Quis Custodiet Ipsos Custodes? Security, Big Data and Secrecy

Dennis Broeders*

‘But who will guard the guardians?’ wrote Juvenal at the turn of the first and second century AD in his satires. Juvenal was writing of marital fidelity – how can men enforce moral behaviour on women when their guards are corruptible by immorality themselves – but the phrase is now mostly used when we talk about the use of power. How can we be sure that those who exercise force in our name – if we are lucky enough to live in a democracy – do so in a legitimate manner that does not violate our rights as citizens and do not overstretch their legal authority in exercising the state’s monopoly on the legitimate use of force. This has always been a tightrope to walk, relying both on restraint on the side of the authorities and on the vigilance of citizens and the institutions of the rule of law. The age of Big Data has not made this any easier.

Orin Kerr of the George Washington Law School put forward an interesting formula for the relationship between law, technology and security: ‘the equilibrium-adjustment theory’.1 His argument runs as follows: ‘When new technologies expand law enforcement’s capabilities, the law does (and should) respond by placing new limits on the government; when new technologies give criminals a leg up, the law does (and should) respond by loosening the government’s reigns’. In principle that looks fine, although it seems to me that many governments have been keener on loosening their own reigns than on placing limits on their use of new technologies. The Snowden revelations did not show a government bent on limiting its newfound technological possibilities for surveillance. Quite the contrary.

Technological progress and the political prioritisation of security however do not develop in a vacuum. There is a context of laws and regulations and public scrutiny and debate. In constitutional states the watchers are being watched. However, the combination of new technology and securitisation also leads to various degrees of complexity and institutional secrecy that hampers the ability of lawmakers, oversight authorities and the general public to form informed views on what is going on.

Security and Secrecy: Necessary, Layered, Convenient and Risky

The security agencies of the state usually operate to some extent in secrecy. The rule of thumb is that the closer they are to national or international security the more their

DOI: 10.21552/edpl/2017/3/4

* Dennis Broeders is Professor of Technology and Society at the department of Public Administration and Sociology of the Erasmus University Rotterdam, The Netherlands, and a Senior Research Fellow at the Netherlands Scientific Council for Government Policy, an advisory body to the Dutch government, in The Hague. For correspondence: <broeders@esb.eur.nl>.

movements are shrouded in a legally defined secrecy. Moreover, ‘national security’ and ‘public safety’ are among the keywords that exempt state agencies charged with security from the direct application of standard data protection and privacy law as laid down in (international) law. That does not mean that they are unregulated in this regard as they usually are covered by specific laws that lay down their own – more limited - version of privacy and data protection. This secrecy serves a purpose. One cannot win the fight against terrorism, organised crime and foreign state actors under conditions of full transparency. There is such a thing as too much disinfectant when it comes to security. That does not mean that Orin Kerr’s formula to rethink powers and safeguards when technology changes does not apply anymore. Quite the contrary, but conditions of secrecy make it all the harder to find new equilibria.

Moreover, new technologies such as Big Data analytics, machine learning and the algorithms on which they operate, add a layer of complexity that effectively amounts to another layer of secrecy. The algorithmic heart at many new security policies that rely on data analytics is a black box; something that is technologically hard to understand and is often set up in such a way that only the experts stand a chance of understanding how it functions. When it comes to the data analytics used by security actors we are talking about a technological black box operating within a legal black box. To make things even more complicated: sometimes the algorithms used are commercial proprietary algorithms that are protected as a trade secret, adding yet another layer of secrecy.

Obviously, secrecy is also to a degree convenient for the agencies involved. It is easier to do a difficult job at the edges of the law if you can do so away from prying eyes. This is not to say that police and security and intelligence organisations in liberal democracies would prefer to operate outside of a legal framework. It seems to me that most of the people that work for these government agencies do so because they want the democratic constitutional state to thrive and not to see it hollowed out. It does mean that in determining the degree of transparency to operate legitimately, they will probably choose to err on the side of secrecy. Secrecy makes their work possible, but everything has its tipping point.

Using new data technologies in security policies also carries risks. Both for the state agencies involved and for the general public. For the authorities, secrecy in the digital age is not what it used to be. Peter Swire, a member of the commission tasked by President Obama with looking into the functioning of the US intelligence services, has said that in the digital era secrets are not likely to remain secrets for as long as they used to. He called this the ‘declining half-life of secrets’. Technological advances, the

---


fact that intelligence services work in public-private partnership far more often (instead of relying on employees with a self-professed lifelong calling), and the multiplicity of sources they use, make the secrets they keep vulnerable. The collection of information is less the issue than keeping secret the fact that you are collecting it, which is getting much more difficult. The resulting leaks of large quantities of classified information (WikiLeaks, Snowden) change calculations of legitimacy and effectiveness.

On the side of the general public, the digital combined with security policies and secrecy has been a game changer as well. Besides obvious, but sometimes hard to legally pin down, risks in the areas of privacy and data protection, some see the biggest risk in the effects of grand scale surveillance on the freedom of the general public. The large-scale collection, storage and analysis of data by government bodies, including intelligence and security services, and the loss of anonymity on the Internet, can give people the feeling that their privacy and freedom of expression are in danger. This can undermine civil liberties and lead to chilling effects, that is, cause people to modify their behaviour and restrict their own freedom because they know or suspect that they are being monitored. Harvard International Relations Professor Stephen Walt maintains that chilling effects, rather than loss of privacy, are the real cost of the NSA activities exposed by Snowden: ‘You should be worried because it is another step in the process of making our vibrant, contentious, and most of all free-minded citizenry into a nation of sheep’. The damaging effects are greatest for people and organizations that matter to the functioning of democracy, such as journalists, writers, whistle-blowers, NGOs and lawyers.

Trust, but Verify…

There is no doubt that technology has given both the criminal and the government a leg up in terms of capabilities. The loosening of the government’s reigns that is needed should however be accompanied by a rethink of the checks and balances to ensure that new powers are being used responsibly and legitimately. The fact that some things are now simply easier and cheaper – 24-hour surveillance through digital means is only a fraction of the cost and effort of 24-hour surveillance in the non-digital realm – is not in itself enough reason to use it. ‘Because we can’ is not a legitimate reason in a constitutional state. Also, the age of big data means that the data of many more people will pass through the servers and algorithms of police and security agencies than in earlier times when investigations were mostly started up on the basis of specific leads and suspicions. Big Data analytics entails profiling and painting large groups of persons in different shades of grey – suspicion – and follow up on the darkest ‘greys’ with investigations. Some of those will lead to operations and arrests, other will stay in the back offices and the servers of the agencies, where we don’t really know if the grey will continue to stick to your name and profile. All of this is a game changer –

both in terms of law enforcement possibilities as well as in terms of possible violations of citizen’s rights.

That means we need a rethink of transparency and accountability. Governments need to get more creative on transparency. Simply saying that it is secret because it is about (national) security is going to be untenable in the age of datafication. Mass surveillance without any meaningful transparency – at a level that does not compromise operations and methodology – is needed to safeguard a minimum level of accountability to the general public. Obviously, transparency when it comes to matters of (national) security can only go so far. Not everything can and has to be held accountable in the full light of sun. But someone does need to guard the guardians on our behalf.

In its 2016 report on Big Data and security policies, the Netherlands Scientific Council for Government Policy, an advisory body to the Dutch government, addressed this question of accountability by advising to implement a system of layered accountability that would shift its regulatory focus from the collection of data to the regulation of the analysis and use of (big) data in security policies. A foreword does not allow for a detailed representation of all the recommendations in the report but the main thrust of the argument is that the use of Big Data analytics in national security, law enforcement and the fight against fraud requires extra safeguards to protect citizens’ fundamental rights. This requires a crucial shift in emphasis from regulating Big Data collection to regulating the phases of analysis and use. In order to benefit from the use of Big Data analytics in the field of security, a framework has to be developed that adds new layers of protection for fundamental rights and safeguards against erroneous and malicious use. Additional regulation is needed at the levels of analysis and use, and the oversight regime is in need of strengthening.

At the level of analysis – the algorithmic heart of Big Data processes – a duty of care should be introduced that is part of an internal audit and external review procedure. This would introduce a layered system of transparency and accountability as the review procedure should result in a report to the competent oversight authority, which can then in turn report to parliament. This way, accountability is divided into stages, with a trusted external party in the form of an oversight authority first of all, followed by a public report to parliament. As reports to oversight authorities are not made public, there is room for greater transparency and detail. The subsequent public report that is sent to parliament does not reveal the ‘tricks of the trade’, ie the specific methods used, but it is written with knowledge and understanding of them.

These would be possible first steps towards a much needed rethink of ‘trust, but verify’ in the age of Big Data.

---

6 The original report was published in Dutch as: Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving* [Big Data in a free and secure society] (Amsterdam University Press 2016). The general argument and recommendations of this advisory report have also been published in English as: Broeders et al (in 2).