Systematic Government Access to Personal Data: A Comparative Analysis

Ira Rubinstein, New York University School of Law
Greg Nojeim, Center for Democracy & Technology
Ronald Lee, Arnold & Porter LLP*

November 13, 2013

Funded by The Privacy Projects

The Center for Democracy & Technology is a leading non-profit advocacy and civil liberties organization dedicated to keeping the Internet open, innovative, and free. Based in Washington, DC, CDT is committed to finding forward-looking, collaborative solutions to today's most pressing Internet and technology policy challenges, while championing global online civil liberties and human rights.
www.cdt.org

For further information:

Jens-Henrik Jeppesen
Representative & Director, European Affairs
Center for Democracy & Technology
Rue d'Arlon 25, B-1050 Brussels
Tel: +32(0) 2 234 61 85
GSM: +32(0) 477 183 285
Fax: + 32(0) 2 234 61 81
Email: jjeppesen@cdt.org

Greg Nojeim
Director, Project on Freedom,
Security and Technology
Center for Democracy & Technology
1634 I Street, NW
Washington, DC 20006
Tel: +1 202 407 8815
Email: gnojeim@cdt.org

* Ronald Lee took no part in the preparation of any portions of this report referring to US government activities and programs.

Table of Contents

Executive Summary……1

Introduction.....4

New Revelations of Systematic Surveillance Activities 11

Common Themes from the Country Reports 15

Comparative Analysis: The Descriptive Framework 20

Comparative Analysis: The Normative Framework 31

Recommendations and Conclusions 42

Executive Summary

In recent years, there has been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors. This includes an expansion in government requests for what we call "systematic access:" direct access by the government to private-sector databases or networks, or government access, whether or not mediated by a company, to large volumes of data. Recent revelations about systematic access programs conducted by the United States, the United Kingdom and other countries have dramatically illustrated the issue and brought it to the forefront of international debates.

Although it seems that systematic access is growing, there are also cases – in Germany, Canada, and the UK - where government proposals for expanded access have recently been rejected due to public and corporate concerns about privacy, cost, and the impact on innovation.

This report is the culmination of research, funded by The Privacy Projects, that began in 2011. In the first phase of the study, outside experts were commissioned to examine and write reports about laws, court decisions, and any available information about actual practices in thirteen countries (Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States). Two roundtables were held with private-sector companies, civil society, and academics. Based on that research, for this report we identified a number of common themes about the countries examined and developed a descriptive framework for analyzing and comparing national laws on surveillance and government access to data held by the private sector. We also developed a normative framework based on a series of factors that can be derived from the concept of "rule of law," from constitutional principles, and from existing (although still evolving) international human rights jurisprudence.

Key Findings

We found that in most, if not all countries, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level.

Even after the Snowden leaks, transparency remains weak, so we lack an accurate or comprehensive understanding of systematic access.

- The relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified.
- Practices are often opaque; it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment.

- Oversight and reporting mechanisms are either absent or limited in scope when they exist, and generally do not reach voluntary data sharing.

In every country we studied, even those nations with otherwise comprehensive data protection laws, access for regulatory, law enforcement, and national security purposes is often excluded from such laws, or treated as accepted purposes for which access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses. Moreover, almost everywhere, when it comes to data protection, access for national security purposes is more sparingly regulated than is access for law enforcement purposes.

Overall, it seems there has been relatively little discussion of the complex legal and political issues associated with asserting jurisdiction over data stored in other countries or relating to citizens of other countries. Also, until the recent disclosures, discussion of the complex questions regarding extraterritorial application of human rights raised by trans-border surveillance has been lacking.

While standards for real-time interception of communications for law enforcement purposes are high in most of the countries we surveyed (but not in India and China), standards for access to stored communications held by third parties are less consistent. When it comes to transactional data regarding communications, standards are even weaker.

With respect to the standards for government access to communications in national security investigations, the overall picture is very complex. Almost half the countries studied do not have provisions requiring court orders for surveillance undertaken in the name of national security or for foreign intelligence gathering.

Most countries handle travel and financial data under laws requiring routine, bulk reporting for specified classes of data.

Conclusions

We reached four major conclusions, each of which has policy implications:

1. Technological developments associated with the digital revolution make it easier than ever for governments to collect, store, and process information on a massive scale. Governments seem to be exploiting these developments and responding to pressing threats such as terrorism by demanding more information.

- Policy implications: The trend toward systematic collection poses challenges to the existing legal frameworks because many of the statutes regulating government access and data usage were premised on particularized or

targeted collection, minimization, and prohibitions on information sharing and secondary use.

2. As Internet-based services have become globalized, trans-border surveillance - surveillance in one country affecting citizens of another - has flourished.

- Policy implications: Statutory frameworks for surveillance tend to be geographically focused and draw distinctions between communications that are wholly domestic and communications with one or both communicants on foreign soil. Moreover, statutory frameworks, as far as we can tell, often draw a distinction between the collection activities that an intelligence service performs on its own soil and the activities that it conducts extraterritorially.

Lowered standards for trans-border surveillance have a substantial impact on companies that offer global services and want to be able to assure their customers worldwide that their data is secure. It also raises human rights questions about the existence and scope of state duties to protect and respect privacy and free expression of people outside the state's territorial boundaries.

3. In the post-9/11 world, as technological capabilities are increasing, and as global data flows are expanding exponentially, national security powers have also been getting stronger.

- Policy implications: This combination of powerful technology and weak laws raises questions relating to the trust that citizens, customers, and users vest in governments and corporations alike, and has begun to upset diplomatic relationships and international trade.

4. This expansion in powers has been conducted in extreme secrecy.

- Policy implications: The lack of transparency makes it very difficult to have a rational debate about governmental powers and concordant checks and balances. The lack of openness is leading to proposals that could fragment the Internet, harming both innovation and access to information.

What we need globally is a robust debate about what the standards should be for government surveillance. That debate should be premised on much greater transparency about current practices and their legal underpinnings. Based on this study, we believe that international human rights law provides the most useful framework for making progress on these issues because it offers well-established criteria for assessing national surveillance and data reporting laws and practices.

I. Introduction

Governments around the world have always demanded that commercial entities disclose data about their customers in connection with criminal investigations, enforcement of regulatory systems, and national security matters. Companies have always felt an obligation - and oftentimes are under legal compulsion - to cooperate, but they have also felt a business need and sense of responsibility to protect their customers' personal data and have diligently sought to balance those interests.[1] In recent years, there has been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors. This has included an expansion in government requests for what we call "systematic access." We use this term to encompass both *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 government access, whether or not mediated by a company, to *large volumes* of private-sector data.

"There has been an increase worldwide in government demands for data held by the private sector"

This study, funded by The Privacy Projects (TPP), began in 2011. In its first phase, legal experts were commissioned to analyze systematic government access to private sector data in nine countries.[2] The country reports, an introductory paper, and other research were published in November 2012.[3] TPP then commissioned an additional four country reports and this comparative analysis.[4] Through June 2013, this research identified various examples of systematic access, while also concluding that there was a widespread lack of transparency about the nature of and legal basis for practices carried out in the name of national security or foreign intelligence. In June 2013, a flood of

[1] "Personal data" generally refers to any data that relates or is linkable to an identifiable individual, and may include aggregations of data.

[2] For each country, the authors were asked to examine legal frameworks (including both the constitutional context and the statutory and regulatory rules) and national practices (including any recent controversies involving systematic access). Generally, the authors were not able to present empirical evidence of the number of government requests per country, largely due to the lack of relevant data in the public domain.

[3] International Data Privacy Law, Volume 2, Issue 4 (2012), http://idpl.oxfordjournals.org/content/2/4.toc.

[4] The thirteen countries whose laws and practices the legal experts have examined are Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States.

disclosures began regarding intelligence programs of the US, the UK, and other countries, adding substantial details to the picture, although each new revelation makes it clear that any understanding of current practices remains fragmentary, even inside the governments themselves.

Here are some examples of what we mean by systematic access to stored data, covering a very wide range of data and justifications:

- In the US, a special court orders telecommunications service providers to disclose to the National Security Agency, on a daily basis, metadata (number making the call, number called, time, duration) for all telephone calls handled by the carriers to, from and within the country. The bulk disclosure orders have been renewed every 90 days since 2006.
- While most countries have longstanding systematic reporting requirements of a regulatory or administrative nature, especially in the area of financial services and employment, mandatory reporting of income data and other data related to the administration of taxes has expanded in recent years.[5] In other countries, there is systematic reporting of hotel registrations or airline travel itineraries.
- In Germany, telecommunication providers are required to collect certain data about their customers, such as name, address, and telephone number, before the service is established. This information, termed "inventory information," is sent to a databank of the Federal Network Agency, and other governmental agencies can make automated requests for this information from the databank.[6]
- The Chinese government maintains almost unlimited and unfettered access to private sector data through a variety of regulatory requirements. As Zhizheng Wang observed in his paper on China, "the government's systematic access to data held by anyone will become possible and realistic with the evolution of the e-government strategy, in accordance with its vital interest of maintaining the state's control on information and 'preserving the stability' of the society."[7]
- The Brazilian Communications Agency (ANATEL) was planning to "build technical infrastructure and enact regulation to allow it to connect directly into telecoms companies' systems and obtain information related to

[5] See, for example, Giorgio Resta, 'Systematic Government Access to Private-Sector Data in Italy,' International Data Privacy Law (forthcoming 2013).

[6] Paul M Schwartz, 'Systematic Government Access to Private-Sector Data in Germany,' (2012) 2/4 International Data Privacy Law 289, http://idpl.oxfordjournals.org/content/2/4/289.full.

[7] Zhizheng Wang, 'Systematic Government Access to Private-Sector Data in China,' (2012) 2/4 International Data Privacy Law 220, http://idpl.oxfordjournals.org/content/2/4/220.full.

customer's usage of services, such as numbers dialed, time, date, amount paid and duration of all phone calls made."[8] ANATEL officials claimed that their goal was to determine whether telecoms were providing services at an appropriate level of quality and to order any necessary expansion of network capacity.

- In India, the government has built a Central Monitoring System that is intended to allow the government to engage in real-time interception of email, chats, voice calls, and texting, without intervention of the service providers.[9]

We also found examples where although the government requested records one at a time regarding particular individuals, devices, facilities, or accounts, the volume of requests was quite large. For example, in the UK, government agencies made 500,000 requests for telephony metadata in one year.[10] In Germany, where local police departments can request cell tower data about any person located in a given area during a specific time period, a Berlin newspaper reported in 2012 that the Berlin police since 2008 had made 410 "radio cell inquiries" that collected information pertaining to 4.2 million cell phone connections.[11] In the US, government agencies issued over 1.3 million demands to mobile carriers in 2011, covering information ranging from basic subscriber identifying data to call detail records to cell site location information to call content.[12] The volume of requests can lead governments and private sector entities to

---

[8] Bruno Magrani, 'Systematic Government Access to Private-Sector Data in Brazil,' International Data Privacy Law (forthcoming 2013).

[9] Sunil Abraham and Elonnai Hickok, 'Systematic Government Access to Private-Sector Data in India,' (2012) 2/4 International Data Privacy Law 302, http://idpl.oxfordjournals.org/content/2/4/302.full. Also see Shalini Singh, 'India's Surveillance Project May be as Lethal as PRISM,' *The Hindu* (June 21, 2013); Bharti Jain, 'Govt Tightens Control for Phone Tapping,' *The Times of India* (June 18, 2013); Anjani Trivedi, 'In India, Prism-like Surveillance Slips Under the Radar,' *Time* (June 30, 2013), available at http://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

[10] Ian Brown, 'Government Access to Private-Sector Data in the United Kingdom,' (2012) 2/4 International Data Privacy Law 230, http://idpl.oxfordjournals.org/content/2/4/230.full. For statistics on the volume of requests for retained transactional data in other European countries, see European Commission, *Report from the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive (Directive 2006/24/EC)* (2011), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.

[11] Schwartz, n. 6 above.

[12] Eric Lichtblau, 'More Demands on Cell Carriers in Surveillance,' *NY Times* (July 8, 2012) http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html (the figure of 1.3 million understated the volume since one major carrier did not disclose the number of requests it had received).

develop automated interfaces or other arrangements that facilitate access at high volumes.[13]

Although it seems that systematic access is growing, we also found cases where proposals for expanded access had been rejected – at least temporarily. In Germany, in 2011, the federal government abandoned the proposed ELENA project, which was intended to streamline the collection of a wide variety of employee data into a central databank run by a government agency, containing name, date of birth, insurance number, home address, time missing work, and "possible misbehavior."[14] In Canada earlier this year the government abandoned Bill C-30, which would have imposed various intercept capability and reporting requirements on communications service providers,[15] while the junior partner in Britain's governing coalition blocked the proposed Communications Data Act, which had stirred public and service provider opposition.[16] In the EU, a directive obliging airlines to pass personal details of EU passengers to the authorities of the EU member states, initially proposed in 2011, remained on hold as of October 2013.[17]

When we began this study, we intended to focus primarily on access to stored data held by businesses, as distinct from real-time interception of communications, however, there have also been recent disclosures about systematic access to data in real-time. Materials released by Edward Snowden regarding collection activities of the US

[13] For example, it has been reported that one mobile operator in the US established an online interface to allow law enforcement agencies to "ping" cell phones for location data. Kim Zetter, 'Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year,' *Wired* (Dec. 1, 2009). The Department of Justice Inspector General reported several years ago that major telephone companies had placed their employees, with access to phone company databases, inside FBI offices in order to respond more quickly to FBI requests for metadata records. See Stephanie K. Pell, 'Systematic Government Access to Private-Sector Data in the United States', (2012) 2/4 International Data Privacy Law 245, http://idpl.oxfordjournals.org/content/2/4/245.full. More recently, The New York Times reported that AT&T was placing its employees "in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987." See Scott Shane and Colin Moynihan, 'Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s,' *NY Times* (Sept. 1, 2013) http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html?_r=0.

[14] Schwartz, n. 6 above.

[15] See Laura Payton, 'Government Killing Online Surveillance Bill," *CBC News* (Feb. 11, 2013) http://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384.

[16] See Kitty Donaldson, 'Clegg Kills U.K. Communications Data Bill after Liberty Concerns,' Bloomberg *Businessweek* (April 25, 2013) http://www.businessweek.com/news/2013-04-25/clegg-kills-u-dot-k-dot-communications-data-bill-after-liberty-concerns.

[17] See Honor Mahony, 'MEPs Vote Down Air Passenger Data Scheme,' *EUobserver.com* (April 24, 2013).

government referred to "upstream" collection, which apparently involves tapping directly into fiber cables or other major pipelines to copy or filter all communications as they pass through.[18] A recent study for the European Parliament, picking up on the term, concluded that the practice of "upstreaming" appears to be a relatively widespread feature of surveillance by several EU member states.[19] Just as most governments have long asserted the power to demand access to stored data held by businesses about their customers, so too have they asserted the power to intercept in real-time communications passing over networks of telecommunications service providers. Sometimes such interception is conducted with the cooperation of the service provider, sometimes without. The rules and practices surrounding real-time collection can be very complex, but in certain circumstances the electronic surveillance activities of governments have long entailed large scale or systematic collection of communications for later analysis, especially for national security purposes and especially when conducted outside, or targeted at persons outside, the intercepting nation's territory. As we discuss later, recent revelations in the press suggest that the digital revolution has been accompanied by a growth in large-scale, real-time interception. In addition, it appears that there is a growing overlap between access to stored data and real-time interception. It has been reported that the US intercepts huge volumes of stored data in real-time as it is shifted globally from server to server.[20]

Systematic access as we define it also relates to concerns over data retention and design mandates. Data retention refers to legal requirements that certain service providers collect and retain specific categories of information about the users and usages of their systems for a specified period of time (often ranging from six months to two years), so that the data is available to the government upon demand. Most recently, debates over data retention have focused on government proposals that telecommunications service providers (both traditional telephone and wireless operators and Internet Service Providers (ISPs)) maintain subscriber identifying information or connection data, such as

[18] See Charlie Savage, 'N.S.A. Said to Search Content of Messages to and From U.S.,' *NY Times* (Aug. 8, 2013) http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all&_r=2&.

[19] European Parliament Study, 'National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law' (Oct. 2013) http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf.

[20] Barton Gellman and Ashkan Soltani, 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Show,' *Washington Post* (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

customer billing information and dialed number information, for a set period of time.[21] Design mandates include requirements that service providers design their systems to be "wiretap ready," that is, to be capable of facilitating real-time or near real-time interception upon request.[22]

Our research into actual practices, although hampered by a lack of transparency, confirmed that governments are in fact increasingly turning to the private sector for information that they see as critical in countering criminal activity, terrorism, and other threats. Recent disclosures dramatically reinforce this conclusion, augmenting it with new information regarding extraordinary programs of systematic collection in real-time.

"Governments are increasingly turning to the private sector for information that they see as critical in countering criminal activity, terrorism, and other threats"

The reasons for these trends are simple enough. To begin with, private sector firms hold an increasingly large amount of data about individuals collected in the course of ordinary commercial transactions or created by users and stored on cloud platforms, supplemented in some countries by data retention mandates. The volume of digital data routinely generated, collected, and stored about individuals' purchases, communications, relationships, movements, finances, and tastes is staggering. At least three developments have fed the growing government appetite for this information. First are concerns about new and dangerous threats to national security, demonstrated by terrorist attacks in New York, Washington, Madrid, London, Mumbai, Boston, and elsewhere, and compounded by the rise in militant Islamic fundamentalism. Second are a range of other criminal threats, including organized crimes, as well as more mundane interests in tax collection and other regulatory or administrative goals. The third major factor is the steadily growing ability of businesses and governments to analyze large data sets in search of useful insights, a development often summed up with the phrase "big data."[23]

---

[21] Center for Democracy and Technology, 'Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development' (October 2011) https://www.cdt.org/files/pdfs/CDT_Data_Retention_Long_Paper.pdf.

[22] In the US, see Communications Assistance for Law Enforcement Act (CALEA), Pub L No 103-404, 108 Stat 4279, 4280–81, codified at 47 USC § 1002 (2000); in the UK, see Regulation of Investigatory Powers Act 2000 (RIPA), section 5; see also Andrei Solatov, 'Lawful Interception: The Russian Approach,' Privacy International (Mar. 5, 2013) available at https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach (describing "SORM," Russia's nationwide system of automated and remote legal interception).

[23] See Fred H. Cate, James X. Dempsey, and Ira S. Rubinstein, 'Systematic Government Access to Private-Sector Data' (2012) 2 International Data Privacy Law 195, http://idpl.oxfordjournals.org/content/2/4/195.full.

Other commentators have observed that governments in the post-9/11 era are increasingly dependent on the private sector to assist them in collecting and analyzing data for national security purposes and have applied various theories in analyzing these modes of cooperation.[24] This project's focus on systematic access was, until recently, somewhat unique.[25] So too was its effort to explore the issue not only from the perspective of the governments' needs or the countervailing civil liberties and human rights values, but also from the perspective of companies that are responding to governmental demands in numerous countries and are, therefore, caught in the middle between competing interests.[26]

"In most if not all countries, existing legal structures provide an inadequate foundation for the conduct of systematic access"

In the latest phase of this project, summarized here, we focused on the legal and human rights issues posed by the apparent trend towards systematic access. Part II of this report briefly describes the recent flurry of disclosures regarding mass collection of communications and associated data by the US, UK and other governments. Part III considers the common themes emerging from an analysis of the law and practice of systematic access in the thirteen countries we surveyed. Part IV lays out a descriptive framework that can be used to analyze national laws that set standards for governmental access to privately held data, while Part V lays out a normative framework, based on human rights principles, and offers some comparative observations. Finally, Part VI offers preliminary recommendations and next steps in responding to the challenges of systematic government access to private sector data.

Our basic conclusion: In most if not all countries, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level.

---

[24] See, e.g., Michael D. Birnhack & Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Virginia Journal of Law & Technology 6; Jack M. Balkin, 'The Constitution in the National Surveillance State' (2008) 93 Minnesota Law Review 1; Jon D Michaels, 'Deputizing Homeland Security' (2010) 88 Texas Law Review 1435; Jon D. Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror' (2008) 96 Cal. Law Review 901.

[25] For an earlier study of the issue, focused on Australia, see Nigel Waters, 'Government Surveillance in Australia' (Aug. 2006) http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf.

[26] See Albert Gidari, Keynote Address at the University of San Francisco Law Review Symposium, 'Companies Caught in the Middle: Legal Responses to Government Requests for Customer Information' (Oct. 28, 2006).

II. New Revelations of Systematic Surveillance Activities

On June 5, 2013, *The Guardian* began publishing information regarding surveillance activities of the US National Security Agency (NSA), based upon the leaking of classified documents by former contract employee Edward Snowden. Further disclosures by *The Guardian* and other major news outlets followed, along with official US government releases of previously classified documents in response to FOIA litigation and public demands for transparency.

One of the surveillance programs described in these disclosures involves systematic access of exactly the kind this project has been concerned with: the ongoing, bulk collection by the NSA of metadata on a large percentage of telephone calls to, from and within the US. Under court orders issued by the Foreign Intelligence Surveillance Court (FISC), major telecommunications companies are required to disclose to the NSA call detail records on all calls by all of their customers.[27] The data at issue includes communications routing information, including originating and terminating telephone number and time and duration of call. It does not include the substantive content of any communication and the orders compelling disclosure expressly state that they do not authorize the production of cell site location information.[28]

The program covers calls to, from and within the US. The companies are required to deliver the records to the government on a daily basis. In its current form, the program has been ongoing for seven years.[29] The court orders compelling service provider compliance run for 90 days and have been renewed regularly. All data obtained through the program may be retained by the NSA for five years and may be queried by NSA analysts without prior court approval.[30] The program draws no distinction between US

[27] Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily,' *The Guardian*, (June 5, 2013) http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also*, FISC, *Order* (May 24, 2006) available at http://www.dni.gov/files/documents/section/pub_May 24 2006 Order from FISC.pdf.

[28] Foreign Intelligence Surveillance Court, *Primary Order* (July 19, 2013), available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf. See also Office of the Director of National Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013), available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information ("DNI June 2013 Statement").

[29] Parmy Olsen, 'Senators: NSA Cellphone Spying Has Gone On 'For Years',' *Forbes* (June 6, 2013) http://www.forbes.com/sites/parmyolson/2013/06/06/u-s-senators-nsa-cellphone-spying-has-gone-on-for-years/. The initial order was issued in May 2006: FISC, *Order* (May 24, 2006) available at http://www.dni.gov/files/documents/section/pub_May 24 2006 Order from FISC.pdf.

[30] *DNI June 2013 Statement*, n. 28 above. See also Foreign Intelligence Surveillance Court, *Amended Memorandum Opinion (Eagan, J.)* (August 29, 2013) at p. 5, available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

citizens and non-US citizens; the vast majority of people whose records are disclosed to the NSA under the telephony metadata program are US citizens, although persons outside the US making calls to or receiving calls from the US are also caught up in the dragnet.

The program operates under Section 215 of the USA PATRIOT Act, which authorizes the government to make an application to the FISC for an order requiring the production of "any tangible things (including books, records, papers, documents, and other items)" so long as "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[31] In interpreting "relevance," the government contends that if there is a relevant needle in a haystack of data, the entire haystack may be subject to collection under Section 215,[32] even though, as the government itself admits, the vast majority of the data is not relevant.[33] Orders from the FISC have agreed with the government's broad interpretation of the term "relevant."[34]

It has also been revealed that the NSA conducted for many years a program of systematic collection of Internet metadata. That program was discontinued in 2011 due to an assessment by NSA that it was ineffective as a counterterrorism tool. [35]

Snowden also disclosed documents describing activities of the US government, conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA), as adopted by the FISA Amendments Act of 2008 (FAA), involving the collection of the *contents* of communications.[36] Section 702 authorizes the collection from service

---

[31] 50 U.S.C. § 1861.

[32] *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act Reauthorization* (August 9, 2013), available at https://www.eff.org/sites/default/files/filenode/section215.pdf.

[33] See Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, Department of Justice, to Rep. James Sensenbrenner (July 16, 2013), available at http://sensenbrenner.house.gov/uploadedfiles/ag_holder_response_to_congressman_sensenbrenner_on_fisa.pdf ("[M]ost of the records in the dataset are not associated with terrorist activity.").

[34] In August 2013, after the Snowden leaks, a judge of the FISC wrote the first detailed opinion explaining the legal basis for the program; that opinion was made public in September 2013. *See* Foreign Intelligence Surveillance Court, *Amended Memorandum Opinion (Eagan, J.)* (August 29, 2013), available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[35] See, Siobhan Gorman and Jennifer Valentino-Devries, 'Details Emerge on NSA's Now-Ended Internet Program,' *Wall St. Jnl.reet Journal,* (June 27, 2013), http://online.wsj.com/article/SB10001424127887323689204578572063855498882.html.

[36] Barton Gellman and Laura Poitras, 'U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program,' *Washington Post* (June 6, 2013) http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-

providers inside the US of foreign intelligence about persons reasonably believed to be outside the US. Initial news reports about a program referred to as "PRISM" relied heavily on one slide in a government PowerPoint presentation saying that the government was collecting "directly from the servers" of leading communications service providers.[37] The government and the companies involved have denied that there is any direct access to service provider computers,[38] and other than that one slide there has been no evidence of direct access to the servers of US-based companies providing online services.

However, another program conducted under Section 702 has some elements of systematic access, in real-time. According to *The New York Times*, one way that the NSA acquires communications is by "systematically searching—without warrants—through the contents of Americans' communications that cross the border …. temporarily copying and then sifting through the contents of what is apparently most [international] e-mails and other text-based communications."[39]

Snowden also leaked documents disclosing systematic surveillance programs in the UK, including one called "Mastering the Internet" and another called "Global Telecoms Exploitation." According to *The Guardian*, Britain's "GCHQ [the UK's signals intelligence agency] has secretly gained access to the network of cables that carry the world's phone calls and Internet traffic and has started to process vast streams of sensitive personal information."[40] In an operation code named Tempora, GCHQ stores large volumes of data drawn from fiber optic cables for up to 30 days so that it can be sifted and

---

companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. See 'NSA Slides Explain the PRISM Data-Collection Program,' *Washington Post* (June 6, 2013) http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[37] The slide is available at http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[38] See blog posts of Facebook founder and CEO Mark Zuckerberg (June 7, 2013) https://www.facebook.com/zuck/posts/10100828955847631 and of Google's CEO Larry Page and Chief Legal Officer David Drummond (June 7, 2013) http://googleblog.blogspot.co.uk/2013/06/what.html. See also Declan McCullagh, 'No Evidence of NSA's 'Direct Access' to Tech Companies,' *CNet* (June 7, 2013) http://news.cnet.com/8301-13578_3-57588337-38/no-evidence-of-nsas-direct-access-to-tech-companies/.

[39] Charlie Savage, 'N.S.A. Said to Search Content of Messages to and From U.S.,' *NY Times* (August 8, 2013) http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all&_r=2&. This program appears to involve real-time interception, as opposed to access to stored data.

[40] Ewen MacAskill, 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications,' *The Guardian* (June 21 2013) http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

analyzed.[41] According to *The Guardian*, GCHQ is able to "survey about 1,500 of the 1,600 or so high-capacity cables in and out of the UK at any one time" and was capable of extracting and collecting information (both content and metadata) from 200 of those cables at a time.[42] According to *The Guardian*, citing official documents, as of 2011 GCHQ recorded 39 billion separate pieces of information during a single day. According to another document cited by *The Guardian*, GCHQ "produces larger amounts of metadata collection than the NSA." The tapping operations within the UK were done under agreements with the commercial companies that own the fiber optic cables.

The UK programs are presumably conducted under the Regulation of Investigatory Powers Act (RIPA), enacted in 2000. Under RIPA, a Secretary of State (the Home Secretary or the Foreign Secretary) issues interception warrants in criminal and intelligence cases, not judges. Normally such warrants must be specifically targeted, however, the particularity requirement does not apply to surveillance consisting of the interception of "external communications," defined as those "sent or received outside the British Islands." The Secretary of State may issue non-particularized warrants for one of three purposes delineated in Section 5(3): "in the interests of national security," "for the purpose of preventing or detecting serious crime," or "for the purpose of safeguarding the economic well-being of the United Kingdom." Such warrants remain subject to the provision of RIPA requiring the Secretary of State to believe that "the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct."[43]

The controversy surrounding the Snowden leaks prompted journalists and activists to write about similar programs in a number of countries. Press reports have revealed the following:

- Germany's foreign intelligence agency, the BND, is monitoring communications at a Frankfurt communications hub that handles international traffic to, from, and through Germany, presumably using the strategic monitoring authority described by Paul Schwartz in his paper published last year, and the BND is seeking to significantly extend its capabilities.[44]

---

[41] Ewen MacAskill, 'Mastering the Internet: How GCHQ Set Out to Spy on the World Wide Web,' *The Guardian* (June 21, 2013) http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

[42] Ewen MacAskill, 'How Does GCHQ's Internet Surveillance Work,' *The Guardian* (June 21, 2013) http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

[43] This description of RIPA is drawn from Aidan Booth, 'GCHQ Surveillance: TEMPORA Program' (July 11, 2013) http://johnjayresearch.org/ccs/2013/07/11/gchq-surveillance-tempora-program/.

[44] Staff, 'The German Prism: Berlin Wants to Spy Too,' *Spiegel Online* (June 17, 2013) http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html; 'German Intelligence Admits to Frankfurt E-Mail Tap,' *Wall St. Jnl*. (Oct. 9, 2013)

- France runs a vast electronic spying operation using NSA-style methods, reportedly with even fewer legal controls.[45]

III. Common Themes from the Country Reports

Caution should be exercised in extrapolating from our survey of 13 countries. Among other limitations, our survey included not a single country in Africa. Moreover, by being heavily weighted to democracies, it may suggest more commonality of legal norms than would be found in a broader survey. With those significant caveats, our country reports analyzing the law and practice of systematic access identified a number of common themes about the countries examined:[46]

- **Lack of Transparency:** Even after the Snowden leaks, systematic access is difficult to assess.

    - The relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified.
    - Practices are often opaque; it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment.
    - Oversight and reporting mechanisms are either absent or limited in scope when they exist, and generally do not reach voluntary data sharing.

    In the US, the Snowden revelations have altered this imbalance in a profound way by publicizing the legal and technical details of several highly classified surveillance programs. The same is true to a lesser extent in the UK, although the Snowden leaks revealed little about the legal basis for the UK programs that have been disclosed. The Snowden leaks have also led to some further revelations about surveillance programs in other countries.

---

http://blogs.wsj.com/digits/2013/10/09/german-intelligence-admits-to-frankfurt-e-mail-tap/ ("the German weekly Der Spiegel reported in this week's issue that the German intelligence service … has been tapping the giant De-Cix exchange point in order to spy on foreign targets for at least two years").

[45] Jacques Follorou and Franck Johannès, 'Révélations sur le Big Brother français,' *Le Monde* (July 4, 2013) http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html; Angelique Chrisafis, 'France 'Runs Vast Electronic Spying Operation Using NSA-Style Methods',' *The Guardian* (July 4, 2013) http://www.guardian.co.uk/world/2013/jul/04/france-electronic-spying-operation-nsa.

[46] See Cate, Dempsey, and Rubinstein, n. 23 above, at 197-99.

But leaking is by its nature episodic and incomplete; even the most extensive leaks of classified documents can be misleading and are no substitute for structural and ongoing transparency mechanisms rooted in constitutional, legal, and political norms, and supporting vigorous democratic oversight and debate. Outside the US and the UK, the picture remains very murky, although it is clear that systematic access occurs in many countries.[47]

The shock expressed not only by civil society, but also by government officials at the scope of systematic access as revealed by the Snowden leaks demonstrates how deeply these programs and legal interpretations were hidden from public scrutiny and democratic debate.[48] In the US at least, the revelations accelerated an already growing corporate movement to demand greater legal authority to disclose at least the numerical scope of government demands and companies have also started taking steps to make surveillance without their consent more difficult.[49]

- **Significant Commonality Across Laws:** While differences abound, and can be significant, there is some commonality across most of the countries we surveyed.
    - Almost all have privatized their telecoms and thus recognize some arm's length relationship between the government and the network operators.
    - Almost all recognize the right to privacy.
    - Most of the countries surveyed either exempt data collection for law enforcement and national security purposes from general data protection laws or treat government access as a permissible use, subject to separate, varying restrictions.

[47] European Parliament Study, 'National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law' (Oct. 2013) http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf.

[48] Justin Sink, 'Patriot Act Author "Extremely Troubled" by NSA Phone Tracking,' *The Hill* (June 6, 2013) http://thehill.com/blogs/hillicon-valley/technology/303937-patriot-act-author-extremely-troubled-by-nsa-phone-tracking; Letter from Congressman F. James Sensenbrenner to Attorney General Eric H. Holder, Jr. (June 6, 2013) http://www.scribd.com/doc/146169288/Sensenbrenner-Letter-to-Attorney-General-Eric-Holder-RE-NSA-and-Verizon.

[49] Claire Cain Miller, 'Angry Over U.S. Surveillance, Tech Giants Bolster Defenses,' *NY Times* (Oct. 31, 2013) http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html?_r=0.

- Most countries impose a variety of limits and controls on government access and surveillance requests, whether by courts, senior government officials, or committees or oversight bodies established for this purpose.

A major question, of course, is whether those control and review mechanisms are strong enough in the face of technological changes and more aggressive government demands.

With the exception of mandatory reporting laws, the applicable laws and regulations in the countries surveyed generally focus on defining standards for requests for data regarding specific persons, and they seem to presume a world of limited and particularized access rather than systematic government access. The UK's RIPA and Germany's G-10 law specifically authorize non-particularized interception of communications to or from persons abroad. The NSA revelations show how one of these laws (Section 215) has been interpreted in secret to authorize bulk, ongoing disclosures.

China and India stand out due to almost total lack of protection and oversight in both law enforcement and national security. At the opposite extreme, Japan and Brazil are notable for the severe limits they impose on interceptions undertaken for foreign intelligence security purposes.

- **Inconsistency Between Published Law and Practice:** In many countries, the published law appears to say something different from what governments are reportedly doing. Even after the Snowden leaks, we lack an accurate or

"In many countries, the published law appears to say something different from what governments are reportedly doing"

comprehensive understanding of systematic access because both its legal basis and actual practice are hidden from public view.

As the disclosures about the US government's telephony metadata program show, governments may be operating under secret interpretations of the applicable laws. In other cases, they may be operating in the interstices of national regulation, obtaining access that is not specifically authorized but also not specifically prohibited. In the US and in other democracies (especially Israel), the inconsistencies between publicly available laws and reported practice suggest areas of struggle or tension between legal requirements and perceived national security necessities. In light of these

responsibilities to protect the nation against external and internal threats, the executive branch does not so much ignore existing law as rely on executive orders, secret court opinions, and other non-transparent means to interpret the law in the pursuit of the executive branch's objectives.[50] Additionally, after 9/11, several countries, notably Canada, Germany, the US, and the UK, modified their anti-terrorist statutes, thereby granting intelligence agencies more expansive surveillance powers.

Again, China and India are different. The former explicitly carves out broad exceptions for national security from both the constitution and relevant security and surveillance laws, whereas privacy protections under Indian law are weak, ambiguous, or non-existent.

- **Different Standards for National Security and Law Enforcement:** In every country we studied, even those nations with otherwise comprehensive data protection laws, regulatory, law enforcement, and national security access are often excluded from such laws, or treated as accepted purposes for which such access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses.[51] Moreover, almost everywhere, national security access is more sparingly regulated for data protection purposes than requests for law enforcement purposes.

- **The Declining "Wall" Between National Security and Other Uses:** Prior to the terrorist attacks of 9/11, many of the countries we studied maintained a "wall" that prevented law enforcement and other government agencies from obtaining and using data collected by intelligence or national security agencies under relaxed data protection standards. In many countries, this wall has been dismantled, with the result that intelligence agencies may now, at least as a matter of legal authority, pass information to law enforcement officials, while data collected for law enforcement and other purposes may be shared with intelligence agencies. This is certainly the case in the US post-9/11,[52] in Canada, where anti-terrorism policy explicitly calls out the importance of information sharing among law enforcement and intelligence

[50] One of the documents leaked by Snowden indicates that, starting in 2004, the Executive Branch in the US began to seek and obtain court approval for its bulk collection programs, bringing them under statutory authority, but based entirely on secret interpretations of those statutes. See 'Draft NSA Inspector General Report on Email and Internet Data Collection,' dated 24 March 2009, *The Guardian*, (June 27, 2013) http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

[51] Adequate standards based on human rights instruments are discussed below in Part V.

[52] See Pell, n. 13 above at 245-46.

agencies,[53] and in Germany, where recent laws have eroded the wall somewhat, thereby permitting the creation of an "anti-terrorist database."[54]

- **Systematic Volunteerism:** In some of the countries studied, the government obtains systematic access to private sector information through voluntary arrangements. 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."[55] An additional motivating factor for bulk disclosure may be efficiency (easing the administrative burden of processing many individualized requests).

- **Importance of Trans-Border Access and Sharing:** Although most of the countries appear to consider multinational access and sharing essential to national security and law enforcement activities, these arrangements received relatively little attention in the papers we commissioned. Overall, it seems there has been relatively little discussion of the complex legal and political issues associated with asserting jurisdiction over data stored in other countries or relating to citizens of other countries. This reflects, of course, the continuing difficulty of jurisdictional issues across a wide spectrum of areas in the globalized information society. Also, until the recent disclosures, there seems to have been little discussion of the complex questions regarding extraterritorial application of human rights raised by trans-border surveillance.[56] Most countries, even those that have recognized privacy as a universal right, seem to apply much lower protections (if any) to

[53] See Jane Bailey, Systematic government access to private-sector data in Canada,' (2012) 2/4 International Data Privacy Law 207, 213, http://idpl.oxfordjournals.org/content/2/4/207.full.

[54] See Schwartz, n.6 above at 296-97.

[55] See Cate, Dempsey, and Rubinstein, n. 23 above at 199. In the US, it seems that concerns about liability discourage voluntary cooperation.

[56] One highly prescient exception was the April 2013 report of Frank La Rue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression, who expressed "serious concern with regard to the extraterritorial commission of human rights violations and the inability of individuals to know they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance or seek remedies." *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue, to the Human Rights Council*, at 64 (April 17, 2013), *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

surveillance directed at foreigners.

The Snowden leaks have drawn major attention to the fact that, with the emergence of globalized services, access in one country can easily affect large numbers of people outside that country. Separately, even before the Snowden leaks, several authors duly noted the existence of the UK-USA agreement (which also extends to Australia, Canada and New Zealand) to share information obtained by electronic surveillance. Recent leaks have exposed further details about this and other sharing and cooperation agreements.[57]

IV. Comparative Analysis: The Descriptive Framework

This paper now presents a more detailed comparative analysis, proposing a set of descriptive and normative frameworks that might help governments, the private sector, privacy advocates, and other stakeholders confront the issues associated with government access to privately held data in general, and the issue of systematic access in particular. We approach this assessment with considerable humility. Comparative legal analysis is always difficult without an in-depth knowledge of the systems at issue, and in the context of government access the task is made more difficulty by the ambiguity in laws and lack of transparency in practices that we have repeatedly mentioned. Nevertheless, in the spirit of beginning a more nuanced international dialogue around standards for government access, we offer some comparative observations.

We first offer a descriptive framework for government access laws. Using this framework, we have attempted to summarize the laws of the thirteen countries previously surveyed. We prepared two charts, attached as appendices to this report and published online at govaccess.cdt.info. One chart summarizes the basic laws and practices relevant to government surveillance and access, and the other summarizes laws and practices relevant to government access to specific kinds of business records. In Part IV.B, we offer some comparative observations. We caution that our charts and analysis suffer from the limitations of any effort to summarize a great deal of complex information.

[57] See Peter Beaumont, 'NSA Leaks: US and Britain Team Up on Mass Surveillance,' *The Guardian* (June 22, 2013) http://www.theguardian.com/world/2013/jun/22/nsa-leaks-britain-us-surveillance; Linton Besser, 'Telstra Storing Data on Behalf of US Government,' *Sydney Morning Herald* (July 16, 2013) http://www.smh.com.au/it-pro/security-it/telstra-storing-data-on-behalf-of-us-government-20130716-hv0w4.html; Glenn Greenwald, Laura Poitras and Ewen MacAskill, 'NSA Shares Raw Intelligence Including Americans' Data with Israel,' *The Guardian* (Sept. 11, 2013) http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

In Part V, we offer a normative framework, drawing on widely-accepted understandings of "the rule of law" and on the case law of the European Court of Human Rights, which represents the most comprehensive trans-national body of law on government surveillance. In an effort to map how the laws of the thirteen countries surveyed measure up against this normative framework, we prepared two additional charts, one addressing standards for access to communications and associated traffic data in law enforcement investigations, and one analyzing laws on national security surveillance against the same framework. The charts are published in the appendix and online at govaccess.cdt.info. In Section V.B, we offer comparative observations on the normative framework.

A. The Descriptive Framework

In researching governmental access rules and practices, we found that most legal systems had addressed the question of government access to communications and metadata associated with communications, and to business records of various types. The laws relating to access to communications and communications metadata seem to have grown out of an almost universal recognition of two competing propositions: that communications privacy is an essential right, and that the ability to intercept communications in real-time or to access communications and associated data in storage is an important investigative technique for both criminal investigations and the protection of national security interests. Accordingly, most countries seem to have laws addressing communications privacy and governmental access to communications. Whether those laws have kept pace with technological development is another question. However, we found that certain basic issues presented themselves time and again across different legal systems. For example, are there separate rules for law enforcement and national security access? Is judicial or senior level executive approval required for access? Are companies subject to data retention or network design mandates?

"Most countries seem to have laws addressing communications privacy and governmental access to communications. Whether laws have kept pace with technological development is another question."

As a framework for cross-border comparisons of government laws regulating access to communications and associated metadata, we identified nine of these recurring factors:

TABLE 1: THE DESCRIPTIVE FRAMEWORK

1. Source of authority, standards and limits
a. Constitutional – Does the national constitution include a protection of privacy or other limits on governmental power to obtain communications or other customer data from private sector entities?
b. Statutory – Are standards for governmental access established in statute?
c. Law enforcement vs. national security – Does the legal system set separate rules for law enforcement access as compared to national security access?
2. Distinction between content and non-content – Does the legal framework draw a distinction between the content of communications and transactional data (addressing or routing data, subscriber identifying data, financial data, data about commercial transactions)?
3. Technology neutrality (same standards for different media) – Do legal standards apply consistently to data collected online and offline? To data in transit and data in storage?
4. Targeted vs. bulk access – Does the legal framework (outside of the regulatory context) expressly draw a distinction between targeted collection and systematic or bulk collection? Is there express authorization for bulk collection?
5. Third party doctrine – Does the legal system treat data stored with a third party (for example, a cloud provider) differently from data stored locally?
6. Use, retention, disclosure limits – Does the law impose limits on the government's use, retention, and disclosure of data after the data are lawfully acquired?
7. Oversight mechanisms – What are the executive, judicial, legislative oversight, public transparency, and redress mechanisms?
8. Design mandates – Does the law require service providers to design their networks or activities to facilitate government access? Does the government regulate encryption?
9. Retention mandate – Does the law require entities to store certain data about customers for specified periods of time?

Chart 1, in the appendix and online, applies this descriptive framework to the communications surveillance laws of the 13 countries surveyed.

Of course, as we noted earlier, government demands for access to data, including for systematic access, are directed at many other sectors, particularly financial services and travel. Accordingly, we sought to analyze laws and practices in the thirteen countries surveyed in terms of standards for government access to other types of business records. This task proved much more difficult, because in many countries, even those with otherwise comprehensive privacy laws, rules on government access to data and on systematic reporting may differ sector by sector. Chart 2, in the appendix and online, attempts to summarize laws and practices considering the following factors:

TABLE 2: GOVERNMENT ACCESS TO BUSINESS RECORDS

1. Different rules for different sensitivity of data
a. Location
b. Travel
c. Financial
d. Other
2. Systematic disclosure demands
3. Use, retention, disclosure limits
4. Oversight mechanisms
5. Redress/due process mechanisms
6. Transparency
7. Automatic disclosure mandates
8. Retention mandate

B. The Descriptive Analysis: Comparative Observations

The following section highlights the similarities and differences in the government access rules in the thirteen countries studied. The discussion touches on both standards for real-time access and standards for access to stored data. It focuses mostly on communications content and metadata, in part because of the recent intensive governmental, public, civil society, and media focus on these matters, rather than on other forms of business records, where the issues are also important and inherently transnational.

1. Source of authority, standards and limits:

a) **Constitutional authority:** The majority of countries surveyed recognize the right to privacy in their national constitutions, with the exception of Australia and the UK. Both the US (Pell, n. 13 above at 247) and Canada (Bailey, n. 53 at 208) apply a "reasonable expectation of privacy" test to define the scope of that right vis-à-vis the government. In Germany and Israel, the constitutional basis of information privacy is especially strong. Germany recognizes a constitutionally based "right of informational self-determination" and a highly engaged German public and press ensure that such rights are taken very seriously (Schwartz, n. 6 at 289). In Germany, for example, intrusions on privacy require a valid basis in law and must satisfy a principle of proportionality (Schwartz, id. at 290). Similarly, privacy in Israel is a constitutional right subject to a "limitation clause,"[58] with the result that government access must be expressly authorized and pass constitutional muster, including a proportionality test.

"The application of constitutional standards is by no means an absolute bar against government access to private sector data"

However, in all of the countries studied, the application of constitutional standards is by no means an absolute bar against government access to private sector data. To the contrary, governments enjoy substantial powers to collect or intercept data, under a variety of laws and programs. In the US, a major exception to the right to privacy is the third-party doctrine, which leaves business records outside the Constitution's protection. In Germany and Israel, access laws have been upheld even after the courts applied balancing tests that heavily weigh the fundamental right to privacy. As previously noted, art. 8 of the European Convention tolerates secret surveillance in signatory states (Germany, the UK, France, and Italy) provided that national laws provide adequate safeguards against potential abuse. In Brazil, however, at least one judicial decision suggests that article 5, item XII of the Constitution (secrecy of correspondence, telegraphic data, and telephone communications) protects the flow of data "even against judicially authorized wiretapping" (Magrani n. 8).

In sharp contrast, China stands out among the thirteen countries we surveyed in two fundamental respects. First, it is the only non-democratic country. Second, its constitution (and laws) grant extensive surveillance powers to the state for purposes

[58] See Omer Tene, 'Systematic Government Access to Private-Sector Data in Israel', (2012) 2/4 International Data Privacy Law 278, http://idpl.oxfordjournals.org/content/2/4/277.full.

of national and public security. Thus, the government has extensive authorities and "generous room for flexibility" in accessing private data in the name of maintaining state security and the social order (Wang, n. 7 at 221).[59] In India too, although India is a democracy, the constitution imposes few meaningful limits on the government's broad surveillance powers (Abraham and Hickok n. 9).

b) **Statutory authority:** Australia, Canada, Israel, Japan, South Korea and all of the European counties have comprehensive privacy statutes. The US has no omnibus privacy law, but rather follows a sector-specific approach, with separate laws protecting communications data, financial data, health data, and other categories.

However, in all the countries surveyed, whether the nation has a comprehensive privacy statute or sectoral laws, those statutes have exceptions permitting government surveillance of communications and government access to stored records. Real-time surveillance is addressed in the majority of countries (other than China and India) in surveillance laws whose principles and concepts generally fit within the descriptive and normative frameworks outlined above.

Against this commonality of approach, China and India stand out among the 13 countries surveyed. In China, it is very easy to override existing statutory restrictions on national security or public order grounds. Thus, Chinese law explicitly authorizes governmental access to privately held data and/or lacks explicit limitations on such access. Indeed, Chinese national security law allows for the inspection of electronic communication instruments belonging to "any organization or individual" for purposes of state security with few if any limitations (Wang, n. 7 at 222).[60]

Indian surveillance laws also have very limited or very weak restrictions on government access. Although a 1997 decision established certain safeguards under India's longstanding Telegraph Act of 1885 governing telephone interception, the Information Technology Act of 2008 substantially weakened existing standards. It permits interception of electronic communications to prevent "incitement" of any cognizable offense related to public emergency, public safety, and public order, or for investigation of any offense as well as for a range of cyber security purposes (Abraham and Hickok, n. 9 at 307). Under the relevant rules, intermediaries must provide a high degree of assistance to law enforcement; agencies can freely share data; and the rules relating to the collection of traffic data also permit extensive monitoring for cyber security matters (id. at 308). India's ISP licensing system also

[59] Chinese government access to private sector data is further strengthened by the Chinese Communist Party's "absolute control over the law" and the absence of an independent judiciary. Wang n. 7 above at 220.

[60] Although security officials must follow their own internal procedures, these procedures are largely secret and give rise to no due process rights; id.

permits extremely broad government access rights while neglecting well-established international safeguards, such as requiring a court order, internal agency restrictions on access to intercepted materials, and individual redress (id. at 309).

Among the countries we studied, Israel faces unique national security concerns.[61] Both the courts and the Attorney General (which in Israel is a non-political and highly autonomous function) play a key role in interpreting a set of laws that deal with surveillance by both the police and by the various intelligence services (military intelligence, internal security (GSS), and foreign intelligence (Mossad)). The Israeli intelligence services enjoy far more leeway than the police in conducting surveillance. For example, the Wiretap Act allows military intelligence and GSS to obtain wiretap permission from a very senior official without judicial oversight (Tene, n. 58 at 281). The Communications Data Act regulates access to traffic data by the police under multiple tracks, some of which require judicial oversight and some of which do not. In contrast, GSS (which is regulated by a separate law) has much broader access without judicial scrutiny. This includes a requirement that fixed line and cell operators must transfer to GSS certain categories of communications data as determined by the Prime Minister (id. at 285-86).[62] Although concerns about law enforcement access have sometimes spawned government inquires and public outcry, the press and the public seem more acquiescent with regard to access for internal security purposes (id. at 282). On the other hand, the law regulating GSS imposes certain accountability and transparency requirements (id. at 286).

c) **Law enforcement vs. national security:** The majority of countries have enacted separate laws or separate procedures addressing access in the domestic law enforcement context as opposed to national security (or foreign intelligence) activity. In the UK and other countries, the rules for both arenas are set out in a single law (Brown n. 10 at 232), whereas the US applies quite different standards in the two arenas through separate statutes – the Wiretap Act and the Electronic Communications Privacy Act (ECPA) for law enforcement and FISA for foreign intelligence (Pell, n. 13 at 248-49). In India, there is no clear distinction between law enforcement and national security access (Abraham and Hickok, n. 9 at 314), while China distinguishes them, but imposes few if any restrictions on the latter (Wang, n.

[61] We agree with Tene (n. 58 at 277-78) who notes that this account must be qualified by two distinctions: first, it concerns only "Israel proper" and not the occupied territories, which are subject to a military regime; second, Israel has been in a near constant state of war or armed conflict since its beginnings as an independent state, and therefore national security considerations "have a profound impact on Israeli constitutional and legal discourse."

[62] These transfers to the GSS are subject to certain "secret annexes" setting out detailed procedures and protocols. After examining the secret annexes *in camera,* a court denied a public records request seeking their release on the grounds that they "do not provide the GSS with surveillance powers, but rather set forth technical specifications for operating the 'pipe' through which the data are channeled strictly where access to data is authorized by law" (Tene n. 58 at 288).

7 at 222). Although Australia,[63] Canada (Bailey, n. 53 at 212-13), and the US (Pell, n. 13 at 248) apply special, arguably more lenient rules to national security access, these rules remain subject to constitutional limitations.

At the opposite extreme is Japan, where the government's statutory authority to engage in surveillance either for law enforcement or intelligence purposes is very limited as compared with all of the other countries studied. Although Japan enacted its first wiretap law in 1999, Japanese society strongly disfavors the use of wiretaps and the number of communications intercepts is miniscule.[64] Moreover, Japanese law lacks any statutory basis for authorizing wiretaps for counter-terrorism purposes. Similarly, the Brazilian constitution only authorizes interception of communications for criminal investigations and, while Brazil maintains an intelligence apparatus, the lead intelligence agency lacks both investigative and surveillance powers (Magrani, n. 8).

2. **Content/non-content distinction:** A number of countries (Australia, Brazil, Canada, Germany, Italy, Israel, South Korea, the UK and the US) draw a legal distinction between the content of communications and various types of non-content,[65] establishing higher standards for government access to the former and lower standards for access to the latter. For example, Brazilian courts have ruled that "judicial authorization is not required for the Police or the Public Prosecutor's Office to have access to subscriber-identifying data from companies," on the grounds that anonymous speech is constitutionally prohibited (Magrani, n. 8). British law imposes very few controls on access to non-content data (both communications attributes and subscriber data), which are easily accessible by a very large number of central and local officials, simply requiring that a senior official make a request. There were over half a million such requests in 2010 (Brown, n. 10 at 235). Similarly, non-content requests are subject to lower standards in Australia, Brazil, Israel, Italy, South Korea, and the US. On the other hand, it appears that neither India nor Japan

[63] Dan Jerker B. Svantesson, 'Systematic Government Access to Private-Sector Data in Australia', (2012) 2/4 International Data Privacy Law 268, 269 http://idpl.oxfordjournals.org/content/2/4/268.full. For example, federal police are entitled to obtain documents that are "relevant to, and will assist in, investigations of serious terrorism offenses," without any court order. Similarly, the Australian Security Intelligence Organization (ASIO) may obtain computer access by requesting the Minister to issue a warrant (id. at 270).

[64] See Motohiro Tsuchiya, 'Systematic Government Access to Private-Sector Data in Japan', (2012) 2/4 International Data Privacy Law 239, 242 (Table 1) http://idpl.oxfordjournals.org/content/2/4/239.full.

[65] "Non-content" data, also referred to as "transactional," "connection" or "envelope" data, includes both communications attributes such as the time, duration and medium of communication, the technical parameters of the relevant transmission devices and software, the identities and physical locations of the parties, and their electronic addresses; and b) subscriber data such as name, address, phone number, and/or credit card information.

distinguishes between content and non-content requests.

3. **Technology/business model neutrality:** Most of the countries studied apply the same standards for real-time interception of content (voice communications, text messages, email, and so on) regardless of the technology on which the content is transmitted or the business model of the service provider, with three exceptions. China has enacted multiple, Internet-related laws regulating very specific services (e.g., traditional ISPs, telecoms, content providers, data centers, messaging services, news services, etc.) (Wang, n. 7 at 225-27). Germany follows a "layer model" that draws complex distinctions between the content of online communication, the services provided on the Internet, and the "levels" at which data transfer takes place, all of which are regulated under different laws. (Schwartz, n. 6 at 295). Finally, the US distinguishes between communications in real-time, and in storage and protects them differently.[66]

4. **Third party doctrine:** In the US, there is longstanding precedent that the Constitution's Fourth Amendment, which protects against unreasonable searches and seizures, does not apply to records held by third parties.[67] Accordingly, in the US, privacy protection for business records mainly derives from statute (Pell, n. 13 at 252).[68] The US is more or less unique in affording no Constitutional protection to third-party data, although a few other countries also handle third party data somewhat differently. For example, in Canada, a reasonable expectation of privacy may not attach to information held by a

"The US is more or less unique in affording no Constitutional protection to third-party data"

[66] A campaign is underway in the US to reform ECPA by extending to stored communications content many of the protections that apply to content in transit. See Ryan Gallagher, 'Ancient Electronic Communications Law May Finally Be Updated to Protect Email Privacy,' *Slate* (Mar. 23, 2013) http://www.slate.com/blogs/future_tense/2013/03/19/patrick_leahy_introduces_legislation_to_update_ancient_electronic_communications.html.

[67] Fourth Amendment protections are unavailable both for financial records, see *United States v. Miller*, 425 U.S. 435 (1976), and transactional information held by third parties that is associated with either phone calls or email, see *Smith v. Maryland*, 442 U.S. 735 (1979).

[68] In 2010, a federal appeals court (covering four states) held that the Constitution does in fact protect the content of stored communications. See *United States v. Warshak*, 631 F. 3d 266 (6th Cir. 2010). In 2013, the US Department of Justice stated to Congress that it followed the Warshak rule nationwide, obtaining a warrant under the Constitution in order to compel a service provider to disclose the contents of stored communications. In a 2011 decision, the US Supreme Court rejected the absolute claim that a person loses all Constitutional interest in whatever is disclosed to a third party, see *United States v Jones*, 565 US ___, 132 S. Ct. 945 (2012); however, the majority's holding was much narrower and the third party doctrine is still being applied in full force to non-content data.

third-party with no obligation to maintain confidentiality (Bailey, n. 53 at 209). In the UK, communications traffic data (including data in the cloud) may be voluntarily shared with the government for purposes of national security, law enforcement, and taxation (Brown, n. 10 at 235). Finally, China seems to accord *higher* protection to data stored in the cloud, apparently in an effort to attract international investors who might otherwise be scared away by the "golden shield" projects (Wang, n. 7 at229).

5. **Use, retention, disclosure limits:** The European countries in the survey have all implemented the EU Data Retention Directive, which limits collection, retention, and disclosure of personal data by the public and private sectors. However, the Directive expressly does not apply to the processing of data for law enforcement or national security purposes. Israel also has a comprehensive privacy law but it too does not apply to the activities of the police or internal or external security services. Canada and the US have Privacy Acts that regulate the collection, use and retention of personal data by federal governmental entities; those Acts apply to law enforcement and intelligence agencies, but the US law allows many exceptions for law enforcement and intelligence databases. Key provisions of South Korea's comprehensive data protection law do not apply to data collected for national security purposes. Of the remaining three countries, draft data protection laws are under consideration in both Brazil and India, while the Chinese legislature recently passed a data protection resolution. The Chinese law contains "significant and far-reaching requirements applicable to the collection and processing of electronic personal information via the Internet,"[69] but it does not impose any meaningful limits on government access for security purposes.

6. **Oversight mechanisms:** Each country, except China, has some process of independent oversight of surveillance and government access, although standards vary widely. In the UK, courts play no role in authorizing interceptions for criminal or national security matters; rather, the Home Secretary or the Foreign Secretary issues authorizations, while a panel of independent lawyers (the Investigatory Powers Tribunal) carries out oversight duties (Brown, n. 10 at 297). In India, courts also play a very limited role. Although older laws required a court order for access to letters and telegrams, these safeguards are "no longer relevant in today's information society" (Abraham and

"Each country, except China, has some process of independent oversight of surveillance and government access"

[69] See 'Chinese Legislature Passes Data Privacy Resolution,' (Jan. 2, 2013), Privacy and Information Security Law Blog, http://www.huntonprivacyblog.com/?s=china (also noting that "one provision … could actually erode the protection of personal privacy: ISPs must require that customers provide their real names on agreements for the provision of access or information-related services").

Hickok, n. 9 at 311). More recent enactments in India offer much weaker protections and seem to minimize the role of courts in authorizing wiretaps (id. at 306), access to non-content data (id. at 311), and access for national security reasons (id. at 305). In particular, the Information Technology Act of 2008 dispenses with case-by-case authorizations for access to data in favor of blanket authorizations and permits the use of such data for broad and generic purposes (id. at. 305). India also suffers from problems with corruption, and there are reports that "law enforcement officials abuse their positions to dilute data access safeguards" (id. at 313). In Germany, prior judicial approval is required for wiretapping by the police in ordinary criminal cases, but interception for intelligence purposes is conducted upon the approval of the Interior Minister. Before conducting "strategic surveillance" for foreign intelligence purposes, the government must obtain the permission of a Parliamentary Controlling Commission; when the government is conducting individualized intelligence gathering, the Parliamentary Controlling Commission and the G-10 Commission fulfill only a "controlling function," which seems to mean they exercise after-the-fact oversight. Germany's Constitutional Court has played a key role in overseeing the surveillance activities of Germany's foreign intelligence agency, the BND, forcing several amendments to the G-10 statute that regulates so-called "strategic surveillance" for intelligence purposes (Schwartz, n 6. at 297). In the US, prior court approval is required for both law enforcement and foreign intelligence surveillance conducted inside the US, with one exception that has loomed large after the Snowden leaks: When surveillance conducted inside the US targets non-citizens who are believed to be outside the US at the time of the access, the courts approve only the broad outlines of the surveillance program and individual targeting decisions are made by the NSA.

7. **Design mandates:** As far as we know, based on the country papers and additional research, only a few of the countries studied have explicit design mandates. For example, Israel (Tene, n. 58 at 280), Australia, Germany, and the US (Pell, n. 13 at 254) have enacted laws authorizing government officials to seek changes to the design of telecom equipment, facilities, and services to ensure that they have built-in surveillance capabilities. In the UK, the government may impose obligations on public telecom services to ensure that they maintain interception capability (Brown, n. 10 at 233).[70] China and India have sought to control network design without explicit statutory authority. While China has undoubtedly succeeded (Wang, n. 7 at 225), the results in India are more ambiguous (Abraham and Hickok, n. 9 at 307). In other countries, the issue has not surfaced in public debate, perhaps due to the close relationship between government authorities and service providers, with the latter voluntarily taking steps to ensure that their facilities are wiretap-ready.

[70] The British design mandates are part of the Regulation of Investigatory Powers Act 2000 (RIPA), which has broad surveillance provisions, a design mandate akin to CALEA, and a data retention requirement.

8. **Retention mandates:** A few of the countries studied have imposed data retention mandates on telephone companies, ISPs and other service providers. The UK, France, Italy, and Germany enacted data retention laws as required by the EU Data Retention Directive. The German statute required telecommunications providers to store specific kinds of traffic and location data for a period of six months. In 2010, however, the German Constitutional Court struck down the statute and the German parliament has yet to enact a new statute (Schwartz, n. 6 at 294).[71] China imposes extensive mandatory data retention on telecoms, ISPs, and content providers (Wang, n. 7 at 224). Brazil, Canada, Japan, and the US lack data retention mandates.

V. Comparative Analysis: The Normative Framework

In this section, we turn from a description of government access rules to the normative question of how national rules measure up against the standards for surveillance identified by the European Court of Human Rights.

A. The Normative Framework

Government surveillance demands, whether for access to one account at a time or for systematic access, and whether for regulatory, law enforcement or national security purposes, do not arise in a normative vacuum. A series of factors for assessing governmental demands can be derived from the concept of "rule of law" and from existing (although still evolving) international human rights jurisprudence.

The "rule of law" is an internationally recognized concept encompassing, at a minimum, principles of transparency, limits on the discretion of government officials, and accountability.[72] A leading legal philosopher, Joseph Raz, identified eight key principles of the rule of law, of which six are especially relevant to questions of government surveillance and access to data held by the private sector:

1. Laws should be prospective, open, and clear
2. Laws should be relatively stable
3. The rules for making particular laws should be open, stable, clear, and general

[71] Both Ireland and Slovakia are now challenging the EU Data Retention Directive in the European Court of Justice. See Karlin Lillington, 'Data privacy battle plays out before European court,' *The Irish Times* (July 11, 2013), http://www.irishtimes.com/business/sectors/technology/data-privacy-battle-plays-out-before-european-court-1.1459277.

[72] For a classic statement of these principles, see Lon Fuller, *The Morality of Law*, revised edition (Yale University Press, New Haven, 1969).

4. The judiciary should be independent
5. Courts shall have review power over all other principles
6. "The discretion of the crime-preventing agencies should not be allowed to pervert the law."[73]

"The 'rule of law' is an internationally recognized concept encompassing, at a minimum, principles of transparency, limits on the discretion of government officials, and accountability"

These principles have been embodied in major international human rights instruments. In addition, major human rights instruments protect the right to privacy. Of greatest relevance, because it has generated the largest body of interpretative case law setting out standards of global relevance, is Article 8 of the European Convention on Human Rights (1950), which states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[74]

The European Court of Human Rights (Strasbourg Court), whose decisions are binding on the 47 member states of the Council of Europe, has issued multiple rulings on the applicability of Article 8 to secret systems of surveillance.[75] Although the Convention preceded the Internet by many years and does not explicitly contemplate modern means of communication, the Strasbourg Court has successively applied art. 8-1 to

[73] Joseph Raz, 'The Rule of Law and its Virtue,' in *The Authority of Law: Essays on Law and Morality* (Clarendon Press, Oxford, 1979). Raz's other two principles address the need for making courts easily accessible to all and the necessity of observing principles of natural justice.

[74] Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention") http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm. Article 7 of the EU Charter reproduces but slightly updates the wording of art. 8(1): "Everyone has the right to respect for his or her private and family life, home and communications." See Charter of Fundamental Rights of the European Union of the European Parliament, December 7, 2000, *O.J.,* No. C 364, 20000, p. 1 et seq.

[75] For an overview, see R. White & C. Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights* 365-71 (Oxford Univ. Press, 5th ed., 2010).

telephone conversations,[76] telephone numbers,[77] computers,[78] and the Internet and e-mail.[79] The Court has held that the existence of legislation which allows a system of secret monitoring entails a threat of surveillance for all those to whom the legislation may be applied, and that this threat itself amounts to an interference with rights under Article 8, allowing persons to invoke the Court's jurisdiction even if they cannot prove that they themselves have been subjected to surveillance. In addition, the Court has held that the sharing of data with other government agencies, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with Article 8 rights.[80]

Once it is determined that surveillance of a given form of communication constitutes interference with the rights guaranteed by art. 8-1, the Court next considers whether the interference is justified under art. 8-2 by assessing it in light of three tests: First, is it "in accordance with the law"? Second, is it pursued with one or more legitimate aims (including national security) in mind? And, third, is it "necessary in a democratic society"? The Court's decisions have enumerated specific criteria for applying these standards.

A very clear statement of these criteria is found in the *Weber and Saravia* case,[81] which examined "strategic surveillance" under Germany's G-10 Act.[82] In deciding that the G-10 Act did not violate art. 8, the Strasbourg Court first reiterated that the expression "in accordance with the law" has two elements. It requires "that the impugned measure should have some basis in domestic law." It also refers, the Court said, to "the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law."[83]

---

[76] *Klass and others v. Germany,* Application no. 5029/71, Judgment of 6 September 1978, § 41.

[77] *Malone v. United Kingdom*, Application no. 8691/79, Judgment of 2 August, 1984, § 84*; Copland v. the United* Kingdom, Application no. 62617/00, Judgment of 3 April, 2007, § 43.

[78] *Leander v. Sweden,* Application no. 9248/81, Judgment of 26 March, 1987, § 48*; Rotaru v. Romania,* Application no. 28341/95, Judgment of 4 May, 2000, § 42-43.

[79] *Copland*, § 41.

[80] See *Weber and Saravia v. Germany,* Application no. 54934/00, Judgment of 29 June, 2006, §§. 78-79.

[81] *Weber and Saravia,* id.

[82] See Schwartz. n. 6 at 291-292, 297-298.

[83] *Weber and Saravia*, § 83.

In *Weber and Saravia*, the Court found that the German law readily satisfied the "basis in law" requirement. As to the foreseeability requirement, the Court said that, in the context of surveillance, this does not require any self-defeating form of notification that would allow an individual to adapt his conduct accordingly to avoid interception of his communications. Rather, the Court said, in view of the risks of the arbitrary exercise of secret powers, it is essential to have detailed rules that are clear enough to give citizens "an adequate indication" as to the circumstances and conditions under which government agencies are allowed to resort to surveillance measures.[84] The Court went on to specify certain minimum safeguards that must be set out by statute for surveillance laws like the G-10 Act to avoid abuses of power and satisfy the "in accordance with law" standard. Specifically, a statute must specify:

> "… the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."[85]

In another case, the Court made it clear that the requirement that conduct be prescribed by law also applies to the treatment of material after it has been obtained, meaning that the law must specify the "procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material."[86]

Next in *Weber and Saravia*, the Court turned to the purpose and necessity tests. As the aim of the G-10 Act is to safeguard national security and/or prevent crime, its purposes squarely fit within the terms of art. 8(2). As to whether the interferences permitted by the G-10 Act are "necessary in a democratic society," the Court relied on a balancing test that weighs "all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."[87] Under this balancing test, the Court concluded that while national authorities retain a degree of discretion over how best to structure a system of surveillance in response to terrorism and related threats, domestic surveillance laws may not grant unfettered power to law enforcement or intelligence agencies.

---

[84] Id., § 93.

[85] Id., §95.

[86] *Liberty and others v. U,K*, Application no. 58243/00, Judgment of 1 July 2008, § 69.

[87] *Weber and Saravia*, §106.

Based on the tests developed in earlier cases and reiterated in the *Weber and Sarvia* case, the Strasbourg Court has developed fairly detailed guidelines for assessing national surveillance law. For example, in *Weber and Saravia* itself, the Court found that an amended version of the G-10 Act authorizing strategic interception of international communications was consistent with Article 8 because the statute contained the following elements: The search terms had to be listed in the monitoring order, which also had to set out detailed rules on storing and destroying any data obtained using these search terms, and the authorities storing the data had to verify every six months whether the data was still necessary to achieve the purpose for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed or deleted from the files, or access to them had to be blocked, and all of these steps had to be recorded and, in some cases, supervised by a senior official.[88]

"The Strasbourg Court has developed fairly detailed guidelines for assessing national surveillance law"

In the *Klass* case, which concerned the targeted surveillance provisions of the German G-10 Act (distinct from those at issue in *Weber and Saravia*), the Court identified a series of limiting factors in the Act that also led it to find those targeted surveillance provisions in conformity with Article 8: the Act required a factual indication of suspicion; exhaustion of less intrusive means; particularity as to a specific suspect and his presumed contacts (hence "exploratory or general surveillance" is not permitted); a written application for a surveillance order from a senior official; a decision by a senior official; limited duration of no more than three months; implementation by an official qualified for judicial office; and oversight by an independent entity.[89]

Based on these and other cases[90] assessing surveillance laws under art. 8, we have identified fourteen normative factors that should be considered in evaluating laws for systematic assess:

[88] Id., §§ 97-100.

[89] *Klass*, § 51-60.

[90] See also *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 27 June, 2007. This case examined the adequacy of Bulgaria's "Special Surveillance Means Act" (SSMA) and concluded that it violated art. 8 because it provided neither sufficient guarantees against the risk of abuse inherent in any system of secret surveillance nor effective remedies against the use of such special means.

TABLE 3: THE NORMATIVE FRAMEWORK

1. "In accordance with law" - Are surveillance standards spelled out in a public law or regulation precisely enough to protect against arbitrary application and to inform the public of which entities can conduct surveillance and under what criteria? Does the law specify the procedures to be followed for examining, using and storing the data obtained?
2. Court order - Does surveillance (data acquisition) require authorization by an independent judicial officer (with possible exception for emergency circumstances)?
3. Approval of senior official – For surveillance in criminal investigations, is approval of a senior police or ministry official required? For national security matters, is approval of a senior intelligence official required, and is approval required from a senior official outside the security service (for example, the Attorney General or a legislative body)?
4. Limited to serious crimes or serious threats - Is surveillance limited to the investigation of specified serious crimes? In the national security context, are the topics of surveillance narrowly defined and/or limited to specified serious threats or subjects, or is surveillance permitted, for example, for all matters affecting national security?
5. Particularity as to target - Must each surveillance be limited to a specifically designated person or account, or is "strategic" or generalized monitoring permitted?
6. Showing of suspicion – In the criminal investigative context, does application and approval require a showing of a strong factual basis for believing that the target is engaged in criminal conduct? In the national security context, does application and approval require a showing of a strong factual basis for believing that the target is a foreign power, is engaged in terrorism or other activities that threaten national security, or is otherwise suspected of being engaged in activities or having information of national security significance?
7. Exhaustion of less intrusive means - Does approval require a showing that other less intrusive means will not suffice or are unlikely to obtain the needed information?
8. Limit on duration – Is the duration of the surveillance limited (e.g., to 30 days, subject to renewal)?
9. Limit on scope ("minimization" of irrelevant data) – Is the government required to ensure that irrelevant data is not recorded or, if collected, is destroyed or neither searched nor used?

TABLE 3: THE NORMATIVE FRAMEWORK (cont.)

10. Limit on use and disclosure - Are there limits on the use and disclosure of data that is collected? For example, in the criminal investigative context, does the relevant law specify that data collected can be used only for investigation of the crimes that justified the surveillance? Does the law prohibit disclosure to other entities? In the national security context, does the relevant law specify that data collected cannot be used for investigation or prosecution of crimes, or does the law prohibit disclosure to other entities?
11. Retention limit/limit on storage – Is there a time limit set on how long the government can retain intercepted communications?
12. Notice to target – Must the target of the surveillance, or other persons whose communications are intercepted, be provided notice of the surveillance (normally after the investigation is concluded)?
13. Oversight by independent entity – Does an independent body (judicial, executive, legislative) oversee the actual implementation of surveillance procedures to protect against abuse?
14. Redress (remedy) - Can individuals obtain redress for violations of the established standards?

Using these factors, we developed a chart that summarizes the laws of the thirteen surveyed countries as they apply to surveillance in the law enforcement context (Chart 3), and one that does the same for the rules in national security matters (Chart 4).

B. The Normative Analysis: Comparative Observations

With respect to the standards for real-time surveillance in criminal investigations, the laws in all of the countries we surveyed (except China and India) are broadly consistent with the normative factors set forth in Table 3. That is, the countries generally have statutes expressly authorizing ("in accordance with law") real-time interception of communications content only for the investigation of serious offenses and only upon the approval of both a senior executive branch official and an independent judicial officer. Such statutes generally place limits on the duration of the surveillance and the use of information obtained. The statutes seem to be premised on the principle of particularity – that is, they only authorize surveillance targeted at a specified person, device, or account. The UK is an outlier on one major point in that it does not require judicial approval for electronic surveillance, but rather vests approval authority with an executive branch official (a Secretary of State). Also, almost half the countries studied do not have provisions expressly limiting the scope of the content that can be recorded (by requiring that government agencies not record irrelevant data or, if they do, that they do not retain such data) and almost the same number lack laws requiring notice of surveillance to the target of surveillance or other persons whose communications are

intercepted. China meets none of the fourteen standards identified in our normative framework and India meets only one of the fourteen (approval of a senior officer required) and somewhat addresses another standard (loosely tying surveillance to suspicion of criminal conduct by requiring that the surveillance be "necessary or expedient" for the investigation of an offense).

While standards for real-time interception of communications for law enforcement purposes are uniformly high in the countries we surveyed (except in India and China), standards for access *to* stored communications held by third parties are less consistent. In France, for example, stored documents can be accessed in some circumstances by the judicial police or customs authorities and in other cases upon the approval of the public prosecutor. In the US, the Electronic Communications Privacy Act states that service providers can be forced to disclose stored content with a mere subpoena, issued without judicial approval, although an appellate court has held that process to be in violation of the Constitution, and service providers and the Justice Department now seem to agree that a judicial warrant is needed to compel third party disclosure of content. To the extent that any laws expressly address stored content, it is not clear whether any of them give attention to the questions of scope or minimization; that is, while real-time interception is normally approved for periods of limited duration and some laws limit the recording of irrelevant information, it is not clear whether orders for disclosure of stored communications contain any temporal scoping limitations, and it is not clear how rules on minimization of irrelevant data would be applied in the case of disclosure of stored data.[91] In Europe, however, under art. 8 of the Convention, acquisition of stored content might be subject to a requirement that the law authorizing the collection must specify the procedure to be followed for selecting the material to be collected.[92]

When it comes to transactional data regarding communications, standards are even weaker. In the UK, traffic data can be obtained upon the demand of a very wide range of government officials, including in non-criminal matters. In the US, stored telephone metadata is available without a court order (but not cell site location information), while access to Internet metadata and real-time interception of telephone or Internet metadata require a court order. In Australia, the law permits voluntary disclosure of communications metadata to law enforcement and intelligence agencies while also providing for mandatory disclosure upon request. In South Korea, while it is clear that the government must obtain a court order to require a telecommunications service provider to disclose transactional data ("communications confirmation data"), the

[91] See Orin Kerr, 'The Next Generation Communications Privacy Act,' (2013) 162 U. Pa. L. Rev. (noting the absence of any scoping or minimization limits in ECPA, the US law regulating access to stored communications).

[92] See *Liberty and others v. UK* at § 69.

vagueness of the provisions seemed to allow ISPs to voluntarily disclose such data to the government without a court order, and such voluntary disclosures used to be customary. However, a major court ruling in 2012 casts doubt on the legitimacy of voluntary disclosures.

With respect to the standards for government access to communications in national security investigations, the overall picture is very complex. For example, whereas most countries surveyed (again, leaving aside China and India) require a court order for surveillance in criminal investigations, almost half the countries studied do not have provisions requiring court orders for surveillance undertaken in the name of national security or for foreign intelligence gathering. Likewise, at least half do not pose limits on the scope of national security requests, or require notice to targets.

"Almost half the countries studied do not have provisions requiring court orders for surveillance undertaken in the name of national security or for foreign intelligence gathering"

While laws setting standards for interception in criminal cases generally require targeted surveillance, the rules for national security are much less consistent in imposing a particularity requirement. The statutes in Germany and the UK expressly allow large-scale, untargeted collection of communications with one leg originating outside the country. The American and French laws distinguish between communications carried by wire (including fiber) and communications transmitted over radio waves (including satellite transmission). In both countries, the relevant statutes permit non-targeted surveillance of radio communications where one end of the communication originates abroad. Canada and Australia have long collaborated with the US and the UK in bulk collection programs.

In addition, it is worth noting the diversity of oversight mechanisms in both criminal and national security investigations. They include annual reports on the number of intercepts and other information, which are delivered either to senior government officials or to legislative committees; reviews by appointed oversight commissions; audits; and legislative investigations. The US has multiple oversight mechanisms. Even warrantless surveillance under the now notorious PRISM program is overseen by the Foreign Intelligence Surveillance Court, which approves the targeting and minimization procedures and monitors implementation of the program. Recently, Congress created (and after long delay, approved the nominations of the members of) a board to review and analyze executive branch anti-terrorism efforts and ensure they are balanced with the need to protect privacy and civil liberties and consider liberty concerns in the

formulation of related law and policies.[93] As Paul Schwartz has suggested, however, many such formal oversight mechanisms are quite ineffective and amount to little more than what he calls "privacy theater."[94] In countries with an independent press and/or strong laws protecting the freedom of speech, informal oversight mechanisms, though raising their own complications under criminal and national security laws, also play a role thanks to the efforts of the press, advocacy groups, government watchdog groups, and various dissenters, whose work calls attention to illegal or abusive surveillance practices, thereby enhancing government accountability.[95]

"Most of the countries studied permit location tracking subject to a weak standard"

In terms of location data, most of the countries studied permit location tracking subject to a weak standard. For example, location data may be tracked without a warrant in Australia, China, Germany, India, Israel, and the UK. In the US, however, the relevant doctrine is more complex thanks to a recent Supreme Court decision, *US v. Jones*, announcing a new, trespass-based test for what counts as a search under the Fourth Amendment. Although *Jones* applied the trespass test to find that the installation of a GPS device on a vehicle with the intent to use it was a search, the exact circumstances under which the use of such a device requires a warrant are not yet clear The standards under which government agencies can compel disclosure of cell site location information are less settled. ECPA requires, at a minimum, a court order, and a majority of courts have held that a warrant is needed for real-time tracking, while a majority of courts have held that a full warrant is not necessary to compel disclosure of stored location records.

Most countries handle travel and financial data under laws requiring routine, bulk reporting for specified classes of data. For example, most countries require passenger data reporting for air travel (Australia, Brazil, Canada, China, Israel, South Korea, the UK, and the US). International arrangements for sharing passenger data are more

[93] For an overview of the Privacy and Civil Liberties Oversight Board (PCLOB), see http://www.pclob.gov/.

[94] Paul M. Schwartz, 'Reviving Telecommunications Surveillance Law' (2008) 75 University of Chicago Law Review 287.

[95] *See* Jack L. Goldsmith, *Power and Constraint: The Accountable Presidency After 9/11* 205-43 (Norton, New York, 2012)(arguing that the executive branch is forced to account for its actions by the constant gaze of "courts, Members of Congress and their staff, human rights activists, journalists and their collaborators, and lawyers and watchdogs inside and outside the executive branch" who together constitute a highly effective "presidential synopticon"). The latest NSA revelations would seem to confirm this insight yet it remains highly debatable whether such informal mechanisms suffice.

controversial.[96] All thirteen countries also require anti-money laundering reporting under generally similar national laws, under which large financial transactions must be reported. Italy and others require certain entities to notify the tax authorities of various other transactions. In Italy, this is a direct response to the high level of tax fraud and evasion.[97]

With respect to the normative standards for government access to business records, the results are more difficult to summarize. In Australia, for example, a police officer seeking documents (including in electronic form) may make an application to a federal magistrate for a "notice to produce" order. To grant such an order, the magistrate must be satisfied, on the balance of probabilities, by information on oath or by affirmation, that: "(a) the person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious offence; and (b) giving the person a notice under this section is reasonably necessary, and reasonably appropriate and adapted, for the purpose of investigating the offence" (Svantesson, n. 63 at 270). However, if an authorized police officer considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offense, no prior court approval is required. Similarly, in the UK, Section 19 of the Counter-Terrorism Act provides that "A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions" (Brown, n. 10 at 235). Most countries, with the exception of China and India, observe some limits on use, retention, and disclosure; provide oversight and redress mechanisms (ranging from complaints to a Privacy Commissioner to civil actions); and must satisfy various reporting requirements. However, limits on use and disclosure often have many exceptions. In Australia, for example, information obtained by one agency for a specific purpose may be available to a range of other agencies for quite different purposes. The European Court of Human Rights has explicitly held that a transmission of data to and their use by other authorities constitutes "a further separate interference" with the right to privacy under art. 8 of the Convention. Such disclosures are not flatly prohibited but must be subject to the same principles of "in accordance with law" and necessity; in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, the Court expressly declared

[96] In 2012, the European Parliament approved a passenger name record (PNR) agreement with US, under which US authorities are permitted access to EU citizens' airline records; see Kirsten Fieldler, 'EU Parliament Agrees to EU-US PNR Agreement,' *EDRI* (April 25, 2012) http://www.edri.org/edrigram/number10.8/ep-agrees-us-eu-pnr. A year later, however, it rejected a proposal to create a pan-European system for sharing and storing passengers' phone numbers, addresses and credit card details whenever they entered or departed the 27-country European Union, on the grounds that it breached citizens' fundament rights; see Tedd Nykiel, 'European Lawmakers Reject Passenger-Data Scheme,' *Reuters* (April 24, 2013) http://uk.reuters.com/article/2013/04/24/uk-eu-data-idUKBRE93N0U020130424.

[97] See Resta, n. 5 above. Additionally, Italian hotels automatically report the identity of all hotel clients to the police.

Bulgaria's intelligence surveillance law to be inconsistent with the Convention because it did not place adequate limits on disclosure and use.

"Germany has most expressly addressed the issues associated with systematic access to business records"

Of all the countries surveyed, Germany has most expressly addressed the issues associated with systematic access to business records and the application to those records of analytic techniques for law enforcement purposes. On the one hand, as Paul Schwartz noted, data mining is an established law enforcement technique in Germany (the German term for the practice is a "screening search"). On the other hand, the German Constitutional Court has set limits on the use of the technique. In Germany, laws at the federal and state levels distinguish between the use of "data screening" to (1) investigate past crimes, or (2) permit a preventive response to potential crimes. Data screening to investigate past crimes is regulated by various state laws and at the federal level by section 98a of the Criminal Procedural Code. The federal statute permits screening searches only where there are "sufficient factual indications to show that a criminal offense of significant importance has been committed." However, there are state statutes that permit a *preventive* use of data screening. In 2006, the German Federal Constitutional Court established significant limits on such law enforcement use of this practice. In its *Data Screening* opinion, the Constitutional Court used a proportionality standard to find that data screening for preventative purposes was constitutionally permissible only when the police had concrete facts indicating that a serious crime was being planned (Schwartz, n. 6 at 292-93). Further study of the use of screening searches in Germany since the Constitutional Court's decision may yield useful lessons.

VI. Recommendations and Conclusions

Our research into systematic access, augmented by recent revelations about the scope and scale of surveillance programs in the US and in other countries, suggests at least four conclusions, each posing unresolved challenges.

First, technological developments associated with the digital revolution make it easier than ever for governments to collect, store, and process information on a massive scale, and governments seem to be exploiting those developments, and responding to pressing threats such as terrorism, by demanding more and more information. At the same time, ongoing developments in the ability to analyze large data sets are leading governments to assert that they can extract crucial but otherwise unobtainable insights from big data. For example, in the context of defending its telephony metadata program, the US government has expressly argued that, in order to find "the needle in the haystack," it needs to acquire the entire haystack. Though governments have long

required corporate entities to systematically report certain data, such as currency transactions over certain thresholds, that information used to remain "siloed." Government agencies today are under information sharing imperatives, and modern analytic techniques are seen as offering increasingly powerful abilities to draw from data inferences that are unrelated to the purposes for which they were initially collected.

- **Policy implications:** The trend toward systematic collection poses challenges to the existing legal frameworks because many of the statutes regulating government access and data usage were premised on particularized or targeted collection, minimization, and prohibitions on information sharing and secondary use.[98]

Second, as Internet-based services have become globalized, trans-border surveillance – surveillance in one country affecting persons in another- has flourished. Gone are the days when intelligence agencies had to acquire data from a point within the country where the data originated or with an antenna aimed at the targeted country. Now, in many instances, communications to or from people in one country pass through or are stored in other countries, where they are available to those governments. The US is perceived as having unique advantages in this respect, both because a large percentage of the world's communications pass through or are stored in the US and because the US has invested vast resources in collection capabilities, but the US is not alone in exploiting global data flows. Moreover, the global flow of data and the popularity of US-based services not only means that the US has access, inside the US, to the communications of those living and working outside the US. It also means that the US has access, outside the US, to communications of persons living and working inside the US. This is because communications to and from people in the US, and even purely domestic communications, can be captured as they move between servers outside the US.

- **Policy implications:** The rise in trans-border surveillance raises complex questions. To begin with, statutory frameworks for surveillance tend to be geographically focused and draw distinctions between communications that are wholly domestic and communications with one or both communicants on

[98] A cornerstone of the privacy framework that has guided privacy laws globally for the past 30 years is the principle that data collected for one purpose should not be used for another purpose, yet big data analytics explicitly promises to find unanticipated meanings in data. Big data equally challenges other core privacy principles. See Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?* International Data Privacy Law (2013) vol. 3, no. 2 pp.74-87 ("when this advancing wave arrives, it will … overwhelm the core privacy principles of informed choice and data minimization"). See generally Christopher Kuner, Fred H. Cate, Christopher Millard, and Dan Jerker B. Svantesson, *The Challenge of "Big Data" for Data Protection*, International Data Privacy Law (2012) vol. 2, no. 2 pp. 47-49.

foreign soil. Moreover, statutory frameworks, as far as we can tell, often draw a distinction between the collection activities that an intelligence service performs on its own soil and the activities that it conducts extraterritorially. This is certainly true of the US: The Wiretap Act and the Foreign Intelligence Surveillance Act do not regulate the conduct of the US outside US territory (with a minor exception for intelligence surveillance outside the US targeting US persons outside the US).

"Lowered standards for trans-border surveillance have a substantial impact on companies that offer global communications services"

Lowered standards for trans-border surveillance have a substantial impact on companies that offer global communications services and want to be able to assure their customers worldwide that their communications are secure. They also raise human rights questions about the existence and scope of state duties to protect and respect privacy and free expression of people outside the state's territorial boundaries. While privacy is universally recognized as a human right, some governments (including the US) assert that their human rights obligations have a territorial limit.[99]

Third, national security legal authorities have become increasingly powerful since 9/11 in the UK and other European countries, the US, and globally. It has long been the case that governments have claimed greater powers to collect data in the name of national security than in ordinary criminal law enforcement cases.

- **Policy implications:** In the post-9/11 world, at precisely the time that technological capabilities are increasing, and at precisely the same time that global data flows are expanding exponentially, national security powers have been getting stronger, raising new questions relating to the trust that citizens, customers, and users vest in governments and corporations alike.

Fourth, this expansion in powers has been conducted in extreme secrecy. In the US, for example, a provision in the PATRIOT Act that seemed to authorize particularized

[99] As Frank La Rue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression, noted, there is "serious concern with regard to the extraterritorial commission of human rights violations and the inability of individuals to know they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance or seek remedies." *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue, to the Human Rights Council*, at 64 (April 17, 2013), available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

disclosures has been interpreted by a secret court order to authorize ongoing bulk collection. Moreover, judicial doctrines in the US (and probably elsewhere) make it very difficult to obtain an effective remedy for possible violations of privacy, free speech, and association rights.[100]

- **Policy implications:** The lack of transparency makes it very difficult to have a rational debate about governmental powers and concordant checks and balances. The lack of openness is leading to proposals that could fragment the Internet, harming both innovation and access to information.

What we need globally is a robust debate about what the standards should be for government surveillance. That debate should be premised on much greater transparency about current practices and about the legal underpinnings of those practices.

Perhaps the most useful framework for making progress on these issues can be found within the context of international human rights law.[101] As we explain above, the most fully developed body of international law on government surveillance and privacy is that of the European Court of Human Rights, which over the years has issued multiple decisions on wiretapping, including national security surveillance. The court has never suggested that secret surveillance is per se a violation of human rights. Instead, it has identified a set of checks and balances that could offer sufficient guarantees against the risk of abuse.

Among the questions to explore:

- How can we give meaning to privacy in an era of systematic collection and trans-border surveillance?
- If bulk collection is an inevitable reality of the digital age, how can we apply human rights principles, such as necessity and proportionality, to claims that

[100] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1141, 185 L. Ed. 2d 264 (2013).

[101] Brazil and Germany have drafted a UN resolution calling on the General Assembly to request "the United Nations High Commissioner for Human Rights to present an interim report on the protection of the right to privacy in the context of domestic and extraterritorial, including massive, surveillance of communications, their interception and collection of personal data, to the General Assembly at its sixty-ninth session, and a final report at its seventieth session, … with the purpose of identifying and clarifying principles, standards and best practices on how to address security concerns in a manner consistent with States' obligations under international human rights law and in full respect of human rights, in particular with respect to surveillance of digital communications and the use of other intelligence technologies that may violate the human right to privacy, freedom of expression and of opinion." See Sangwon Yoon, 'Brazil Joins Germany in Seeking UN Probe of U.S. Spying,' *Bloomberg* (Nov. 1, 2013) http://www.bloomberg.com/news/2013-11-01/brazil-joins-germany-in-seeking-un-probe-of-u-s-spying.html.

it is necessary to collect all the data to serve certain compelling governmental needs?

- Given the widely held view that privacy is a universal right and the equally universal rule that governments have broad powers to protect themselves from foreign threats, how should we regulate trans-border surveillance?

In a networked word, the standards for government access must be judged not so much in the context of a debate between EU and US laws, but rather on the basis of international human rights standards. The US government may argue that the PRISM standards actually comport with international law, but that will be an illuminating debate in which Europeans must explain and defend their own laws by the same standards. If they can have this debate, then government officials in Europe and the US can work with human rights institutions, civil society, and the Internet industry to move the rest of the world towards a set of principles based on transparency, proportionality, and accountability.