Systematic Government Access to Private-Sector Data

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

James X. Dempsey  
*Center for Democracy and Technology*

Ira S. Rubenstein  
*New York University School of Law*

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

Part of the *Information Security Commons*, and the *Privacy Law Commons*

**Recommended Citation**

Cate, Fred H.; Dempsey, James X.; and Rubenstein, Ira S., "Systematic Government Access to Private-Sector Data" (2012). *Articles by Maurer Faculty*. 2615.  
https://www.repository.law.indiana.edu/facpub/2615

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 rvaughan@indiana.edu.
Governments around the world have long sought access to personal information about individuals. The past half century witnessed the rise of what Professor Paul Schwartz has described as the ‘data processing model of administrative control’, in which data are routinely collected and used for many purposes including to deliver social services, administer tax programmes and collect revenue, issue licences, support hundreds of regulatory regimes ranging from voter registration to employee identity verification, operate public facilities such as toll roads and national parks, and for law enforcement and national security.

Government appetite for information about individuals has intensified in the twenty-first century, largely fed by three developments. The first is the appearance of new and dangerous threats to national security, demonstrated by terrorist attacks in New York, Washington, Madrid, London, Mumbai, and elsewhere and compounded by the rise in militant Islamic fundamentalism and increased concerns about chemical and nuclear weapons and cybersecurity vulnerabilities. The second is the explosion in the volume of digital data routinely generated, collected, and stored about individuals’ purchases, communications, relationships, movements, finances, tastes—in fact, about almost every aspect of people’s lives in the industrialized world—and the ever growing power of technologies to collect, store, and mine such data.

The third is that most of these data are collected and stored by third parties, often by service providers as a necessary incident to providing the service or because the data have independent value to third parties for marketing, research, or other purposes. Email and other electronic communications, online data storage, credit and debit card payments, wire transfers, social networking, remote monitoring, internet photo- and video-sharing services, browsing and searching, online commerce, and thousands of other services result in vast quantities of personal data being held by third parties. Increasingly, governments view these third parties as a ready, efficient, and cost-effective source of data about individuals and organizations.

In recent decades, governments around the world have obligated a wide variety of businesses to collect, retain, and share data about their customers and clients to assist in curtailing money laundering, drug trafficking, tax evasion, terrorism, and other offences. Governments have sought access to personal information held by the private sector not only by asking companies to produce specific records about a single target or a small number of people at a time but increasingly via what we refer to here as ‘systematic’ government access. As used throughout this issue, this term refers both to (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.

Government demands for systematic access are noteworthy because of the potential number and scope of records involved, the fact that the records disclosed may pertain to broad groups of individuals who are not suspected of wrongdoing, the fact that the individuals affected need not be citizens of or even resident within the territory of the government seeking the data, and the low—and declining—costs to governments.

Fred H. Cate*, James X. Dempsey**, and Ira S. Rubinstein***

* Fred H. Cate, Editor. Email: fred@fredhcate.org
** James X. Dempsey, Vice President for Public Policy at the Center for Democracy & Technology and head of CDT West in San Francisco. He coordinates the Digital Due Process coalition.
*** Ira S. Rubinstein, Senior Fellow at the Information Law Institute, New York University School of Law, and a member of the Board of Directors of the Center for Democracy & Technology.


seeking the data. In addition to demanding systematic access, governments are requiring private-sector entities to retain data so they are available when the government asks or requiring service providers to design their systems to facilitate government access.

Systematic government access to records held by third parties raises substantial challenges for individuals whose communications, transactions, and other activities are exposed to government scrutiny. But systematic access also creates challenges for businesses—both providers of digital services and the commercial customers of those services—that go beyond privacy concerns. These challenges include:

• When access sweeps in the communications and stored data of commercial entities, trade secrets and sensitive business information may be put at risk.
• The technical measures deployed on private systems and networks to support systematic access may introduce security vulnerabilities.3
• Given the lack of transparency about national practices and misunderstandings about different countries’ legal regimes, competition may be distorted as business customers shop for jurisdictions in which they believe their data may be less exposed to government access, and governments may use claimed disparities in laws to advantage domestic service providers
• Innovation may be limited if services must be designed to ensure government access.
• Lack of public trust may make individuals hesitant to use new services and new business models.4

These issues have proven especially controversial in the context of cloud computing. While the provision of services from, and the storage of data in, large shared facilities that are accessible around the world provides advantages in terms of efficiency, data security, and cost, fear of broad government access to stored data is being cited as a basis for restricting the deployment and use of cloud services. For example, the Data Protection Commissioner of Schleswig-Holstein in Germany ruled in 2011 that under certain circumstances personal data could only be stored in cloud computing facilities located within the 27 member states of the European Union.5 In September 2011, the Dutch Minister of Safety and Justice blocked US providers of cloud computing services from bidding on Dutch government contracts because of fear that US law permits too much government access to personal information held by the private sector.6 Canadian provinces have adopted similar restrictions on allowing personal information held by the public-sector to be stored or accessed from outside of Canada.7

While the contretemps over government access to data in the cloud may be motivated in part by trade and other political issues unconnected to privacy, it also reflects (indeed, it may take advantage of) a profound lack of knowledge about the extent to which most governments systematically collect and use personal data from third-parties—for myriad purposes—and the extent to which national data protection laws permit this.

In 2011, The Privacy Projects (TPP), a not-for-profit organization dedicated to improving current privacy policies, practices, and technologies through research, collaboration, and education, undertook to address this knowledge gap. It solicited proposals from privacy experts in academia and advocacy, and ultimately partnered with Indiana University and the Center for Democracy & Technology to plan and execute a project on Systematic Government Access to Private-Sector Data. Fred Cate and Jim Dempsey directed the project; Ira Rubinstein and Ronald D. Lee, a partner of the law firm of Arnold & Porter LLP, served as senior advisors.

The first phase of the project involved commissioning short, scholarly papers from leading experts on the law and recent controversies concerning systematic access in nine countries: Australia, Canada, China, Germany, India, Israel, Japan, the United Kingdom, and the United States. Each of the authors was asked to follow a common template and to provide the most current information available.

In addition, we invited two additional papers that we believed would be relevant and useful to understanding current controversies over systematic government access to private-sector data. The first addresses

4 See, for example, Deven McGraw, James X Dempsey, Leslie Harris, and Janlori Goldman, ‘Privacy as an Enabler, Not an Impediment: Building Trust into Health Information Exchange’, (2009) 28 Health Affairs 416, 417 (citing public concerns with electronic health records and evidence that patients will withhold information from doctors if not assured that it will be protected against inappropriate use or disclosure).
7 British Columbia Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004, sect. 30.1; Bill No. 19—the Nova Scotia Personal Information International Disclosure Protection Act, 2006, sect. 5(1); Quebec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, sect. 70.1 (added by 2006, c. 22, s. 47); Alberta Personal Information Protection and Electronic Documents Act, sect. 40(1)(g); Canada Privacy Act, sect. 82(f).
the constitutional privacy jurisprudence of the Supreme Court of the United States, a nation whose privacy laws are shaped by that jurisprudence and are often at issue in controversies over transnational government access to personal information. The second paper addresses the role of encryption in government access to data and the extent to which encryption technologies and practices may influence governments’ desire to access data stored in the cloud.

Those eleven papers provided the background for a day-long workshop of industry, not-for-profit, and academic experts (including authors of several of the papers) in Washington in April 2012. The discussion there reinforced many of the findings of the papers and helped to identify cross-cutting themes. It also guided TPP on possible next steps to reduce the knowledge gap among nations as to their laws and practices concerning broad government access to data held by third parties. After the workshop, the paper authors had an opportunity to revise and update their papers.

The papers that appear in this issue provide detailed information about the laws and publicly reported activities relating to systematic government access to private-sector data in the nine countries. Each of the authors has provided a brief abstract; to try to summarize them further would be unnecessarily duplicative.

However, what first struck us and many of the participants in the workshop when we read the papers were the broad themes that many of the papers—and the laws and practices of the countries they reported on—had in common. We highlight eight of those here:

1. Lack of transparency—Most of the authors, despite being experts in their respective countries’ data-related laws, noted the difficulty inherent in assessing not only the activities, but even the laws concerning systematic access to government data. The difficulty begins with the fact that, even though laws or regulations defining governmental powers to access data are generally public, those laws and regulations are often vague or ambiguous, so it is hard to tell from reading them what the government is actually doing. Interpretations of the law are often not made public. Even when the law seems clear, its application in practice is often secret. National security practices are normally ‘classified’ and it is often hard to get a comprehensive picture of practices in criminal cases.

2. Significant expansion in systematic access—Despite the difficulties with transparency, in every country addressed by these papers there is evidence of a significant expansion in government demands for private-sector data in general and for broad, systematic access in particular. The papers reflect expansive mandatory reporting of financial transactional information, air passenger and visitor data, communications-related data (e.g., subscriber or device information), and other categories. Data collection by governments appears to be on the rise across the countries our colleagues addressed. At the same time, private-sector organizations are facing increased requirements to collect, verify, and retain information on their customers and employees. Sunil Abraham could be describing most of the countries we studied when he writes about India: ‘typically all employers must disclose business transactions to the government, doctors must report the occurrence of specific diseases, and banks must report suspicious transactions that could be connected to money laundering. A growing global trend, though, that has also begun in India, is systematic governmental access, disclosure, retention, and collection of information for the purposes of surveillance, national security, and crime detection.’

3. Significant commonality across laws—There was a surprising degree of commonality in the principles and fundamental concepts reflected in the data privacy laws of most of the countries surveyed: 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; there is some reliance


on (and tension around the adequacy of) external approval or review mechanisms to oversee such access, whether a court, high-ranking government officials, or a committee established for the purpose, such as the German G-10 Commission; and the laws and regulations that are in place focus on individual requests for specific data to the complete or near exclusion of addressing systematic government access. Some other common themes are addressed in greater detail below.

4. Inconsistency between law and practice—Many authors report perceived inconsistencies between what the law says and what their respective governments are reportedly doing. This does not necessarily mean that the activity is illegal, but rather that it occurs subject to a legal interpretation that is withheld from the public or takes place in the interstices of national regulation. For example, the Berlin police have reportedly obtained information on 4.2 million cell phone conversations since 2008; and US law enforcement officials made at least 1.3 million demands for text messages, caller locations, and other subscriber information from cell phone carriers in 2011; and the British government has announced plans to require internet companies to install devices to allow government access to ‘phone calls, text messages and emails as they are made’. The difficulty in squaring the magnitude of access to sensitive data reflected in these and other examples with the respect for privacy often asserted by officials in these countries further illustrates how hard it is to achieve an accurate and comprehensive understanding of actual law and practice.

5. National security and law enforcement exceptions—As noted above, in countries with otherwise comprehensive data protection laws, national security and law enforcement are often excluded from such laws, or are broadly accepted purposes for which such access is permissible. This proved to be the case in every country we examined, even in those nations with the most well developed data protection regimes. For example, Dan Svantesson writes that Australian laws ‘taken together … provide Australian law enforcement and national security agencies with broad access to private-sector data.’ The result is that data collection and use for national security and law enforcement purposes is often excluded from oversight applicable to other data processing activities or subject to far less transparent standards and oversight regimes.

6. The declining ‘wall’ between national security and other uses—The impact of the broad exceptions for national security and law enforcement activities is expanded by the fact that in most of the countries studied, data collected for one purpose may be used for other legitimate government activities, and the ‘wall’ that historically limited the use of data collected under the relaxed standards applicable to national security is disappearing. For example, the United Kingdom’s Counter-Terrorism Act of 2008 explicitly provides: ‘Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.’ As Paul Schwartz writes, typical of all of the countries studied, ‘a significant development in Germany since 9/11, and, indeed, since the end of the Cold War, has been a steady stream of legislation that expands the powers of the BKA, BND, Federal Office for the Protection of the Constitution, as well as related agencies, and an increase in their ability to work together and to share information.’ Sunil Abraham puts it more bluntly in the case of India: ‘Standards for governmental use of accessed information vary across sectors, and in most cases are non-existent.’ ‘Use limitation’ is a key element of fair information practice principles. When combined with the greater ease with which national security and law enforcement gain access to private-sector data in the first place, the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected represents a substantial weakening of traditional data protections.

7. ‘Systematic volunteerism’—The papers that follow suggest that the most frequent way that governments obtain systematic access to private-sector information is by asking for it, what one workshop participant

15 Schwartz, (n 6).
16 Abraham, (n 8).
labelled ‘systematic volunteerism’. What Ian Brown writes about the United Kingdom appears to apply to most of the countries studied: ‘The most plausible means for systematic UK government access to private-sector data is through voluntary agreements with the operators of systems and databases.’\textsuperscript{17} Governments often claim that such arrangements are permitted under existing legal frameworks and are justified as simply making more efficient that which is already permitted. Companies establishing such arrangements appear motivated by a variety of factors including patriotism, a desire for good relations with government agencies (both for regulatory and sales purposes), a lack of understanding that national law does not require compliance with such requests, fear of reprisals if they do not cooperate, and the ability to generate revenue by selling the government access to the data they possess.

8. Importance of multinational access and sharing—Finally, most of the nations surveyed appear to consider cross-border access to data essential to national security, law enforcement, and other government activities. Most assert the authority under their national laws to access data stored in other countries, both by means of demands enforced against the domestic officers of the data custodian and by seeking access through foreign partners under bilateral or multilateral agreements. Jane Bailey captures a common theme when she writes about Canada’s first comprehensive counter-terrorism strategy that a ‘key priority of the strategy appears to be ensuring information exchange between and amongst these domestic players, as well as with similar agencies acting for international partners.’\textsuperscript{18}

In sum, analysis of government demands for systematic access must begin with the recognition that, even in countries with the broadest and most systematic data protection laws, data collection and use for national security and law enforcement are generally beyond the scope of those laws or constitute an express exception to them. The separate laws that do set standards for government surveillance and access are often ambiguous, allow great latitude in the area of national security, and are being outpaced recently by technology. In addition, for many years there have been mandatory reporting requirements in every country surveyed that force the private sector to report varying amounts of sensitive personal information to the government for routine administrative and regulatory purposes; such requirements have always represented a certain disconnect between data protection law and the reality of government access to and use of private-sector data. Now, on top of these realities, to varying degrees, governments worldwide are seeking systematic access to private-sector data, for which the already limited or outdated legal frameworks provide little assurance of proportionality, transparency, or accountability.

Taken together, these global trends suggest that it is time to recognize that the challenges of government access are widespread and should not, at least among the democratic countries, be the basis for cross-border polemics. Instead, 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. We offer the following papers as one initial step in that process.

We are grateful to the authors of the eleven papers included in this issue for their excellent work under a tight deadline, and to the editors of International Data Privacy Law for devoting a single issue to making these important pieces available to a wide audience. We also wish to thank the participants in the April 2012 workshop. Finally, we wish to thank the board of directors of The Privacy Projects for their support throughout this project and for their commitment to expanding multinational understanding of laws and practices relating to systematic government access to private-sector data, both now and in the future.


\textit{Advance Access Publication 17 September 2012}

\textsuperscript{17} Brown, (n 14).