FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency
Collaborative Project

SURVEILLE Deliverable 4.4: Ethics and surveillance in authoritarian and liberal states

Due date of deliverable: 30.04.2013
Actual submission date:

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP04 Prof. Martin Scheinin (EUI)

Author(s): Dr. Kat Hadjimatheou (UW)

Ethics and surveillance[1] in authoritarian and liberal states

Introduction

This paper discusses the ways in which the use of surveillance by the state might lead to authoritarian government. Concerns about the causal link between state surveillance and authoritarianism motivate some of the most prominent and persistent criticisms of surveillance. It has long been commonplace for critics to respond to the adoption of a new surveillance technique with the caution that we are 'sleepwalking towards a surveillance state' (UK ICO, 2010); or by inviting comparisons with techniques used by the Stasi[2] or George Orwell's thought police (Open Society Institute, 2009); or by observing that our governments now know more about us than most totalitarian regimes could ever hope to discover about their own citizens (Grayling, 2009; REF). Such warnings also pervade academic discussion of surveillance. But the arguments put forward in support of them are often obscure or poorly articulated, and the mechanics of the implied slippery slope from surveillance to authoritarianism are rarely explained in detail. This paper surveys, presents systematically, and examines critically a range of arguments put forward in support of the claim that there is a causal link between surveillance and authoritarianism. In doing so, it attempts to shed light on the relationship between surveillance and authoritarianism and to clarify the nature of the threat surveillance might pose to liberal democratic government.

The paper begins by distinguishing liberal democratic governments from authoritarian states and indicating some of the hallmark features of each. It then moves on, in Section 2, to discuss five ways in which the proliferation of state surveillance is thought to lead via a slippery slope to authoritarianism. The discussion in this section identifies a variety of regulatory and other mechanisms that can help to prevent states using surveillance in authoritarian ways. Section 3 discusses two further criticisms of surveillance, both of which rest on the claim that surveillance creates an asymmetry of power between individuals and states which can lead to authoritarian uses of state power. The nature of this asymmetry and proposals to correct it are examined in detail.

---

[1] This deliverable was originally entitled 'ethics and data retention in liberal and authoritarian states' because recent history shows that surveillance by European authoritarian states most commonly took the form of the updating, storage and sharing of files about individuals. Indeed, as is widely recognised (Raab, 2010:255), the collection, storage, processing and sharing of data- also known as 'dataveillance' is the primary form of state surveillance today. Despite this, the term 'data-retention' has been replaced with 'surveillance'. While it is true that 'surveillance' is a broad term incorporating mere watching where no record is kept, 'surveillance' continues to be the term most associated in common speech with all kinds of watching and monitoring by the state.

[2] As did UK Prime Minister David Cameron in a speech to his Conservative party, see http://www.telegraph.co.uk/news/politics/david-cameron/5552360/Video-Cameron-in-trouble-for-fake-German-accent.html. Last accessed March 2013.

1. Background

Liberal democracy and authoritarianism describe approaches to government that lie at opposite ends of a theoretical spectrum. Roughly speaking, liberal democracies aim to represent the people and to govern in ways consistent with respect for the freedom, autonomy and equality of individuals. In contrast, authoritarian governments aim to lead and manage the people in ways that ensure their conformity with the goals set by the state. Authoritarian governments tend to see those who do not share those goals or want to replace them with other goals as enemies of the state. In reality, states can be and can become more or less liberal, more or less democratic, and more or less authoritarian. Liberal states can and sometimes do accumulate powers to surveille in non-democratic ways. Likewise, they sometimes use surveillance powers in authoritarian ways and for illiberal purposes. Governments accumulate surveillance powers in non-democratic ways when they enact them by decree; when they are imposed by an external authority with little democratic legitimacy, such as an unelected and unrepresentative international institution; or when they adopt them by hasty vote in spite of broad public opposition. Surveillance powers are used in authoritarian ways when they are unconstrained or insufficiently constrained by checks and balances of rule of law, impartiality, transparency and accountability: secret surveillance, surveillance outside a legal framework, surveillance that is subject to poor oversight, and surveillance whose proportionality cannot be effectively contested by individuals are all examples. When surveillance powers are used in authoritarian ways, people are exposed to rights-violations resulting from the corrupt, disproportionate, discriminatory uses that result from a lack of rule of law and democratic constraints. Illiberal purposes to which surveillance powers might be applied include the silencing of political dissent, the pursuit of personal or party interests and the restriction of rights in order to impose ideological orthodoxies amongst other things. The arguments considered in this paper spring from a concern that the increasing proliferation of surveillance techniques empowers, encourages and enables liberal states to use them in authoritarian ways and for illiberal purposes.

2. Slippery slopes from surveillance to authoritarianism

A number of the arguments put forward in support of the claim that the use of surveillance invites or opens the door to authoritarian government claim that there is a slippery slope from the former to the latter. These arguments take the following form: the use of power for authoritarian purposes is unacceptable; surveillance leads to the use of power for authoritarian purposes; therefore surveillance is unacceptable.[3] Slippery slope criticisms of surveillance do not object to surveillance on the ground that it is intrinsically or always itself an authoritarian exercise of power. On the contrary, they often allow that some measures of surveillance would be legitimate or justified when viewed in isolation. However, they claim that even these measures of surveillance are

[3] For an analysis of slippery slope arguments in general see van der Burg, 1991.

nevertheless unacceptable, because in practice they lead to authoritarian uses of power.

The strongest form of slippery slope argument claims that surveillance necessarily or inevitably leads to authoritarian government. Weaker versions claim that surveillance removes or diminishes barriers to authoritarian government. Some slippery slope arguments treat all kinds of surveillance techniques as cumulatively responsible for driving us down the slope (Kateb, 2001). More commonly, arguments focus on the use of mass databases (such as ID card registration schemes, DNA databases, the storage of electronic communication records) because these databases store information that can be used for a broad range of purposes, including authoritarian ones (Clarke, 1994; Balkin, 2008).

Five slippery slope arguments are discussed in this section. The first claims that surveillance makes people more tolerant of authoritarian uses of state power and thus removes one important barrier to its realisation. The second claims that surveillance encourages governments to see and treat people as mere conscripts to their purposes, denying their autonomy. The third claims that surveillance powers will inevitably be used for illiberal ends. The fourth claims that surveillance powers will eventually fall into, and strengthen greatly, the hands of authoritarian regimes. The fifth claims that surveillance powers will be used in authoritarian ways against minority groups.

2.1 Surveillance makes people more tolerant of authoritarian uses of state power

This argument states that the proliferation of surveillance techniques normalises their use and reduces opposition to their application for authoritarian purposes.[4] It begins by pointing out that being monitored and having one's information collected, shared, and analysed without one's full knowledge or meaningful consent has become the norm in many modern societies. This is due in part to the spread of CCTV in many public and private spaces as well as the use by websites of cookies (devices that track browsing histories) and of location tracking on mobile devices amongst other things. Despite the fact that people regularly tick consent boxes indicating their approval of surveillance of their online activities, there is often no readily available alternative to accepting cookies other than closing the webpage, and their ideas about who has access to what data and what they are permitted to do with it are vague and inaccurate (Joinson and Paine, 2007). Similarly, the spread of private and public uses of CCTV means that being captured on CCTV is difficult to avoid. This situation has arisen without the prior knowledge or and often without the prior consultation of those affected. As a result, people are often misinformed about its use and have been shown to overestimate greatly the extent to which they are being monitored, believing that they are constantly watched wherever they go.[5] This may lead to resignation about the inevitability of surveillance. It may also lead

[4] For a philosophical analysis of this argument see Kohn, 2010.
[5] See Graeme Gerrard, Camera Survey for Chesire Extrapolated for the UK, 2011. www.acpo.police.uk.

people to feel unsure whether and when their right to privacy has been violated, which in turn may reduce the extent to which they feel justified in objecting to intrusions and therefore the frequency with which they do so.

As people's expectations of data privacy adjust downwards to this reality, actual objections to intrusion may begin to appear less reasonable and receive less and less public and political support. In many jurisdictions, including that of the European Court of Human Rights, reasonable expectations of privacy are used as a determinant of the boundaries of the legal right to privacy. Any downward adjustment in these expectations therefore reduces judicial ability to limit privacy intrusion (Rosen: 2011;[6]). The same downwards pressure may be exerted on legislative efforts to regulate privacy and data protection. For a variety of reasons, including the rapid pace of technological development, as well as confusion about the status of websites and social networks as private or public spaces and the resulting legal uncertainty about ownership of data, the regulation of surveillance techniques is often retrospective, rather than preventive and anticipatory. Expectations of privacy are already half-formed by the time the opportunity for meaningful political debate and legislative action arises. The feared result is a gradual shrinking of the boundaries of the rights to privacy and data protection, a weakening of the power of the judiciary to protect individuals from unjust intrusion, and a corresponding rise in public indifference to the prospect of ever greater monitoring. Kateb argues that indifference to the 'painless oppression' that comes with a gradual and insidious curtailment of the right to privacy will lead to indifference towards 'blatant forms of oppression' by the state in the future (2001:284).

Some claim that these changing attitudes to and protections of privacy are compounded by an increase in and lack of transparency about state uses of surveillance. This leads to a chilling of legitimate political activity, activity which acts as an important source of opposition to authoritarianism. For example, people may be aware that police have access to a wide range of data including publicly available data, data collected by other state agencies, and communications records. However, they may not be sure how police are using such data. This uncertainty, it is feared, may lead people to avoid visiting certain websites, or to self-censor, in order to pre-empt any potentially damaging conclusions being drawn by police about their preferences and intentions. Concerns of this sort are cited in support of a ban on the police use of data mining techniques, for example (Balkin, 2008).

While these claims identify legitimate concerns about the authoritarian potential of surveillance, there are reasons to think that they inflate the extent of political indifference as well as the extent to which political activity is being chilled. Kateb's claim that people are becoming indifferent to the use of surveillance to oppress them seems contradicted by, for example, the considerable public and indeed political opposition in a significant number of European countries to the imposition of the EU's 2005 Data Retention Directive. This Directive required private providers to store the online communications records of all users for a

[6] See also concurring opinion of Justice Alito in the Supreme Court case US vs Jones. p.10-11.

period between 6 months and 2 years, and make these available to police forces for the purposes of fighting serious crime. This Directive expanded the powers of some EU domestic police forces (others already had the power) to monitor individual activity online. But it did so without giving domestic parliaments the opportunity to debate or influence directly that decision. The widespread resistance to the resulting legislation was hardly proof of political resignation in the face of the prospect of greater surveillance. Indeed, the law is currently being re-written with a view to better respecting individual rights to privacy and data protection.

To the extent that the remaining concerns about the chilling potential of surveillance and the contraction of the right to privacy and data protection are correct, introducing more effective systems of transparency about surveillance techniques may go some way to addressing them. These should be accompanied by effective accountability mechanisms and tools facilitating genuine choice about whether to expose oneself to certain forms of surveillance or whether to opt out.[7] If such measures can be implemented, it seems less likely that attitudes to surveillance will become so permissive as to tolerate its authoritarian use. Proposals for specific examples of such checks and balances are discussed in Section 3. For now, it is sufficient to conclude that there may be ways of reinforcing public opposition to the use of surveillance for authoritarian purposes such that this important barrier is not inevitably eroded.

2.2 Surveillance encourages governments to see and treat people as mere conscripts to their purposes, denying their autonomy

One of the defining features of an authoritarian government is its subordination of individual freedom to the goals of the state. The government is the only body with the authority to set those goals, an authority which might be derived from privileged understanding of religious texts or ideological principles, for example, but not from the will of the people freely expressed. An authoritarian government might consider it consistent with state purposes to permit individuals a relatively broad margin of individual freedom. However, the government always retains the discretion to reduce this sphere of freedom when and as it sees fit, irrespective of the preferences of those individuals. Thus authoritarian government fails to respect the autonomy of individuals: their ability and authority to decide for and govern themselves.

It is sometimes argued that, if permitted, certain forms of compulsory state monitoring such as ID card registration schemes will lead states to treat people in ways that are incompatible with respect for their autonomy. The desire for efficiency in the pursuit of security and a range of other legitimate goals of liberal democracy, argues Clarke, invites the use of surveillance tools and techniques 'that have proven effective in managing raw materials, manufactured goods and

[7] For an example of efforts to implement such measures by the EU see 'Take Control of your Personal Data' http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf

animals [and] can be applied to humans too' (Clarke, p.25)[8]. While there is nothing wrong morally speaking with state management of flows of objects and animals for reasons of efficiency, human beings should be free to determine their own goals in life and act in ways that pursue their own individual purposes. Substituting humans for animals and objects allows those using surveillance techniques to view all three as morally equivalent and to feel justified in manipulating or controlling them for whatever purposes the state adopts. Denying individuals the opportunity to choose the greater control over their information that comes with a refusal to participate in an ID card scheme over contribution to the goals set by the state treats them as means to the achievement of those goals, rather than autonomous agents whose authority to decide for themselves should be respected.

Something along these lines is argued in objection to plans to introduce compulsory ID cards: "There is no quicker way to dehumanize an individual" argue Michael and Michael (2007:17) "than by 'removing' someone's name and replacing it with a number. It is far easier to extinguish an individual on every level if you are 'rubbing' out a number rather than a life history". On a similar note, AC Grayling argues that the introduction of compulsory ID cards in the UK would change 'the relationship between individuals and the state, from private citizens, to numbered conscripts' (2009:101). "An ID card or device …" continues Grayling, 'is a surveillance instrument, a tracking device, like a car number plate or the kind of tag punched into a cow's ear. Any animal (including, soon, the residents of Britain) thus tagged and numbered is a trackable, controllable unit, exposed 24/7 to monitoring' (Grayling, 2007). Furthermore, he argues, once such ID cards exist, it is a minor technological step from forcing people to carry them to forcibly inserting them into people's bodies on a chip, something Grayling claims is tantamount to branding a number on their arm (Grayling, 2009:101).

Both of these arguments imply that the introduction of ID cards would remove a necessary barrier to authoritarian government. But this can be refuted empirically. A cursory examination of many states which do currently operate compulsory ID card schemes, including Germany and France, reveals that they bear no meaningful resemblance to the kinds of totalitarian regimes invoked by Grayling and Michaels and Michaels. But there would be serious reasons to reject their line of argument even if real counter-examples were not so easy to find. Much of the argument's force often seems to rely on the aesthetics of ID cards, invoking images of mass movements of faceless people being herded through bureaucratic processes, checked against registers, and ruthlessly excluded in the case of nonconformity. But this aesthetic only depicts reality if the ID cards are actually being used to impose authoritarian goals. In which case there are independent reasons to object to their use.

More importantly, however, these critics mistakenly identify the roots or causes of authoritarianism as lying in the technologies themselves, such that their

[8] See also Grayling who claims ID cards are 'barcodes for citizens' that will transform people into 'controllable, trackable units' (2009:101)

introduction has the effect of transforming a hitherto benign liberal democracy into a totalitarian nightmare. In doing so, they deny the possibility that ID cards can be used for a range of purposes, some of which might be compatible with liberal democratic aims and some of which might not. They also deny the fact that there is any difference, morally speaking, between a system of ID cards that has been authorized by a democratically elected parliament subject to constraints of transparency and accountability and one that has been introduced by decree of a dictatorial regime.

If the introduction of an ID card scheme *were* made by dictatorial decree, then making compliance with it compulsory would indeed impose interferences with privacy on individuals for the sake of goals they did not agree to contribute to. This would indeed interfere with the autonomy of individuals in ways incompatible with genuine liberalism. But citizens compelled to carry ID cards as a result of a legitimate democratic process are in a fundamentally different position, morally speaking, to 'conscripts' to a programme of social engineering they had no role in initiating and no power to control. They could not be described as being used as mere means to the state's bureaucratic ends, because they would have had a crucial, if indirect, part in both setting those ends and approving the means. There may still be good reasons for those citizens to object to the introduction of ID cards. For such schemes might be disproportionate, ineffective, too prone to error or mission creep, or subject to security breach, for example. But, other things being equal, they could not argue that their autonomy was thereby being violated. Neither could they claim that they were thereby reduced in the eyes of the state to *nothing but* a number and thus dehumanized, unless at the same time the state stripped them of their names and their human rights.

This should not be taken to suggest that the fact that a surveillance technology is approved by a democratic authority for a legitimate purpose is by itself sufficient to ensure that it is compatible with respect for the autonomy and dignity of individuals. Liberal democracies make decisions via imperfect systems which are often manipulated by factions or groups with vested interests or by the need to achieve consensus, amongst other things. Democratically elected political parties often force through policies for self-serving reasons rather than the public interest. Secrecy, lack of accountability, and mission creep all regularly affect the legitimacy of government policies, including those relating to surveillance.[9] However, there is an important qualitative difference between surveillance policies made against this admittedly imperfect background and those made by the dictatorships of the East German Democratic Republic or Ceaucescu's Romania. It would be both mistaken and complacent to presume that the injustices of the latter could never be perpetuated in the former, but it is equally erroneous to conflate the two merely because they both employ specific surveillance techniques.

[9] See Bowden, 2002, for a relevant critique of the policy-making process leading up to the implementation of data-retention legislation in the UK.

In some states that are in transition or have recently undergone a change from authoritarian to democratic rule, normal checks and balances of liberal democracy are not yet reliable enough to regulate effectively the use of increased surveillance powers by the state. For example, recent political developments in Hungary give greatly increased surveillance powers to the new counter-terrorism police, the TEK.[10] At the same time, 2011 media regulation included the introduction of laws imposing fines for "imbalanced" or "insulting" media coverage of the prime minister, weakened protections for journalistic sources, and a regulatory Media Council to enforce the law with a minimum of checks to its power.[11] In contexts such as these, where surveillance powers are introduced through processes of limited democratic legitimacy and against a background of weak checks and balances it is highly likely that they will be used for illiberal ends. This situation poses a challenge to the consistency of the European Union's aim to impose a single data retention regime on all member states with respect for human rights. At the same time as the EU exerts a democratizing force on countries such as Hungary, holding the government to account for illiberal practices, it provides the same government with new powers with which to perpetrate such practices. If the former task is insufficiently successful, this undermines the legitimacy of the latter.

2.3 Surveillance power is inevitably abused for illiberal ends

Thus far it has been argued that the institution of a range of liberal democratic checks and balances can serve to prevent the slide from surveillance to authoritarian government. This is contested, however, by those who claim that even if a programme of surveillance is devised and authorized by liberal democratic institutions and even if it appears in principle to be a proportionate means to a legitimate end, and even if it is reined in by apparent checks and balances, in practice these will inevitably be overridden and it will inevitably be used for authoritarian purposes. This account of the slippery slope can be summarized thus: giving states the power to surveille as a means of preventing serious crime might be justified in principle; however, in practice every power is eventually abused (Kateb, 282); it is inevitable that the power acquired through surveillance will be abused; in order to prevent such abuse, we should prevent governments acquiring such knowledge in the first place. The point being made here is not merely that power to surveille will be used inevitably for purposes other than those for which it is originally authorized. It is, in addition, that such information will be inevitably used for *illiberal purposes*, such as the stifling of dissent.

However, merely pointing to the inevitability of some abuses falls far short of providing a complete argument in favour of prohibiting surveillance. This is because there are good reasons to tolerate the prospect of *some* abuse of power

---

[10] Kim Lane Scheppele, 'The New Hungarian Secret Police' April 18 2012, http://krugman.blogs.nytimes.com/2012/04/19/the-new-hungarian-secret-police/ Last Accessed April 2013.

[11] http://www.edri.org/edrigram/number9.1/media-law-hungary-blocks-internet. Last Accessed April 2013.

for illiberal ends, even in a liberal democracy. These reasons relate to the greater harms that can be prevented by granting such power to the state. The decision whether to grant the state new powers must be made on the basis of an all-things-considered assessment. This means taking into account and comparing the likely impact on the rights and interests of individuals of surveilling, not surveilling, and surveilling under varying conditions and constraints. Sometimes some illiberal abuse might be preferable to the alternative. To see how, we might consider the decision to criminalise murder. The inevitability of wrongful convictions is not by itself a sufficient reason to refrain from criminalising murder. Quite apart from the deterrence and other rights-protecting effects of criminalizing murder, *not* criminalizing murder is highly likely to result in many more and graver miscarriages of justice, not to mention more murders. This is because the vigilante groups that would inevitably seek to fill the justice gap would be less able to determine innocence or guilt in an impartial and evidence-based way than modern courts. They are also likely to be less restrained in their choice of punishment. Therefore it seems that the pertinent question is not whether surveillance powers will ever be used for illiberal purposes but how these foreseeable costs could be reduced, and whether they are worth the benefits.

One obvious alternative to prohibiting surveillance is to limit the opportunities for abuse by instituting a range of checks and balances designed to ensure integrity of purpose and effective transparence and accountability. The aim of such a move would be to restrain power effectively enough to ensure than its inevitable use for illiberal purposes does not become so systematic and severe that it outweighs the benefits produced by the prevention of serious crime.

It is important to recognise that the likelihood of data retention powers being used for illiberal purposes and the likelihood of such use becoming routine varies between states as well as between historical moments within them. In some states with recent histories of authoritarianism, the risk may be higher, because political change is not always accompanied by institutional reform. If the institutions responsible for illiberal forms of surveillance remain unreformed, the risk that powers may continue to be used in illiberal ways may be high. This concern appears to motivate heightened public opposition to state use of data retention for security aims in, for example, Greece. From 1950 until 1974 in Greece, a right-wing authoritarian police state maintained detailed files for each citizen recording their and their family's political activities and loyalty to the regime. These were used as a basis for restricting people's rights and access to public benefits. Despite the fall of the fascist dictatorship in 1974 and the transition to democracy, these files were not destroyed until over a decade later, in 1989. Neither did the widespread use of wiretapping for the purpose of surveilling political dissidents (Samatas, 2005:184). One reason for the continuation of illiberal uses of surveillance is that 'security and military structures remained intact' (Ibid.). The political history of a state may in this way affect the extent to which this version of the slippery slope argument applies.

2.4 Surveillance powers will eventually fall into, and strengthen greatly, the hands of authoritarian regimes

A further criticism of surveillance concedes that surveillance technologies can be used in ways compatible with liberal democracy and that any tendencies towards authoritarian purposes can be managed sufficiently through proper regulation and oversight. However, it maintains that surveillance techniques are nevertheless dangerous and problematic morally, because they could be turned into a powerful tool of oppression with great ease if acquired by an authoritarian regime (Jacobs, 2009: 28; Lyon 2010:38). An example of such abuse can be found in 1930s Germany, when the Nazi regime used citizen administrations established long before its rise to power to identify, persecute and ultimately murder millions of Jews (Jacobs, Ibid.). Some argue that, in the absence of any guarantee that such a regime will not one day seize power and control of the surveillance techniques developed in the days of benign liberalism, we should take precautionary measures and keep such techniques out of the hands of government.

The extent to which this argument supports preventive or precautionary action to limit the use of the technology depends on the results of a sober assessment of the risk of such a regime coming to power. Precautionary prohibition of surveillance is not cost-free. On the contrary, evidence suggests that some forms of surveillance are of vital importance to the prevention and prosecution of crime, including serious crime and terrorism.[12] Any trade-off between current security against crime and future protection against rights-violations by an authoritarian state must be proportionate. When there is a lack of evidence suggesting that such regimes may rise to power, arguments that appeal to such possibilities as reasons for denying states the power to build such databases or use CCTV seem unnecessarily precautionary.

Just as precautionary arguments against entirely speculative horrors do not justify state interference with individual liberty, neither do they justify denying the state the means to protect individuals from actual, though perhaps less horrific, threats to their security. Liberal theory requires that when we make decisions, we err on the side of liberty. This means that justification must be provided for any state intervention that interferes with the rights of citizens. What is more, the justification must be a liberal justification, which means it must relate to the harms or rights-violations that are prevented by such interference. However, once a sufficient justification *has* been provided, any move to block such interference on precautionary grounds must be supported by further, equally sound and well-supported justification. This contradicts the claim that 'in the absence of any guarantee' (2009:102) that technology will not be seized by a totalitarian regime, we should deny states some important means

[12] UK police described the availability of traffic data as 'absolutely crucial … to investigating the threat of terrorism and serious crime'. Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 18 April 2011, p.23. See also conclusions of the Justice and Home Affairs Council, which state that communications data is a "valuable tool" in the prevention, investigation and prosecution of criminal offences, in particular organised crime. 2477th Council meeting, PRES/02/404, 19 December 2002.

to prevent serious crime. The requirement for such a guarantee is not a requirement of liberal theory. On the contrary, it is an irrational requirement. For it implies that the evidence that our current government, and indeed likely future governments, can be trusted to use surveillance in ways that protect the rights of individuals is *less* relevant to decisions about the regulation of surveillance than the distant possibility of authoritarian rule. It is also an unfair requirement, because it sacrifices the rights of individuals affected by serious crime today in the name of a future threat for which there exists little or no evidence.

None of this should be taken to suggest that ID cards are in fact justified, or risk-free, or indeed the solution to serious crime. Nor should it be taken to suggest that fears of the rise of authoritarian regimes are always irrational. In many real cases they will plainly not be. Probable abuse by an authoritarian regime may well be a good enough reason to block the introduction of an ID card scheme. But before it is, explanation of the nature of the probability must be provided.

It is also important to stress that what has been argued here in relation to ID cards should not be taken to suggest that surveillance technologies are entirely neutral tools whose adoption never exerts any influence on the relations between individuals and states. Research on the use of drones in war zones suggests that, amongst other things, the distance they provide may encourage soldiers to dehumanize their targets and may thereby make it easier to kill (Ignatieff: 2001)[13]. A substantial body of research exists showing how the design of surveillance technologies can make them more or less amenable to security breach, corrupt use, error or mission creep even when used by benign liberal democracies (Jacobs, 2009; Clarke, 1994). Fortunately, the same checks and balances that protect against these kinds of misuse also protect against use for the kind of rights-violating authoritarian purposes identified above. Preventive measures that might be adopted include automatic deletion of records after a certain time, giving individuals control over the content of records, decentralizing storage of data, encryption, privacy-by-design techniques and the use of electronic trails recording who accessed and did what with data when.

2.5 Surveillance powers will be used in authoritarian ways against minority groups

While the prospect of a new totalitarian dictatorship in Europe seems a poor basis for surveillance regulation and policy making, the prospect of other, more subtle forms of authoritarian rule may provide a more reasonable ground for restricting state power to surveille. Governments do not always use their powers in the same ways in respect of all groups within their jurisdiction. For some critics, the primary concern with the use of surveillance technologies is that they may be used by states in authoritarian ways against certain groups, but in legitimate ways in respect of others (Kateb, 2001:295; Samatas, 2010:158). As a result, life for minority groups might come to resemble life under an

[13] For a first-hand account of how drones might make killing easier, see http://www.bbc.co.uk/news/world-us-canada-19820760. Last Accessed April 2013.

authoritarian regime in significant ways. Such a situation, it is claimed, is far from imaginary. On the contrary, it already exists to varying extents in many liberal democratic states.

This argument is often put forward in relation to the use of surveillance techniques to monitor criminals, prisoners, and illegal migrants interned in detention centres awaiting deportation. Life for people in these circumstances does resemble life under an authoritarian regime, because they are denied a very broad range of rights and freedoms and are instead compelled to live within the boundaries set by the authorities. They are also typically subjected to intense surveillance, including observation by guards, CCTV cameras, and a reduction in the range of private spaces and opportunities for private activities such as, for example, intimate conversations and encounters.

The questions of whether prison is a justified response to crime and whether illegal migrants should be treated in ways similar to criminals are challenging for liberal theory. The latter question is particularly challenging because, unlike prisoners, illegal migrants are excluded from the democratic process and therefore have no say in the laws and policies that they are nevertheless compelled to obey. However, the scope of the current paper is limited to an examination of how the use of surveillance techniques might lead to authoritarian government. It seems clear that it would not be correct to describe surveillance techniques as leading to (or removing legal or social barriers to) the use of prisons for criminals or detention regimes for illegal migrants. But it is possible that surveillance techniques are used for illiberal purposes within those institutions, for example, to detect and silence criticism of corrupt behavior by guards. For this reason it is important to establish checks and balances that ensure proportionality, transparency and accountability of surveilling authorities within such institutions.[14]

3. Surveillance techniques create 'asymmetries of power' between individual and state that invite authoritarianism

We can now turn to two arguments about the causal link between surveillance and authoritarianism that do not posit the existence of a slippery slope. Both of

[14] It might be argued that this two-tier society might emerge in more subtle ways if, for example, a party with strong views about the claims to equal rights of certain minority groups came to govern a state through democratic means. While it would not be correct to describe surveillance techniques as the source of the unequal treatment, they might enable unequal treatment and be used to justify and perpetuate it. If prejudice against such groups is widespread and pervades the institutions of government and society, then existing liberal democratic checks and balances may not function as effectively to protect some groups against illegitimate use of surveillance as they do to protect others. The likely failure of checks and balances to prevent and expose the misuse and abuse of surveillance powers in such cases provide good reason to take some precautionary measures in advance. One approach might be to adopt extra measures, specifically geared to the prevention of discriminatory use of surveillance powers. One such measure might be the institution of a body with authority to review all policy for its impact on minority groups, similar to the UK's Equalities and Human Rights Commission. Others might be ensuring the presence of minority group representatives on legislation committees and consultation with such groups prior to the adoption of surveillance techniques by local authorities, by example.

these begin by claiming that one of the defining characteristics of authoritarian states is an extreme 'asymmetry of power' between individual and state (Fuchs, 2012; Lyon, 2010; Dubbeld, 2003). They argue that the proliferation of surveillance techniques introduces and exacerbates such asymmetries, disempowering individuals at the same time as they strengthen the hand of the state, and opening the door to authoritarianism. Surveillance, it is argued, is distinctive as a tool of governance in at least the following way: it increases the power of the state versus the individual (Jacobs, 2009:21; Solove 2004:21; Richards, 2013:28; Lyon, 2007:15). There are two kinds of state power surveillance can be said to increase. The first is the power to enforce the law: surveillance increases knowledge of past and potential transgressions of the law. It therefore enables states to enforce it more effectively, catching more criminals both in and after the act. The second is the power to intrude into the private lives of individuals and to interfere with data about them. The latter kind of power reinforces the former: the greater the power to intrude into privacy and to collect and process data, the greater the power to enforce the law.

3.1 Surveillance aims at perfect enforcement of the law, which is itself an authoritarian aim

In liberal theory, an increase in the first kind of power, namely the power to enforce the law, is not problematic as long as the laws it is used to enforce are themselves justified on liberal democratic grounds. This is legitimate power wielded on behalf and in the name of the people. The fact that it is matched by a corresponding decrease in the freedom of individuals to break the law or to do so with impunity is not a problem. This is because individuals are not 'free'- i.e. permitted morally or legally- to do evil in the first place (Bentham, 1995). Or, put otherwise, the freedom to break justified laws is not a freedom that should be valued and can be protected consistently with liberal principles.

It might be argued, however, that a state in which the law was enforced perfectly, in which every attempt to break it was detected and prevented or punished, would resemble a dystopia rather than a society that could accurately be described as free. A society in which the option of breaking the law is not even a possibility is one in which the choice of whether to act in accordance with the law is removed from individuals. Surveillance, it might be argued, drives us towards such a dystopia, because its ultimate aim is precisely to achieve perfect enforcement of the law by revealing each and every attempt at transgression.

This the criticism has been raised in reference to the Philip K Dick book Minority Report, which depicts a society in which all crime is detected by means of human telepathic monitors ('pre-cogs') and ultimately prevented. What distinguishes the 'pre-cogs' from any current crime prevention technology is their ability to tune in to a telepathic frequency that receives only those transmissions corresponding to actual attempts at criminal acts. Thus none of the usual lineup of risks (disproportionate use, mission creep, discrimination, corrupt use, error and collateral intrusion) that accompany current surveillance techniques in crime-prevention arise.

Technological innovation has not yet produced anything as perfectly targeted and effective as the telepathic monitors or 'pre-cogs' of Minority Report in the context of crime-prevention. But it has produced techniques that make certain forms of rule-breaking and evasion impossible. For example, alcohol and drug testing for pilots prior to each flight is now common practice, and metal detectors and x-ray machines at airports ensure that guns can no longer be taken onto flights. Most objections to these kinds of preventive measures relate to the fact that they impose intrusions on large numbers of the vast majority of whom are expected to be innocent and for whom no evidence of rule-breaking exists (Haggerty and Ericson 1997: 42; Monahan, 2010: 99). The fact that such measures leave no opportunity for evasion does not by itself often raise concern. But perhaps one residual cost of perfect enforcement, in the world of the pre-cogs as well as the real examples just cited, is the loss of trust it implies. For where no opportunity to break the rule exists, there is no role for trust between society at large and those to whom the rules apply. The question of whether a pilot can be trusted to refrain from drinking before flying becomes irrelevant when the means to test for sure are available. Ultimately, the loss of trust that results from perfect enforcement must be weighed against the benefits to security. Thus far experience suggests that the public will assign greater value to the latter. This is compatible with liberal democratic principles.

3.2 Surveillance increases the power of states without corresponding increases in the power of citizens to hold them to account

The notion of asymmetries of power arises in a second criticism of surveillance, but this time in relation to the second kind of power defined above: the power to intrude into individual privacy. The argument states that surveillance techniques are problematic when they increase the power of the state without corresponding increases in the power of individuals to control states (Kohn, 2011, Monahan, 2010). Proponents of this view point out that, when the state compels people to reveal or make available information about themselves to its agents, it is extending the reach of its power, encroaching into the sphere of control or freedom from interference previously enjoyed by individuals. It is this increased power to intrude and gather knowledge that poses a threat to liberal democracy, because it can potentially be directed to purposes other than the enforcement of the law. Unless this increased power is matched by a corresponding increase in the power of citizens to hold governments to account, states will be able and tempted to use it in illegitimate ways and for authoritarian purposes. As Balkin argues, "Without appropriate checks and oversight mechanisms, executive officials will too easily slide into the bad tendencies that characterize authoritarian information states. They will increase secrecy, avoid accountability, cover up mistakes, and confuse their interest with the public interest (Balkin, 2008:21).

The question of what checks and oversight mechanisms are appropriate to the prevention of authoritarian uses of surveillance occupies a significant body of academic and especially legal criticism of state uses of surveillance. Much of this work is devoted to identifying and addressing weaknesses and shortcomings with existing checks and balances, and putting forward innovative proposals for

how these might be improved, extended, and developed to bring surveillance practices back in line with liberal democratic values where these have diverged. This rich and growing body of work can be usefully mined to provide both policy makers and civil society with a range of excellent suggestions for the regulation and oversight of surveillance. It is not possible here to review all such proposals, some of which have already been described in the discussion above. Instead, the remainder of this section will focus on the proposal that the asymmetry of power between states and individuals caused by surveillance is, at least in part, an asymmetry of knowledge, and that this can be corrected by applying the very surveillance techniques governments use on individuals to the scrutiny of state practice.

Kohn (2011) argues that surveillance techniques should not be monopolised by states. Rather, these techniques should be put in the hands of the public and turned on states in an act of 'sousveillance' (literally, surveillance from below).[15] 'Sousveillance' argues Kohn, 'helps ensure some degree of reciprocity so that citizens can monitor the government and powerful groups and use the media or judicial system to hold them accountable for abuses.' (584). Kohn points out that state agents have the legal authority to record individuals without their knowledge in order to reveal and prosecute criminal behaviour. She argues that citizens should also be given this legal right, in order to enable them to expose corruption and other illegitimate uses of state power. Thus sousveillance techniques serve to increase publicity and transparency and to challenge secrecy in government practices.

In a similar vein to Kohn, Monahan (2010) points out that surveillance techniques such as data mining can be applied to the activities of states to ensure greater transparency. Governments themselves can assist these initiatives by releasing raw government data, publishing it online, and allowing citizens to mine and analyse it as they see fit. The UK government's Open Data initiative is one example of such a move. Monahan cites a number of initiatives in the USA that enabled citizens to monitor, for example, the release of toxins into the waters (Monahan, 2010:103), or generating online maps for those wishing to evade capture by CCTV in New York City. Kings University College in London operates a pollution app, showing levels of pollution in individual streets in London and comparing them to the European standards the UK government has pledged to respect. Monahan argues that transparency must be accompanied by meaningful accountability mechanisms. One might imagine, for example, a function on the pollution monitoring site that automatically emails interested civil society groups such as local Greenpeace and Friends of the Earth chapters as well as local MPs and members of environmental select committees whenever pollution exceeds the limit set. Initiatives such as these enable citizens to hold governments to account, analysing whether they have fulfilled their own commitments and met their own targets.

A further way in which individuals might be empowered in the face of greater surveillance is through regulation that provides them with access to information

about government use of their data. The more open government agencies can be about their use of citizen data, the more able citizens are to contest and indeed to approve those uses. As was noted in Section 2.1 above, the ability of citizens to consent meaningfully to the use of surveillance techniques is hindered by the lack of transparency about their use. Moreover, clarity about the uses and extent of surveillance may reduce the risk of chill identified in Section 2.1, as individuals are more aware of when and for what purposes they might be being monitored by the state. Measures that permit individuals to gain access to, correct or delete information about themselves is a further way in which citizens can be empowered in the face of state bureaucracy. The EU is pioneering regulation to enable this online.[16] In the UK, for example, an online social media site, Patients Know Best, aims to empower patients by giving them the key to their medical records so they can share them with whoever they choose.[17] Transparency and accountability can also be built into technologies. For example, electronic trails noting who accessed and modified, added to or deleted data, when, and why can be built into large-scale databases. This can help to reinforce transparency and accountability even across state boundaries.

All of these measures are compatible with more institutional forms of oversight, including judicial review, parliamentary scrutiny, the use of ombudsmen and data protection authorities, as well as those of civil society including a free press and well-funded civil liberties organisations. But they disperse the power both to scrutinise and hold states to account. This can help to empower even those more disaffected, marginalised and excluded in society who may not always be represented effectively by these more traditional mechanisms.

Conclusion

Three conclusions can be drawn from the discussion in this paper. The first is that the slide towards authoritarianism is not inevitable but can be addressed by means of liberal democratic checks and balances. The second is that political context is a strong determinant of whether the proliferation of surveillance techniques is likely to result in their authoritarian application: the more varied, well-established, and sturdy the checks and balances are in a society, the less likely power is to be used in authoritarian ways. The third is that checks and balances need to do more than provide institutional oversight of powers: they must also empower citizens directly to impose publicity on governments and hold them to account.

[16] 'Take Control of your Personal Data' http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf

[17] http://news.bbc.co.uk/1/hi/programmes/click_online/9464494.stm. Accessed 28/04/13

List of References

Bentham, Jeremy. 'Panopticon', in *The Panopticon Writings*. Verso, 1995.

Bowden, 'Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terorism Legislation'. *Computer and Telecommunications Law Review,* March 2002.

Clarke, Roger. 'Information Technology: Weapon of Authoritarianism or Tool of Democracy?' IFIP World Congress, Hamburg, September 1994 http://www.rogerclarke.com/DV/PaperAuthism.html

Balkin, Jack. 'The Constitution and the National Surveillance State'. *Minnessota Law Review*, 93(1) 2008

Dubbeld, Lynsey. 'Observing bodies : camera surveillance and the significance of the body'. *Ethics and Information Technology*, 5 (3). 2003

Grayling, A.C. 'Are ID cards either philosophically or pragmatically justifiable?' *Prospect Magazine*. October 27, 2007.

Haggerty and Ericson, *Policing the Risk Society*. Toronto: University of Toronto Press. 1997.

Ignatieff, *Virtual War*. 2001.

Jacobs, Bart. 'Keeping our Surveillance Society Nontotalitarian' Vol 1, No 4. 2009.

Joinson Adam and Paine, Corina. 'Self-disclosure, privacy and the internet' in Oxford *Handbook of Internet Psychology*, Joinson et al. Oxford. 2007.

Kateb, George. 'On Being Watched and Known' *Social Research*. Spring 2001 (68)1

Kohn, Margaret. 'Unblinking: Citizens and Subjects in the Age of Video Surveillance, *Constellations* 17(4) 2010

Lyon, David *Surveillance Studies, an Overview.* 2007

Lyon, David. 'Identification, Surveillance and Democracy' in *Surveillance and Democracy*, Eds. Haggerty and Samatas. 2010

Monahan, Torin. 'Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance', in *Surveillance and Democracy*, Eds. Haggerty and Samatas. 2010

Open Society Institute. *How the EU is watching you: the rise of Europe's Surveillance State* (2009)

Raab, Charles. 'Impacts of surveillance on civil liberties and fundamental rights' in *Surveillance, Fighting Crime, and Violence.* Deliverable D1.1. IRISS Project: Increasing Resilience in Surveillance Societies. 2012.

Richards, Neil. 'The Dangers of Surveillance'. Harvard Law Review Symposium. 2012. http://www.harvardlawreview.org/symposium/papers2012/richards.pdf

Samatas, Minas. 'Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture' *Surveillance & Society* 3(2/3).

Solove, Daniel. *The Digital Person: Technology and Privacy in the Information Age*. 2003

UK House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-I, para. 3.
UK ICO, 2010

van der Burg, Wibren. 'The Slippery Slope Argument' in *Ethics* Vol. 102, No. 1. Oct., 1991.