Systematic Government Access to Private-Sector Data Redux

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*

Follow this and additional works at: [https://www.repository.law.indiana.edu/facpub](https://www.repository.law.indiana.edu/facpub)

Part of the Comparative and Foreign Law Commons, Information Security Commons, and the Privacy Law Commons

**Recommended Citation**

Cate, Fred H.; Kuner, Christopher; Millard, Christopher; and Svantesson, Dan Jerker B., "Systematic Government Access to Private-Sector Data Redux" (2014). *Articles by Maurer Faculty*. 2626.  
[https://www.repository.law.indiana.edu/facpub/2626](https://www.repository.law.indiana.edu/facpub/2626)

This Editorial is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact kdcogswe@indiana.edu.
In November 2012 we published a symposium issue (volume 2, number 4 of IDPL) containing a series of papers analysing the laws and practices of nine countries (Australia, Canada, China, Germany, India, Israel, Japan, the UK, and the USA) relating to systematic government access to personal data held by the private sector. Those papers, developed as part of a multi-year project funded by The Privacy Projects—a not-for-profit organization dedicated to improving current privacy policies, practices and technologies through research, collaboration, and education—demonstrated considerable consistency in the laws and practices of the nine countries examined.

According to a guest editorial that accompanied the papers, common trends included:

- A 'significant expansion in government demands for private-sector data in general and for broad, systematic access in particular', which the authors defined as both (1) direct access by the government to private-sector databases, without the mediation or interaction of an employee or agent of the entity holding the data, and (2) 'government access, whether or not mediated by a company, to large volumes of private-sector data'.
- A consistent lack of transparency about 'not only the activities, but even the laws concerning systematic access to government data'.
- A 'surprising degree of commonality in the principles and fundamental concepts reflected in the data privacy laws of most of the countries surveyed', including the fact that 'data collection for law enforcement and national security are either exempted from general data protection laws or constitute permissible uses under those laws, subject to varying restrictions'.
- Significant inconsistencies between 'what the law says and what the irresponsible governments are reportedly doing'.
- The prevalence of 'systematic volunteerism'—suggesting that 'the most frequent way that governments obtain systematic access to private-sector information is by asking for it'.

Although published more than a year ago, those papers proved remarkably prescient in light of the subsequent disclosures by Edward Snowden and others during the past year about sweeping surveillance programmes in the United States and the United Kingdom. The programmes disclosed seemed to bear out the common themes previously identified, especially about the intensity of government demands for private-sector data, the lack of transparency about the surveillance, and the wide chasm between what the laws (and governments) say and what really takes place.

In this issue we publish four additional papers, describing the laws and practices relating to systematic government access to private-sector data in Brazil, France, Italy, and the Republic of Korea. These papers grew out of the second phase of the project supported by The Privacy Projects and, like the first set of papers, these were reviewed at a workshop of industry and academic experts prior to their publication here.

These four papers evince similar themes to those identified in 2012. The already broad requirements for industry systematically to disclose wholesale information on its customers and employees to support a wide variety of government programmes is being supplemented, and in some
cases outpaced, by government demands for systematic access to such data for national security and law enforcement purposes. The presence of sometimes vigorous privacy laws seems to have little effect on this type of access, either because national security and/or law enforcement are exempt from those laws or because it appears that the laws are not being followed.

In Brazil, for example, ‘Google was forced to sign an agreement giving authorities a direct communication channel with the company allowing officials to request data retention, removal of content, and identification of users.’ In Italy, “‘systematic’ access to private data, although starkly infringing on personal liberties, is increasingly being favoured by the most recent legislation.”

Perhaps the most striking examples of expanding direct or unmediated access to broad swaths of personal data held by the private sector come from France. French law ‘not only requires telecommunications operators to retain for one year traffic data (including location data and Internet logs), but also requires hosting providers to retain similar logs relating to persons who create or store data using their hosting service.’

French government officials have access to this and other information through three different provisions of national law. The first allows the government access to traffic and location data from telecommunication operators for any ‘terrorism-related’ investigation with recourse only to the Prime Minister’s agreement giving authorities a direct communication channel with the company allowing officials to request data retention, removal of content, and identification of users. In Italy, “‘systematic’ access to private data, although starkly infringing on personal liberties, is increasingly being favoured by the most recent legislation.”

The second permits access to the same data ‘in connection with potential national security interceptions’ with recourse only to the Prime Minister’s office. And the third, and most broad, authorizes the government ‘to conduct generalized monitoring of the radio transmissions in order to protect France’s national interests.’

This third avenue for ‘generalized monitoring’ without oversight has generated considerable controversy in the French press, and promises by the French parliament to restrict this power. But as recently as 5 July 2013, Le Monde reported that France’s external intelligence agency, the Direction Générale de la Sécurité Extérieure: ‘collects telephone data of millions of subscribers—the identifier of the calling parties, of the called parties, the place, date, duration and size of the message. The same thing exists for e-mails (with the possibility to read the subject line of the e-mail), SMSs, faxes . . . and all Internet activity that goes through Google, Facebook, Microsoft, Apple, Yahoo!’

According to the French Minister of Justice in 1991, generalized monitoring of radio transmissions, which may be conducted ‘without any authorization or ex post supervision,’ ‘cannot be considered as a violation of the secrecy of correspondence.’ It is hard to distinguish this type of signals intelligence gathering from that conducted by the NSA which has understandably caused so much controversy in Europe, except that the NSA had judicial authorization from the US Foreign Intelligence Court.

As the four papers that follow make clear, the issues raised by our 2012 articles on systematic government access to private-sector data—given new urgency by the disclosures by Edward Snowden and others over the past nine months—remain real and relevant around the globe. As the guest editorial that introduced the first set of country-specific articles noted, ‘[s]ystematic government access to private data thus goes far beyond a particular country and a particular intelligence agency.’

We are grateful to The Privacy Projects; the organizers of the second phase of its project on systematic government access to private-sector data—James Dempsey, Ira Rubinstein, and Ronald Lee; the authors of the four papers that follow; and the participants in the workshop who helped to review and critique the papers for their collective efforts to expand our appreciation of the challenge we face.

The next issue of IDPL will feature a detailed analysis by the organizers of all of the country-specific papers. But while we work together to shine a light on the critical challenges presented by systematic government access to private-sector data and other forms of government surveillance, there is urgent need for action. In a fall 2013 editorial, written in response to the Snowden disclosures, we stressed that:

[G]overnments 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

8 Bruno Magrani, ‘Systematic government access to Private-Sector Data in Brazil’ (2013) 4/1 International Data Privacy Law __.
9 Giorgio Resta, ‘Systematic government access to Private-Sector Data in Italy’ (2013) 4/1 International Data Privacy Law __.
10 Winston Maxwell, ‘Systematic government access to Private-Sector Data in France’ (2013) 4/1 International Data Privacy Law __ (citations omitted).
11 Id., at __.
12 Id., at __.
13 Id., at __.
17 Guest Editorial, at __.
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.18

We can only reiterate that call today. The need to modernize data protection law and to bring national security and law enforcement data collection squarely within its purview grows more urgent with each passing day and more necessary as our understanding of the breadth and scope of the problem increases. Obviously, data collection and use for national security and law enforcement presents special considerations that must be taken into account, but those do not justify wholesale exemptions from data protection laws or from the oversight that accompanies those laws.

Given the scope of the issue, we believe that action is more likely to be effective if it is undergirded by thoughtful dialogue across national borders involving data protection officials, law enforcement and national security officials, industry leaders, and advocates. To date, the 13 countries examined as part of The Privacy Projects’ work suggests that no country is immune from the problem and no country has found a perfect answer, but that there is a great deal to be learned from our collective experiences. We can do better, and we must. But as the four new papers we publish in this issue make clear, it is high time we got started.
