2015

Internet Balkanization Gathers Pace: Is Privacy the Real Driver?

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

Orla Lynskey
London School of Economics

Editorial

Internet Balkanization gathers pace: is privacy the real driver?

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

'[W]e do not really trust the Data Acts in other countries or . . . we understand that there are none at all. So we feel unprotected in those countries with our data – walking down Fifth Avenue in our underwear'.

Provocative exclamations of distrust have become commonplace in recent skirmishes between the EU and the USA over data privacy and trade policy. This is, however, well-trodden ground. Indeed, the statement above was made in the late 1970s by Kerstin Amer, an Under Secretary of State in the Swedish Government, as a justification for the world's first national data protection law, a statute which included a requirement that prior authorization be obtained for exports of personal data. During the 1970s and early 1980s various other countries also raised concerns about 'data sovereignty'. Not all were European, though several appear to have been motivated by anxiety about a US hegemony that was already emerging in cross-border data services. For example, a 1972 Canadian Federal Government report entitled *Computers and Privacy* acknowledged that 'as a sovereign state, Canada feels some national embarrassment and resentment over increasing quantities of often sensitive data about Canadians being stored in a foreign country'. With the benefit of hindsight, this juxtaposition of injured sovereignty and privacy concerns looks like an early example of confused thinking about data export controls. A few years later, the Brazilian Government declared its commitment "to maximize the information resources located in Brazil, declaring that 'teleprocessing services provided by means of computers located abroad are not, in principle, used by Brazil'".[1]

In response to such developments, Mr Justice Kirby, then Chairman of the OECD Expert Group on Transborder Data Barriers and the Protection of Privacy, warned in 1980 that '[t]he bureaucratic nightmare, impossibly cumbersome, ineffective, and expensive impediments to international data traffic could still develop'.[2] Since then, a key stated objective of almost all international initiatives to promote harmonization of data privacy rules has been to facilitate the free movement of personal data between states that make a commitment to enforce certain, more or less basic, data protection principles. This is true of non-binding measures, such as the 1980 OECD Guidelines, as well as treaties and other binding instruments, such as the 1981 Council of Europe Convention on data protection and the 1995 EU Data Protection Directive.

Yet agitation for stronger geographical and jurisdictional restrictions on data flows persists, including recent calls for transfers to be restricted between entities that are already subject to legally binding mechanisms to protect cross-border flows of personal data (such as the EU-US Safe Harbor). The temperature of the debate has risen markedly since the Snowden revelations began to emerge, with suggestions recently that even transfers within established free-flow regions (such as the EEA) should be curtailed.

A specific example of an initiative that might lead to material disruption of cloud and other Internet-based services is talk in Europe about development of a possible virtual Schengen area. Although so far rather inchoate, this appears to be an attempt to create an online free movement zone for data to operate alongside the physical Schengen Area within which internal border controls have already been removed between most EU and EFTA countries. The idea was first aired in February 2011, not in a data protection context, but during a discussion of cybercrime at a Joint Meeting of the EU's Law Enforcement and Customs Cooperation Working

* Editor-in-Chief.
** Editor.
*** Managing Editor.
**** Book Review Editor.

1 For a more detailed discussion with further examples of early calls for localization of data processing operations, see chapter 9 of Christopher Millard, *Legal Protection of Computer Programs and Data* (Carswell / Sweet & Maxwell, Toronto / London, 1985).

2 'Data Flows and the Basic Rules of Data Privacy' (1980) 16 Stan J. Int. L 27–66 at 29.

Parties. As the minutes attest: 'The Presidency of the LEWP presented its intention to propose concrete measures towards creating a single secure European cyberspace with a certain "virtual Schengen border" and "virtual access points" whereby the Internet Service Providers (ISP) would block illicit contents on the basis of the EU "black-list"'. The idea was revived in August 2013 when Thierry Breton of EU cloud provider Atos (and France's former Minister of Economy, Finance and Industry) proposed 'a kind of Schengen for data'.[3] It is far from clear what this might mean in practice. For example, what would be the status of the two major EU countries that are outside the existing Schengen Area? One, the UK, is the main centre of gravity for financial services in Europe; the other, Ireland, hosts a substantial proportion of Europe's cloud computing infrastructure.

Initiatives in some individual EU member states have gone even further, with Deutsche Telekom announcing in October 2013 that it planned to build a German-only 'Internetz' to keep German Internet traffic within Germany's physical borders.[4] Meanwhile, the war of words between the EU and USA over systematic mass surveillance has provided fertile ground for states like Russia to argue that they too can no longer trust their citizens' data to invasive foreign regimes. In terms rather reminiscent of the quote from Kerstin Amer that opened this Editorial, Russian MP Vadim Dengin is reported to have justified to the State Duma the mandatory local storage obligations in Russia's new data protection law with the rousing words: 'Most Russians don't want their data to leave Russia for the United States, where it can be hacked and given to criminals. Our entire lives are stored over there'.[5]

Would any of this really enhance privacy protection? There are serious reasons for doubting that any of the current initiatives would actually do so. This is largely because strategies of this type that are supposed to protect individual rights, in particular by constraining data location and transfers, continue to be commingled with motivators based on vague concepts of national sovereignty and economic advantage. As we have noted previously, the Snowden revelations of systematic government surveillance have led to soul-searching about both the relevance of fundamental privacy concepts and the effectiveness of existing frameworks for ensuring protection of personal data.[6] As with that surveillance debate, arguments about Internet regionalization and data localization are often stymied by a fundamental lack of transparency. Indeed, by mandating storage of data within their own national boundaries, governments may hope to gain increased access to such data. Mixed messages and hypocrisy abound and privacy is increasingly invoked as a justification, or at least used as a smokescreen, for policies that are incoherent and, in many cases, far from privacy-enhancing.

What is needed, and what we have not yet seen, is a detailed and credible explanation by proponents of data localization as to how such initiatives would enhance privacy protection, restrain intelligence surveillance, and generally increase the level of privacy online. Until such an explanation based on serious legal and computer science considerations is put forward, it is right to remain skeptical about the motivations behind data localization initiatives, and what their results would be.

doi:10.1093/idpl/ipu032

3 <http://www.europe1.fr/Economie/Breton-creer-une-sorte-de-Schengen-des-donnees-1620759/> accessed 17 December 2014.

4 <http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html> accessed 17 December 2014.

5 For a discussion of these and other recent 'Balkanization' initiatives see Kuan Hon and others, 'Policy, Legal and Regulatory Implications of a Europe-Only Cloud', available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2527951##> accessed 17 December 2014.

6 See our early Editorial on 'PRISM and privacy: will this change everything?' (2013) 3/4 Int Data Privacy Law. <http://idpl.oxfordjournals.org/content/3/4/217.full.pdf+html?sid=b7d189ef-0ab1-4b92-8dd9-dbaa2b4b024f> accessed 17 December 2014.