2013

PRISM and Privacy: Will This Change Everything?

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Brussels Privacy Hub

Christopher Millard
Cloud Legal Project

Dan Jerker B. Svantesson
Bond University

Editorial

PRISM and privacy: will this change everything?

Christopher Kuner*, Fred H. Cate**, Christopher Millard**, and Dan Jerker B. Svantesson***

Both the offline and online media have reported extensively on access by the US National Security Agency (NSA) to electronic communications data held by private companies, most notably via the so-called PRISM program. Meanwhile, there is growing concern regarding reports the UK's Government Communications Headquarters (GCHQ) is conducting massive surveillance of communications traffic both on its own behalf and for the benefit of other members of the 'Five Eyes Alliance' (comprising the UK, the USA, Canada, Australia, and New Zealand), and other European governments have been reported to have entered into arrangements to share the data collected by the USA and the UK. At least one European government (France) allegedly also runs a vast electronic surveillance operation of its own.

We hesitate to make pronouncements about such developments before the facts are clear, but feel justified in predicting that they will have significant long-term impacts on data protection and privacy law around the world, and on the political, economic, and social climate for data processing.

Not that there is anything new in systematic governmental access to private sector data. In November 2012 we published a symposium issue (volume 2, number 4 of *IDPL*) containing legal analysis of such access in nine countries (Australia, Canada, China, Germany, India, Israel, Japan, the UK, and the USA; further reports will be published in an upcoming issue), and a guest editorial concluded that it is a widespread phenomenon and gives rise to a number of legal issues that should be urgently addressed. Systematic government access to private data thus goes far beyond a particular country and a particular intelligence agency.

Nevertheless, in their scope and detail, the recent revelations have exceeded what was publicly known, and have put the phenomenon of government access to online data in a whole new light. We acknowledge that data protection and privacy are not absolute rights, and the difficulty of balancing them against other important societal values, such as public security. These sorts of determinations go beyond what can be dealt with in an editorial; rather, we want to stress the importance of asking the right questions so that decisions can be made about what the proper balance is between privacy and security.

The following are a few fundamental questions raised by these revelations:

Should the notions underlying data protection law be reconsidered?

In its ground-breaking 'Census Judgement' rendered in 1984 and recognizing a right to informational self-determination, the German Federal Constitutional Court relied on the conclusions of the German sociologist Niklas Luhmann that a functioning democracy is only possible if citizens have the ability to oversee and control the kind of personal data about them that is available. It is now clear that online activity results in the collection and processing of a huge amount of data not only by the private sector, but by law enforcement authorities as well. Is informational self-determination the correct paradigm for data protection law, since it seems that, in fact, individuals have no way to control whether (for example) their online data are analysed by law enforcement authorities, or even to know if they are being analysed? If a new theoretical paradigm for data protection is needed, what is it?

Can both traditional and new regulatory models remain relevant?

Traditional data protection regulatory models have been based on steps such as registration of data processing with data protection authorities, informing individuals about the processing of their data, and requiring a legal basis for processing. Do such models retain any power to protect the rights of individuals in the face of large-scale law enforcement data access? Newer regulatory concepts like accountability place less emphasis on bureaucratic requirements, and more emphasis on the responsibility of data controllers to comply with the law. But is it consistent on the one hand to require data controllers to

* Editor-in-Chief
** Editor
*** Managing Editor

implement detailed compliance steps, while on the other hand obliging them to make their databases available to law enforcement authorities? And what is left of transparency when controllers are forbidden even to reveal that access has been given?

Is there justification for different data processing rules governing the private and law enforcement sectors?

The law typically places differing obligations on data processing in the private and law enforcement sectors. Does this distinction retain any justification in a world where law enforcement relies heavily on access to data initially collected by private companies?

What are the implications for cybersecurity?

The public has long been told that allowing the creation of massive databases, and storing data online, can lead to an increased level of data security, since technology companies can implement a higher level of security than individual users can. But is this really true if the companies allow law enforcement agencies to have access to the data? Could individual storage of data by users have security advantages over mass online storage?

Are companies always innocent victims in clashes between data protection and government data access?

Many companies have portrayed themselves as caught in a conflict between data protection requirements on the one hand, and government data access requirements on the other. Will such assertions remain credible if it is proven that some companies have been cooperating voluntarily with law enforcement authorities in allowing them access to data they hold?

Are governments willing to take a consistent position on their data access practices?

As an example, the German government expressed concern about the revelations concerning NSA and GCHQ data access, while simultaneously proposing a substantial expansion of its technical capability to monitor data traffic on the Internet. Do governments realize that they are sending mixed messages on whether law enforcement data access is necessary, and if so, do they care about the effect this is having on public trust?

What effect will government data access have on current and emerging business models?

Business models such as 'big data' and 'cloud computing' are only viable if the individuals and companies using them have confidence in the confidentiality and security of data processing. Could the recent revelations lead to the increased use of national or regional 'clouds' (and thus to further balkanization of the Internet), and to new legal restrictions on data analytics?

What are the implications for global privacy harmonization efforts, and indeed free-trade initiatives, of an apparent disregard for the privacy interests of 'foreigners'?

President Obama and senior members of his administration were quick to assure the American public that PRISM and similar surveillance systems are only targeted at non-Americans. This has not played well outside the USA, and has led to headlines such as 'Who authorised the NSA and GCHQ to spy on Germans?' (*Spiegel International*) as well as allegations by the Chinese government of US hypocrisy on human rights issues. Meanwhile, the UN's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has expressed concern at 'an alarming trend towards the extension of surveillance powers beyond territorial borders, increasing the risk of cooperative agreements between State law enforcement and security agencies to enable the evasion of domestic legal restrictions'. The Rapporteur also called on States to 'refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services'. The current EU data protection reform process has provoked intense lobbying by and on behalf of US multinationals to limit what are characterized as unnecessarily restrictive rights for individuals. Will we now see a counter-initiative by the European Commission, EU data protection regulators, and other interested bodies, with calls for enhanced US privacy protection (even for foreigners) to be an integral part of a comprehensive transatlantic free-trade accord?

We do not know the answers to the above questions, and some of them may turn out to be more relevant than others. But we are certain that we are not the only ones who are currently asking them.

In our symposium issue last year, the guest editorial concluded that 'global companies, governments committed to human rights, and privacy advocates should undertake a serious dialogue leading to a better understanding of current practices and of the legitimate needs of governments, businesses, and individuals, thus contributing to the development of more effective frameworks for privacy protection, commerce, and governmental interests'. The revelations of the last few weeks have demonstrated that such a dialogue is long overdue; governments are moving ahead with sweeping data gathering and analysis initiatives while too much of our approach to data protection remains mired in the last century. Indeed, there seems to

exist a kind of 'parallel universe' concerning the collection and sharing of electronic surveillance data for law enforcement purposes that operates independently of the regular legal standards for data protection. The lack of any transparency concerning the operation of this separate framework, and the justification for it, is worrisome, to say the least.

A serious dialogue about all of these issues is essential if fundamental rights—to both privacy and security—are to be protected and individuals throughout the world are to have confidence in the rule of law.

doi:10.1093/idpl/ipt020
Advance Access Publication 12 September 2013