Debate

Surveillance and the Rule of Law

Lisa M. Austin

Faculty of Law, University of Toronto, Canada.

lisa.austin@utoronto.ca

Introduction

Although the discussion of global surveillance post-Snowden has generally taken place within the framework of “privacy” rights, in this short paper I would like to propose instead a focus on the rule of law. In addition to widely discussed privacy issues raised by contemporary surveillance, there are additional, more serious failures regarding the rule of law. States often claim that their surveillance activities are “lawful” because undertaken pursuant to some statutory authority. The rule of law refers to something more ambitious: a set of ideas concerned with the capacity of law to guide individual action and act as a constraint on state power. Surveillance activities can be “lawful” in a narrow sense but still violate the rule of law in this more robust sense, a condition I describe elsewhere as one of “lawful illegality” (Austin 2015a). In this paper I outline one of the reasons why current state surveillance practices in relation to national security are best characterized in these terms. The surveillance debate, I conclude, has to focus more on the deep reasons for this tension with the rule of law and less on the nature of the impact of such practices on individual privacy rights.

Privacy and the rule of law are not completely unrelated. Constitutional doctrines regarding unreasonable search and seizure—understood to protect privacy rights—have deep roots in rule of law ideas concerning the need to constrain the arbitrary discretion of state authorities (Austin 2013). Indeed, much of the recent UN report on privacy in the digital age details classic rule of law concerns, including ideas of publicity and non-arbitrariness (United Nations 2014). Connecting with these issues as rule of law issues generally, rather than as aspects of a narrow right to privacy, links the debate regarding state surveillance to other debates about the nature of law and not merely the nature of privacy, the characteristics of state power and not only the harm suffered by individuals.

Post-9/11 discussions of national security and the rule of law were dominated by concerns about “emergencies” and “exceptional practices” (Vermeule 2009). This discussion suggests that the basic rule of law question regarding state surveillance is whether it can be regulated through law or is inherently exceptional. This, I argue, points us to the key questions, which is to understand the kind of threat that terrorism actually poses to national security, whether there is a principled difference between citizen and foreigner, and the difference between law enforcement and state security. Our answer to these questions will determine the extent to which state surveillance is a necessary and proportionate limit on privacy rights.

Austin, L.M. 2015. Surveillance and the Rule of Law. *Surveillance & Society* 13(2): 295-9.

<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author, 2015 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.

The Exceptional Nature of National Security

The debate about national security and the rule of law that emerged in the aftermath of 9/11 focuses on the question of whether “emergencies” demand a space for unfettered executive discretion in order to respond to situations that are, by definition, difficult to anticipate in advance. Such discretion might take the form of a “black hole”, where the legislature essentially carves out a space for unfettered discretion, or a “grey hole” where “there is the façade or form of the rule of law rather than any substantive protections” (Dyzenhaus 2006: 3). The rule of law debate concerns whether these “holes”, black or grey, are necessary (Dyzenhaus 2006; Vermuele 2009; Criddle 2010).

Although US Supreme Court Justice Scalia has indicated that the question at the heart of the constitutionality of state surveillance practices is that of “balancing the emergency against the intrusion” (Hurley 2014), it is not clear that the “emergency” framework is appropriate. If the Snowden revelations have shown us anything, it is not a nimble response to an unanticipated emergency. It is instead a rational, systemic, planned response to the perceived threat of terrorist attacks, applying analytic techniques precisely in order to anticipate those situations and respond to them. If surveillance falls into a legal black or grey hole, the invocation of “emergency” offers little justification for it, or illumination of its nature.

State surveillance is exceptional in another way. Consider what it might mean to have state information practices conform to our basic understandings of the rule of law. I have written elsewhere that Fair Information Practices (FIPs), which underpin our data protection law statutes, are better understood in rule of law terms than in terms of privacy (Austin 2014). FIPs ensure that personal information collection, use and disclosure is done under conditions that enable individuals to understand how their information is being collected, used or disclosed (the guidance function of law) and ensures that this collection, use or disclosure remains within the bounds of legal authority (the constraint function of law).

In national security, rather than the operation of the rule of law dimensions of FIPs, we see the operation of *exceptions* to FIPs and, more recently, proposals to further expand those exceptions (Austin 2015b). State surveillance practices that involve the collection, use or disclosure of personal information are inherently in tension with our basic understandings of what it means to bring these information practices within a framework of law.

Does this look different if we think about surveillance within the constitutional framework for unreasonable search and seizure? The constitutional framework is one that originally is very much about dealing with the exceptional nature of some forms of state power. One way to understand it is that the state cannot do something contrary to the ordinary law (e.g. trespass or wiretap) unless it has special authorization. This is a rule of law idea—that state agents are subject to the ordinary laws of the land unless they have special authorization (e.g. a warrant). The traditional standard for such a warrant is reasonable and probable grounds to believe that an offence has occurred and that the search will yield evidence of that offence.

Rather than an exception to the rule of law, this standard for search and seizure can be understood in rule of law terms. The idea is that the state needs to be able to obtain exemptions from the ordinary operation of the law to uphold the law more generally; otherwise, individuals could hide behind the law to avoid prosecution for their illegal behaviour. However, this rationale only applies if the exception is narrowly tailored—it is permitted only to the extent that is necessary and proportional to its purpose of upholding the law more generally. Otherwise the exception swallows the rule, for in the name of pursuing law enforcement in general state officials would be able to operate outside of the ordinary operation of the law. Citizens might be kept within the terms of the law, but state officials would not.

Of course, one could formally empower police to do many things that ordinary citizens are not permitted to do through different forms of statutory authorization. Police actions pursuant to this authority would be “lawful” in one sense of the word. However, if those powers are not limited to what is considered necessary and proportional in relation to the rule of law, then this patina of lawfulness fails to address the deeper problem. In such a situation public authorities exercise power against citizens according to a different set of rules than those that apply to citizens and this different set of rules does not derive their legitimacy from the basic logic of the rule of law. That is the sense in which the exception swallows the rule—departures from what is necessary and proportional in relation to maintaining the rule of law undermine the rule of law. We are left with “lawful illegality” (Austin 2015a).

State surveillance in the national security context might very well be “exceptional” in this sense of “lawful illegality”, for several reasons. First, it involves activities that private individuals are not permitted to engage in and so allows state agents to operate according to a different set of rules. To take only one example, consider the private-public “partnerships” revealed by Snowden. There are many ways in which laws permit, and even require, cooperation between private sector internet intermediaries and the state while at the same time there are many privacy laws that restrict the extent to which such intermediaries can share information with other non-state parties. In other words, special rules apply to the state.

Second, one of the main goals of such state surveillance is to obtain foreign intelligence. This is not a goal directly related to maintaining the rule of law. Instead, it has more to do with collecting information in furtherance of general state interests such as those involving foreign policy goals. Historically this involved collecting information beyond domestic borders and operated in its own “black hole”, legally speaking, often involving actions abroad in breach of the domestic laws of other nations and would be illegal in the nations sponsoring them (Forcese 2011). Given the realities of global communications, this distinction between foreign and domestic activities comes under strain: foreign communications can be collected domestically and domestic communications can be swept up “incidentally”. This brings the “black hole” of foreign intelligence surveillance within the domestic legal sphere.

Third, one of the contemporary goals of state surveillance is to prevent terrorism on domestic soil. Prevention will always involve a lower threshold than those that operate when seeking to identify someone who has already committed an offence. As Cole argues, “[i]f preventive sanctions could be imposed only when we know beyond a reasonable doubt that an individual will commit an illegal act in the future, such sanction would almost never be imposed” (Cole 2014: 4). Similarly, “no objective measure exists by which one can reliably know how much is too little, too much, or just enough prevention” (Cole 2014: 5). We can add to this the idea that terrorism is not understood as mere criminality but is considered a threat to the existence of the state itself, adding an additional dimension to the prevention mandate. If the political context is one where the goal is to prevent *all* terrorist attacks, then the level of surveillance that is necessary and proportionate to this goal is high indeed. If we note the difficulties associated with defining terrorism and further note that often the goal is to prevent terrorist activities broadly construed rather than specific terrorist offences, then the scope of the exception broadens even further.

State surveillance therefore involves exceptional state activities that combine both the legal “black hole” associated with collecting foreign intelligence and the constraint-erasing logic of preventing terrorism. The result is indeed something exceptional.

Conclusions: Boundary Issues

The previous analysis of the exceptional nature of state surveillance in the national security context suggests two ways to bring it back within the rule of law and avoid a situation of “lawful illegality”.

Neither is likely to be implemented, but understanding why can help to crystalize the deep underlying question regarding the relationship between surveillance and law.

The first would be to insist that foreign intelligence information only be collected in relation to foreign states and their agents and not foreign citizens more generally. This would place that information collection within a state-state relationship rather than a state-individual relationship. The dubious legality of foreign intelligence collection still raises important issues as between states but these are different issues than those raised by the classic rule of law focus on the exercise of state power in relation to individuals.

The second would be to focus on the collection of information regarding terrorist offences in the same way that the state focuses on the collection of information regarding other criminal offences. The standard way of understanding necessity and proportionality in this latter context is to say that the state can infringe privacy only when it has reasonable and probable grounds to believe an offence has or will be committed and the search will yield evidence of that offence.

Why are these suggestions unlikely to be implemented? The problem is that the focus on foreign citizens rather than only foreign states and their agents comes with the logic of understanding foreign intelligence priorities in an era marked by the threat of terrorism. Terrorism is a threat to the state and state security but not one that comes from another state. Terrorists are typically understood as individuals rather than state agents. States also see the rule of law question as yielding different answers depending on whether they are dealing with their own citizens or foreign citizens—as the President’s Review Group put it, abuse from one’s own state requires heightened protection domestically and justifies the differential treatment between citizen and foreigner (The President’s Review Group 2014). This is also why treating surveillance in the context of terrorism is not seen as the same thing as surveillance in the general law enforcement context—state security is thought to raise unique issues and justify broader preventative measures.

The heart of the matter, therefore, is not the question of privacy. Rather, the central issue is how we understand the goals of state surveillance and what is necessary and proportional to achieve these goals. This involves questioning the kind of threat terrorism actually poses to national security, the differences between national security and law enforcement, and whether there is a principled distinction between foreigner and citizen, among others. These are not privacy questions but their answers will define the scope of privacy protection.

Acknowledgements

I would like to thank Randy Lippert and Arthur Ripstein for their helpful comments on an earlier draft.

References

- Austin, Lisa M. 2015a. “Lawful Illegality: What Snowden has Taught us About the Legal Infrastructure of the Surveillance State.” In: *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, ed. Michael Geist. Ottawa: University of Ottawa Press.
- Austin, Lisa M. 2015b. “Anti-Terrorism’s Privacy Sleight-of-Hand: Bill C-51 and the Erosion of Privacy.” In: *After the Paris Attacks: Responses in Canada, Europe, and Around the Globe*, eds Edward M. Iacobucci and Stephen J. Toope. Toronto: University of Toronto Press.
- Austin, Lisa M. 2014. “Enough About Me: Why Privacy is About Power, Not Consent (or Harm).” In: *A World without Privacy?: What Can/Should Law Do*, ed. Austin Sarat. New York: Cambridge University Press.
- Austin, Lisa M. 2013. “Getting Past Privacy? Surveillance, the Charter, and the Rule of Law.” *Canadian Journal of Law and Society* 27: 381-98.
- Cole, David. 2014. “The Difference Prevention Makes: Regulating Preventive Justice.” *Criminal Law and Philosophy*. (March 25) Accessed May 4, 2015: <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2363&context=facpub>.
- Criddle, Evan J. 2010. “Mending Holes in the Rule of (Administrative) Law.” *Northwestern University Law Review* 104(3): 1271-1280.
- Dyzenhaus, David. 2006. *The Constitution of Law: Legality in a Time of Emergency*. Cambridge: Cambridge University Press.

- Forcese, C. 2011. "Spies Without Borders: International Law and Intelligence Collection." *Journal of National Security Law & Policy* 5(1): 179-210.
- Hurley, Lawrence. 2014. "Supreme Court Will Likely Rule on NSA Programs, Antonin Scalia and Ruth Bader Ginsburg Suggest." *Huffpost* (17 April): http://www.huffingtonpost.com/2014/04/17/supreme-court-nsa_n_5170559.html.
- The President's Review Group on Intelligence and Communications Technologies. 2014. *The NSA Report: Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*. Princeton: Princeton University Press.
- United Nations Office of the High Commissioner for Human Rights. 2014. *The Right to Privacy in the Digital Age*. A/HR/27/37.
- Vermeule, Adrian. 2009. "Our Schmittian Administrative Law." *Harvard Law Review* 122(4):1095-1149.