be exempt from police scrutiny, nor can it be off-limits to social researchers. However, just as our privacy interests in parks, cinemas, streets and pubs are more complex and diverse than is often assumed, so our privacy interests in public communications, including on the internet, cannot be simply divided into a public area – where police scrutiny or social research is assumed to pose no problems – and a private area where complex legal safeguards are supposed to be required before we are subject to such scrutiny. If we would be troubled by the routine presence of unidentified police officers in health-clinics or public libraries, we should be uncomfortable with the suggestion that no special justification or supervision is required for police scrutiny of, and participation in, debates on public websites.

A uniformed police presence might inhibit us from picking up the information pamphlets on sexually transmitted diseases discretely available in the health clinic or seeking information about cancer or drug addiction in the library. But official surveillance that we do not know about leaves us vulnerable to misinterpretation of our thoughts and actions as well as to the misuse of state power. Once widespread, it creates a climate in which we are encouraged to

see others as threatening, and ourselves as powerless and defenceless individuals. Surveillance can adversely affect the quality of our social relations and our subjective sense of ourselves, then, as well as our objective capacities to shape our own lives, whether we are concerned with places that are open to all, or those in which we are able to seclude ourselves.

Our legitimate interests in privacy are not negligible, or inherently of lesser importance than our interests in security. Nor are they always selfish or self-regarding. The latter assumption, I suspect, often underpins ideas about the lesser importance of privacy relative to other things. But a moment's reflection reminds us of the importance of confidentiality to our ability to keep *other people's secrets*, even when it might be in our personal interests to disclose them; and of the importance of anonymity, solitude and confidentiality to our abilities to act with tact, discretion and consideration for others, even when we do not share their particular sensibilities, interests and commitments. Just as our willingness to grant privacy to others can reflect respect and trust - and be valued and desired for that reason - so our willingness to act anonymously, confidentially or discreetly can reflect a mature and considered decision to avoid burdening others with our problems, or to avoid forcing on them the need to confront features of the world with which they may be unwilling or unable to cope.

Our interests in privacy, then, can be varied and inescapably tied to our sense of ourselves as moral agents. They are not, therefore, especially trivial, or of obviously lesser importance than our interests in self-preservation - individual, or collective. This is partly because our interests in privacy are not purely instrumental but seem sometimes to be ways of affirming, even constituting, ourselves as people to be trusted, respected, deserving of liberty, equality and happiness. Indeed, while privacy can be necessary to our security and be desired for that reason, people are sometimes willing to risk their lives and health in order to maintain anonymity, seclusion and confidentiality. This would be unreasonable were privacy less important than security but if, as I have suggested, it is inseparable from relationships and ideals that have ultimate value, then a willingness to risk physical security for privacy can be comprehensible, and even admirable.

Not all arguments for limiting privacy in the interests of security are consistent with democratic principles, or with the ways in which privacy can express our collective, as well as individual, interests in freedom, equality and solidarity. We should therefore be wary of 'ethical guidelines', such as those propounded by Sir David Omand, which assume that whenever it is impossible to protect both privacy and security, the former should bow before the latter. (<http://www.theguardian.com/uk/2009/feb/25/personal-data-terrorism-surveillance> ; <http://www.theguardian.com/commentisfree/2013/jun/11/make-surveillance-ethical-and-effective> ; <http://www.ippr.org/publication/55/1675/the-national-security-strategy-implications-for-the-uk-intelligence-community>). Omand's 'ethical guidelines' for when the state is entitled to limit people's privacy in the interests of security include 'sufficient sustainable cause; integrity of motive; proportionate methods; proper authority; reasonable prospect of success; no reasonable alternative'. Such guidelines ignore the ways in which privacy can be *necessary* to the security of at least some people, given prejudice, discrimination and unfounded fear and hostility. In addition, they overlook the ways in which democratic government and principles depend on our willingness to constrain the quest for security in the interests of the privacy of members. In short, one worry about Sir Omand's pronouncements are their one-sided and unqualified character, which turn a problem in *jointly protecting* two values into a reason to *sacrifice one* to the other. This is unjustified, and has the predictable consequence that some people's security will be threatened because we are contemptuous of their privacy.

The US Supreme Court decision in *NAACP v. Alabama* (357 US. 1958) is interesting in this context. The NAACP is the National Association for the Advancement of Coloured People, and was originally founded as a non-profit membership association. By 1957 the state government of Alabama was seriously concerned with its growing membership and use of civil disobedience against racial segregation. The state government therefore sought access to the membership list of the NAACP under an existing state statute aimed at ensuring that business associations be held responsible for any damage to life, liberty or property that their activities cause. But while the Court accepted that the government of Alabama had a legitimate interest in ensuring that associations, like individuals, can be held accountable for harm to others, it denied that this required them to have access to the full membership list of the NAACP, rather than to the names and contact information of its leaders. Freedom of

association, the Court argued, is a fundamental democratic right, and protections for anonymity can be essential to its exercise. So while the state has a duty to provide security for its citizens, the Court maintained that people's interests in privacy and associative freedom legitimately constrain the ways that the state may fulfil that duty.

According to Sir David's guidelines, 'integrity of motive' is essential to determine when our interests in security justify curtailing people's privacy by spying on them. But this appears to confuse the conditions necessary for the state to be morally justified in *exercising* its rights of surveillance with the question of *what rights* – whether moral or legal - the state is entitled to claim. At best, integrity of motive is relevant to the former, however as the US Supreme Court realise, in *NAACP v. Alabama*, it is irrelevant to the latter.

For example, the purpose of requiring the NAACP's to disclose its membership list was not fear for people's lives, liberty or property, so much as the desire to thwart the movement for Civil Rights. The motives for requiring the membership list in 1957, then, were not particularly reputable. They would surely have failed Omand's test of 'integrity of motive'. Nonetheless, as the Court thought, democracy requires governments to be able to hold associations to account for their actions, although not to record the names, addresses (or, as happened in the UK, the license plates and photos) of ordinary people, even if they are engaged in social protest, or campaigning for radical change. In short, Omand's six criteria - 'sufficient sustainable cause; integrity of motive; proportionate methods; proper authority; reasonable prospect of success; no reasonable alternative' - provide guidance on the morally appropriate claiming and exercise of rights of surveillance. They do *not* tell us what moral or legal rights of surveillance follow from the state's duty to keep us all safe.

Democratic Education and Deliberation are necessary to the justification of any public policy on surveillance, although they do not figure in Omand's 'guidelines' for legitimate surveillance. Moreover, while governments and think-tanks stress the importance of education in fighting extremism, and in justifying surveillance, most proposals in this area are astonishing bland and vague. Above all, they seem utterly disconnected from the thought that, as citizens, we *need and are entitled* intelligently to discuss government policy on surveillance, just as we would employment policy, education, welfare or policy on crime and punishment. We may differ in our desire and ability to master many of the relevant

details or controversies - though this is unlikely to be any truer of surveillance than of employment or education policy, let alone pensions or the EU constitution. And some things have to stay secret. We will therefore need to combine historical cases, the experience of other countries, and hypothetical examples in lay as well as expert discussions. But this is perfectly compatible with the assumption that ordinary citizens might be interested in, and should be able to discuss, the principles and basic practices of surveillance, as of counter-terrorism more generally.

So, we ought to be able to consider whether to exclude wiretapped evidence in court, and the grounds on which people are subjected to wire-tapping, and we should not need any more specialised access to information than we would for a comparable issue of economic or foreign policy. We should be free to debate whether, or how far, the state should protect the credibility of spies even at the cost of their involvement in serious crimes like murder or racketeering – or, as more recently, their engagement in duplicitous sexual relationships with those on whom they are spying. The basic information and principles necessary to form an intelligent opinion on such questions needs to be generally available, and should be no harder to obtain than comparable information on other areas of public policy. In short, until we accept that citizens are *entitled to* understand the principles and main practices of surveillance and counter-terrorism, and to debate these openly, we will lack an essential element in a democratic response to terrorism - and to crime more generally. People must be able to talk honestly about their laws, institutions and practices - their history, justification, their strengths, weaknesses and the alternatives to them. This applies to policies on surveillance no less than to other collective policies.

CONCLUSION

Not all forms of privacy are consistent with democratic government – but nor are all forms of security. Unfortunately, even when we are concerned *only* with those forms of privacy and security which adequately reflect people's claims to govern themselves, it is likely that we may have to constrain or compromise people's moral and legal rights quite severely on occasion. It is essential to a democratic conception of security, therefore, that we have adequate *continuous* public discussion on the ethics and empirics of security, just as we do on economic and foreign policy. It is not simply that these are often related - security and,

especially, surveillance is now a competitive industry in the UK, where we lack much in the way of manufacturing – but because foreign policy and the policy of our allies, who are not always democratic, can materially affect our needs for security, as well as our prospects of meeting those needs.

Philosophy clearly has a role in improving debate on surveillance, because reasoned judgements in the area of security are hard to make not simply because of the emotions involved, but also because of the difficulty of extrapolating from individual cases and small samples, of handling counterfactuals, and because so much inevitably turns on explaining what *didn't* happen. Philosophy, therefore – and not just moral or political philosophy, but philosophy of science and social science too- can improve our understanding of the ethics and empirics of surveillance and security. But philosophy is no substitute for political engagement and it may be that, as philosophers, our attention now needs to move from the topic of surveillance to that of political action.

Annabelle Lever is Associate Professor of Normative Political Theory at the University of Geneva. She is the author of *On Privacy*, (Routledge, 2011), and the editor of *New Frontiers in the Philosophy of Intellectual Property*, (Cambridge, 2012). Her articles on sexual and racial equality, security and democracy are available at www.alever.net .