Organizational Accountability, Government Use of Private Sector Data, National Security, and Individual Privacy

Background Paper by
James X. Dempsey, Jennifer Stoddart, Fred H. Cate, and Martin Abrams

May 2014

Problem Statement

Companies that collect personal data in the course of their business must be accountable for the safe and fair management of that data. The accountability of companies as data stewards extends both to their own processing of data and to processing by their vendors and partners to whom data is disclosed. The growing appreciation for the concept of accountability leads companies both to carefully structure their own data collection, use, and retention practices as well as to use contracts and other means to ensure that the entities to which they disclose data will likewise be responsible, in a chain of accountability that can extend through multiple links.

What happens, however, to accountability when a government entity demands that a company disclose data in its possession or control? How can a company follow through on its accountability commitments when the fact of the government's demands and the government's uses of data are cloaked in secrecy? Before the Snowden leaks, there was a quiet concern among many private sector entities that government demands were growing.[1] After the Snowden leaks, it is now apparent that many countries around the world are demanding disclosure of large quantities of data directly from companies or are seizing it as it moves over communications links between data centers.

What does accountability mean when data is requested by government entities? Is it sufficient that the government request is authorized by law? How should the adequacy of the law be assessed? How does the transparency element of accountability interact with the government demand, especially in the national security field, that both the fact of disclosure and the government's uses of the data once obtained must be kept secret? These questions have always threatened to impact the integrity of accountability-based data governance. In the wake of the Snowden revelations, the issues have become even more acute:

- The Snowden revelations exposed the scope and depth of government programs accessing corporate data for national security and counterterrorism purposes;
- While the U.S. National Security Agency and the UK's GCHQ were the focus of the Snowden leaks, there is no doubt that national security institutions world-wide have a thirst for personal data held by private sector entities;[2]

[1] We recognize that there is a difference between an enforceable or compulsory "demand" and a "request" that could, under applicable law, be complied with on a permissive or voluntary basis. This paper concerns both mandatory and permissive disclosures, and we use the words "demand" and "request" interchangeably.

[2] For example, a study for the European Parliament found that "[p]ractices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data) characterize the surveillance programmes" of 4 out of 5 of the EU member states selected for the study. "National programmes for mass surveillance of personal data in EU member States and their compatibility with EU law," a study for the Directorate General for internal Policies (2013), http://info.publicintelligence.net/EU-MassSurveillance.pdf.

- The revelations have severely exacerbated public distrust in institutions, public and private, that process personal data;
- It is not clear that the regionalization of the Internet, proposed by some policymakers, would eliminate all surveillance concerns as it would seem that no government completely refrains from surveillance activities. On the other hand, this approach could impact access, efficiency, and costs of global services.

While government access challenges the accountability framework, can that framework also provide solutions? That is, could the elements of the accountability framework be extended to governmental demands and uses of data? What would accountability look like as applied to governments demanding or otherwise obtaining data from the private sector for use in carrying out governmental functions?

These questions implicate the interests of at least four sets of stakeholders: the companies that collect and process data in the course of providing the vast range of services that characterize the information society; the data protection regulators that enforce privacy laws; the law enforcement and national security agencies that require information about individuals and that rely on the cooperation of the private sector to carry out their vital responsibilities; and individuals, represented by policymakers, regulators, and civil society organizations.

The Current Project

To address these questions, the Information Accountability Project is convening a dialogue, fostered through two workshops, one in Montreal on May 9 and one in London on May 30. The purpose of the meetings is to (1) identify the challenges that systematic government access to personal data held by the private sector presents to accountable stewardship of that data by responsible private sector organizations; (2) explore the potential for standards, norms, or principles that industry, regulators, investigatory and intelligence agencies, and policymakers might look to when developing policies concerning accountable behavior in connection with government demands for broad access to personal data; and (3) craft tools/processes to help achieve those standards and provide companies, regulators, and law enforcement and national security agencies with appropriate oversight to restore public trust in the actions of both corporations and government agencies.

The issue of accountability and government access to private sector data has at least four elements:

- How should accountable companies review and limit requests for disclosure?
- How might those requests be parsed beyond what is legal to what is appropriate?
- How might accountable companies be transparent about both requests for data and how they are parsed?
- How might the concept of accountability extend to the governmental entities that are the recipients of the data?

The first three of these questions have been explored by individual companies and on a multi-stakeholder basis by the Global Network Initiative (GNI) and others.[3] The fourth question–how to extend the principles of accountability to the practices of government–is unique, we believe, and the one where we hope to make the greatest contribution in the current phase of this project.

[3] https://www.globalnetworkinitiative.org/.

Background – The Landscape of Systematic Government Access

In 2011, The Privacy Projects (TPP) began funding research and dialogue on what seemed at the time an obscure and even speculative topic: systematic government access to data held by the private sector. The project, led by the Center for Information Policy Research at Indiana University and by the Center for Democracy & Technology (CDT), commissioned a series of country reports, ultimately totaling 13, detailing, as much as could be determined on the public record, the laws regarding broad government access to private sector data. (The countries studied were Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the UK, and the U.S.) The country reports were published in two volumes of *International Data Privacy Law*. [4]

The project also convened a series of roundtable discussions. The first, comprising private sector leaders, was held in Washington in April 2012; the second brought together companies, academics, and civil society advocates in London in late May 2013 (days before the Snowden leaks began); and the third, a multinational meeting with private sector and civil society representatives, joined by DPAs and other government officials, was held in Brussels in November 2013.

The project managers wrote two major papers. One introduced the first round of country studies and summarized (under the Chatham House Rule) the Washington discussion.[5] The second was a lengthy comparative analysis of systematic access laws, building on both the country reports and the dialogues in London and Brussels. Written by Ira Rubinstein, Greg Nojeim, and Ronald Lee, it too is being published in *International Data Privacy Law*.[6] In addition, comparative charts summarizing the country-specific research materials have been made available on the website of the Center for Democracy & Technology.[7]

Systematic Access – Findings to Date

The TPP research and roundtables described above produced several findings:

First, technological developments associated with the digital revolution make it easier than ever for government to collect, store, and process information about individuals on a massive scale. Governments seem to be exploiting these developments and responding to pressing threats such as terrorism as well as more mundane demands of public administration by demanding more data be held by the private sector.

Second, 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 in those nations with otherwise comprehensive data protection laws, access for regulatory, law enforcement, and national security purposes is often excluded from such laws or is authorized under separate laws that may or may not

[4] http://idpl.oxfordjournals.org/content/2/4.toc (2012) and http://idpl.oxfordjournals.org/content/4/1.toc (2014)
[5] http://idpl.oxfordjournals.org/content/2/4/195.full.pdf+html.
[6] A version of the paper is available at https://cdt.org/files/pdfs/govaccess2013/government-access-to-data-comparative-analysis.pdf.
[7] http://govaccess.cdt.info.

provide adequate safeguards against possible abuses.[8] 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.

Third, transparency about systematic surveillance programs is weak, so no one has an accurate or comprehensive understanding of systematic access (even after the Snowden revelations). The relevant laws are at best ambiguous, and government interpretations of them are often hidden or even classified; practices are often opaque (because it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment); and oversight and reporting mechanisms are either absent or limited in scope when they exist and generally do not reach voluntary data sharing.

Fourth, it seems overall there has been relatively little discussion of the complex legal and political issues associated with asserting jurisdiction over data stored in—or relating to citizens of—other countries.[9] As Internet-based services for communications, data storage, and social networking have become globalized, the trans-border implications of governmental demands pose very hard, unresolved challenges. Until the recent disclosures, there had been essentially no discussion of the complex questions raised by trans-border surveillance. Even since the Snowden disclosures, there has been little progress on those issues. 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.

Fifth, while standards for *real-time* interception of communications for law enforcement purposes are high in most of the countries surveyed (the exceptions being 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.

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

---

[8] A study for the European Parliament of 5 European countries concluded that, "in general, legal frameworks are characterized by ambiguity or loopholes as regards large-scale communications surveillance, while national oversight bodies lack the capacity to effectively monitor the lawfulness of intelligence services' large scale interception of data." "National programmes for mass surveillance of personal data in EU member States and their compatibility with EU law," a study for the Directorate General for internal Policies (2013) http://info.publicintelligence.net/EU-MassSurveillance.pdf. The Article 29 Working party recently confirmed this finding with respect to EU Member States: "It becomes clear from assessing the relevant national legislation that the GDPL [general data protection law] in many countries does not apply to the activities of intelligence services. . . . The GDPL, when applicable, generally provides for a number of exemptions (derogations to one or more principles) for the processing of personal data by intelligence services." http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

[9] Illustrating the issue, a federal magistrate in the US recently ordered a US-based company to retrieve and disclose to US authorities data that the US-based company had stored on a server in Ireland. http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398. "Internet & Jurisdiction" is an international multi-stakeholder project seeking to develop principles for jurisdiction in cyberspace. http://www.internetjurisdiction.net/about/ The project's goal is to draft by the end of 2014 a basic due process framework to govern interactions between governments, Internet platforms or operators, and users on the global Internet; at this point, it is not clear how detailed the principles will be with respect to government surveillance.

The Information Accountability Framework

The global accountability project began in 2009 as a dialogue co-facilitated by the Office of the Privacy Commissioner of Ireland and the Centre for Information Policy Leadership at Hunton & Williams LLP. Privacy enforcement agencies, governments, civil society, and business representatives met twice in Dublin, Ireland. The project published "Data Protection Accountability: The Essential Elements" in October 2009, describing five essential elements that are the structural building blocks for accountability-based data governance.[10] The five elements are:

1. Organizational commitment to accountability and adoption of internal policies consistent with external criteria;
2. Mechanisms to put privacy policies into effect, including tools, training and education;
3. Systems for internal ongoing oversight and assurance reviews and external verification;
4. Transparency and mechanisms for individual participation; and
5. Means for remediation and external enforcement.

These essential elements articulate the conditions that must exist in order for an organization to establish, demonstrate, and test its accountability. One has to look at all five essential elements of accountability to determine whether an organization is fully accountable. For private sector organizations to be fully accountable organizations, they must have mechanisms to assure the obligations that are attached to data (no matter the application) travel with the data. This requires different mechanisms in different situations. Sometimes contracts are enough. In other situations, there need to be assurance reviews or audits. No matter the due diligence a company might do, a company cannot be fully accountable unless the entities it provides the data to are accountable as well.

The principle of accountability has been widely endorsed. An important milestone was reached in July 2010 when the Article 29 Working Party issued an opinion on the principle of accountability, proposing a requirement that data controllers put in place appropriate and effective measures to ensure that privacy rules are complied with and to demonstrate compliance to supervisory authorities. The Federal Privacy Commissioner of Canada and the Information Commissioners of Alberta and British Columbia have released a document articulating what data protection authorities would expect of organizations under an accountability approach. The Asia-Pacific Economic Cooperation forum's Cross-Border Privacy Rules adopt an accountability-based code of conduct. Accountability plays a key role in the EU's proposed Data Protection Regulation.

Accountability and Government Access

This brings us, then, to our challenge: If a national security agency obtaining data from a private sector company is ignoring any of the five essential elements, the company providing the data has a gap in its accountability framework, even if the company provides the data under compulsion.[11] (Question for

[10] http://tiaf01.ipower.com/wp-content/uploads/2013/09/The-Essential-Elements-of-Accountability.pdf. The elements of accountability have been fleshed out in a series of guides and tools. See http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF and http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Accountability_Chart_Phase_IV.pdf. Additional materials on accountability are complied at: http://www.informationpolicycentre.com/resources/.

[11] The European Parliament, in its resolution of March 2014 on surveillance, noted that "wide-ranging access by US intelligence agencies to data transferred to the US by Safe-Harbour-certified entities raises additional serious questions as to the continuity

discussion: What is the impact on a company's accountability if its data is accessed not directly, but as it passes between data centers over supposedly trusted communications channels provided by third parties?)

What steps can be taken to fill this gap by companies, regulators, and agencies demanding data from the private sector? Here are some reference points to guide our discussion in Montreal and London.

What Can Companies Do to Remain Accountable in the Face of Government Demands?

Major companies have already made progress in addressing some of aspects of this challenge. Accountable companies have procedures in place to review requests from government agencies, including national security agencies. Under the Global Network Initiative implementation guidelines, it is not sufficient for companies merely to say, "We only comply with lawful demands."[12] The GNI guidelines specify that companies should have in place procedures to carefully assess not only whether a government demand is lawful but also whether it is overbroad or inconsistent with international human rights standards.[13] The guidelines state:

> When required to provide personal information to governmental authorities, participating companies will:
>
> - Narrowly interpret and implement government demands that compromise privacy.
> - Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law, or inconsistent with international human rights laws and standards on privacy.
> - Request clear communications, preferably in writing, that explain the legal basis for government demands for personal information, including the name of the requesting government entity and the name, title, and signature of the authorized official.
> - Require that governments follow established domestic legal processes when they are seeking access to personal information.
> - Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
> - Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that Country.
> - Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies, or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

The obligation to carefully consider government requests may arise in some countries as a matter of law. For example, our country study on South Korea notes that in 2012 the Seoul High Court found that an

---

of protection of the data of EU data subjects."
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

[12] http://globalnetworkinitiative.org/implementationguidelines/index.php.

[13] The Global Network Initiative is a multi-stakeholder collaboration of companies, human rights advocates, investors, and others, working to help Internet companies meet their human rights obligations with respect to privacy and free expression when responding to government demands to disclose customer information or take down or block content.

ISP, facing a government request for disclosure of data under a law that permitted voluntary disclosures, is responsible in every particular case for deciding whether it should provide the requested personal data based upon a careful examination of specific factors such as the seriousness and urgency of the crime, the importance of the public interest, and the degree of infringement on the personal rights of the data subjects.

Transparency is another key aspect of accountability. Transparency in this context concerns both legal authorities and the scope of the government's exercise of those authorities: what types of information is being disclosed to government agencies and under what legal authorities and for what purposes; and how much data, affecting how many customers, is disclosed? Companies are largely at the mercy of national laws and government policy in terms of what they can disclose. Companies in the US have developed transparency reports in which they publish statistical information about the number of government disclosure demands they receive and/or the number of accounts affected, although they remain constrained by some government-imposed limits. [14] After the Snowden leaks, US-based companies sued the US government to obtain permission to disclose more information about national security demands; the case resulted in a settlement that allowed the companies to publish more granular information, within numerical bands.[15] Some companies also publish detailed explanations of what kinds of data they turn over to the government under what kind of legal authority.[16]

It is probably safe to say that, at this point, more detailed data is available in the US about how surveillance powers are used than in many other countries.[17] One recent report suggests, for example, that the transparency of companies in Canada is limited.[18]

On June 11, the Global Network Initiative, CDT, and Google will host a daylong event on transparency in Berlin. The meeting is intended to share experiences and best practices from efforts across the world to shed light on government surveillance (and content restrictions).

What Can Governments Do to Respect Accountability?

While the GNI principles encourage companies to challenge government demands that appear inconsistent with domestic law or procedures or international human rights laws and standards on

---

[14] See Harley Geiger, Two Ways the Surveillance Transparency Rules for Companies Are Not Transparent (March 19, 2014), https://cdt.org/two-ways-the-surveillance-transparency-rules-for-companies-are-not-transparent/.

[15] The announcement from the US Department of Justice (DOJ) regarding the agreement on transparency reporting for national security orders: http://www.justice.gov/opa/pr/2014/January/14-ag-081.html. The details, in a DOJ letter to the companies regarding two options for reporting: http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf. A joint response from the five companies: http://www.microsoft.com/en-us/news/press/2014/jan14/01-27statement.aspx. A *New York Times* summary: http://www.nytimes.com/2014/01/28/business/government-to-allow-technology-companies-to-disclose-more-data-on-surveillance-requests.html.

[16] Apple recently published its internal guidelines for complying with government demands: https://www.apple.com/legal/more-resources/law-enforcement/ ("These Guidelines are provided for use by law enforcement or other government entities in the US when seeking information from Apple Inc.").

[17] UK-based Big Brother Watch has published specific recommendations for transparency in the UK, drawing in part on the US experience. http://www.bigbrotherwatch.org.uk/files/briefings/BBW_transparency_2014.pdf.

[18] http://ixmaps.ca/transparency.php ("No carrier providing internet services directly to Canadians has yet followed the lead of major US internet service providers, such as AT&T, Verizon, Google, Facebook or Twitter, and proactively reports on the frequency of law enforcement requests and how they respond to them.").

privacy and data protection, companies are limited in what they can do. Following the Snowden leaks, there have been calls on both sides of the Atlantic for greater governmental accountability.

In a March 12, 2014 resolution, the European Parliament strongly criticized the US surveillance programs and noted some of the limitations of the US legal and oversight framework, but the Parliament also called on EU Member States to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny, that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency, and that they are in line with the standards of the European Convention on Human Rights and Member States' fundamental rights obligations. The resolution raised the possibility of developing minimum European standards or guidelines for the (*ex ante* and *ex post*) oversight of intelligence services, including criteria on enhanced transparency by governments as to their surveillance practices.[19]

On April 10, 2014, the Article 29 Working Party adopted an opinion on surveillance in which it made specific recommendations that map the principles of accountability:

- EU Member States should ensure greater transparency. Member States should be transparent to the greatest extent possible about their involvement in intelligence data collection and sharing programs, preferably in public, but if necessary at least with their national parliaments and the competent supervisory authorities. This includes transparency as to legal authorities: "these programs have to be based in clear, specific, and accessible legislation."
- Members States should have a coherent legal framework for the intelligence services including rules on data processing in compliance with the data protection principles as laid down in European and international law. The Working Party stated that EU Member States must comply with the conditions Articles 7 and 8 of the ECHR set for their surveillance programs.
- To ensure that no abuse of surveillance programs will happen again, there should be an effective and independent external oversight of the intelligence services, which implies, the Working Party said, a genuine involvement of the data protection authorities. "Effective and independent supervision on the intelligence services," the Working Party said, "including on processing of personal data, is key to ensure that no abuse of these programmes will take place." [20]

Companies, too, are calling for greater governmental accountability, to restore trust. Under the banner of "Reform Government Surveillance," a group of US-based companies has gone one step further and called for specific reforms to government surveillance laws worldwide in ways that relate to the principle of accountability.[21] In particular, the companies have recommended specific limits be built into government surveillance practices:

> … governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications.
>
> Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong

[19] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230. On transparency, the EP specifically cited the "Tshwane Principles." See "The Global Principles on National Security and the Right to Information" (June 2013) http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.
[20] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.
[21] https://www.reformgovernmentsurveillance.com/.

> checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.

The corporate recommendations share common ground with principles for reform of government surveillance laws signed by more than 300 civil society organizations around the world. [22]

Another major recommendation of the Reform Government Surveillance coalition is for greater governmental transparency:

> Transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly.

A broader group of companies and civil society organizations has also called on the US government to expand the transparency of its surveillance practices by regularly disclosing the total number of requests under specific authorities for specific types of data, and the number of individuals affected by each.[23] Individual companies have also called for greater government transparency. For example, when Verizon released its latest transparency report on March 3, in which it published data on National Security Letters, the company noted that it was still limited in what it could publish and it called on the US government to itself be more open: "We once again call on all governments to make public the number of demands they make for customer data from such companies, because that is the only way to provide the public with an accurate data set."

In the US, there have been several steps to restrain government collection. In January 2014, President Obama announced that he intended to end the bulk collection of telephony metadata, a program that that covers both domestic and international calls.[24] As of May 2014, however, the program was still operating, and the bill to end it passed overwhelmingly by the House—with bipartisan support—contained significant exceptions.[25] Also in January, the President issued a policy directive making certain commitments as to how the US government will handle data collected in the national security context.[26] In particular, the directive says that the US government, when it collects signals intelligence data in bulk, will use that data

> only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession,

---

[22] https://en.necessaryandproportionate.org/text. See CDT, "Common Ground Between Company and Civil Society Surveillance Reform Principles" (January 15, 2014), https://cdt.org/files/pdfs/common-ground-surveillance-principles.pdf.

[23] https://cdt.org/insight/we-need-to-know/.

[24] "Remarks by the President on Review of Signals Intelligence," January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence; FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program (March 27, 2014) http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

[25] "Gutted USA FREEDOM Act Passes," Center for Democracy and Technology Insight, May 21, 2014, https://cdt.org/insight/house-leadership-moves-to-gut-usa-freedom-act/.

[26] http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

> proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

The directive goes on to say "In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to US companies and US business sectors commercially; or achieving any purpose other than those identified in this section."

These use limits apply to data regarding any persons, "whatever their nationality and regardless of where they might reside."

In April, senior US officials issued a major policy review document on "big data." The report did not focus on national security surveillance (leaving that to other policy processes set in motion by the President's January directive), but it did address both administrative and law enforcement uses of big data by government. Moreover, it explicitly recognized the global implications of global data flows and the global impact of US practices. It stated, "Privacy is a worldwide value that the United States respects and which should be reflected in how it handles data regarding all persons." The report recommended eliminating or reducing distinctions between privacy protections afforded citizens and non-citizens with respect to all other US government data collection and use activities.[27] The report is likely to guide development of privacy policy for the remainder of President Obama's administration.

Pending International Efforts to Examine and Reform Government Surveillance and Data Access Practices

UN Special rapporteur Frank LaRue, in a very prescient report issued in 2013 before the Snowden revelations, warned of burgeoning government surveillance worldwide:

> Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted, and broad-scale surveillance than ever before.

LaRue found that "Generally, legislation has not kept pace with the changes in technology. In most States, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment." LaRue made several concrete recommendations to improve government practices in ways that would give assurance to private sector entities and their customers:

> The provision of communications data by the private sector to States should be sufficiently regulated to ensure that individuals' human rights are prioritized at all times. Access to communications data held by domestic corporate actors should only be

[27] "Big Data: Seizing Opportunities, Preserving Values" (May 2014) at p. 60 http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (recommending applying the Privacy Act of 1974 to non-US persons where practicable or establishing alternative privacy policies that apply appropriate and meaningful protections to personal information regardless of a person's nationality).

> sought in circumstances where other available less invasive techniques have been exhausted.
>
> The provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism.

LaRue called on governments to update and strengthen laws regulating government surveillance. Among other elements, he recommended:

> Legal frameworks must ensure that communications surveillance measures:
>
> (a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;
> (b) Are strictly and demonstrably necessary to achieve a legitimate aim; and
> (c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

In response to the LaRue report and the Snowden revelations, the UN General Assembly adopted resolution 68/167,[28] requesting that the Office of the High Commissioner for Human Rights (OHCHR) prepare a report on the right to privacy in the digital age.[29] The OHCHR is to examine, in the words of the resolution: "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale." The report will be presented later this year to the Human Rights Council and to the General Assembly. To prepare this report, OHCHR has encouraged all interested parties to share information and perspectives on the issues raised.

Other pending efforts include:

- The Article 29 Working Party announced that it intends to organize a conference on surveillance in the second half of 2014 bringing together all relevant stakeholders.
- The Freedom Online Coalition, currently comprising 23 governments, has a Working Group on Privacy and Transparency online, which is developing recommendations likely to touch on the relationship between businesses and governments with respect to surveillance. First findings of the Working Group will be presented at the Internet Governance Forum in September 2014, with the final outcome presented at the next FOC conference in Mongolia in spring 2015.[30]
- Several work streams called for by the European Parliament in its March 2014 resolution.

A case pending before the European Court of Human Rights challenging the UK's surveillance practices may also produce further limits on government data collection and use. Already, the cases of the ECtHR constitute perhaps the fullest body of international law on government surveillance. The earlier TPP research identified certain basic criteria that the ECtHR has articulated in assessing government access programs (although recent revelations make it is clear that these criteria are not uniformly adhered to). These may provide reference points in assessing government accountability:

---

[28] http://undocs.org/A/RES/68/167.
[29] See http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.
[30] https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-3/.

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 the 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? (This question gets to the core of whether systematic access is clearly authorized or not.)
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 the 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 is not searched or used?
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?[31]

[31] Douwe Korff, professor of international law at London Metropolitan University, has identified a similar list of criteria. See Korff, D., "Note on European and International Law on Transnational Surveillance prepared for the Civil Liberties Committee of the European Parliament" (23 August 2013),

Questions for Discussion – Mapping the Accountability Framework to Government Access Programs

Can the five essential elements of accountability be transposed into the governmental context? Without trying to be comprehensive now, here are some thoughts:

1. ***Organization commitment to accountability and adoption of internal policies consistent with external criteria.***

When applied to a government data processing program, this element may pose squarely the question of how adequate are the external criteria (that is, the law authorizing government demands). The formulation used by the ECtHR is that a law must describe a governmental power precisely enough to protect against arbitrary application and to inform the public of which entities can conduct surveillance and under what criteria.

2. ***Mechanisms to put privacy policies into effect, including tools, training and education.***

"Tools" suggests use of audit trails, documentation, and permissioning systems for internal access and query. Further elaboration on the essential elements conducted in Paris, Madrid, Brussels, Warsaw, and Toronto suggests processes that assess the risks to individuals associated with new processing (including collection), and that mitigating those risks be part of the final processing plan. Such privacy by design practices should be part of an agency's comprehensive privacy program. Training should probably start with an understanding of privacy and data protection, since the terms, although widely used, are often misunderstood.

3. ***Systems for internal ongoing oversight and assurance reviews and external verification.***

The Article 29 Working Party has specifically called for more meaningful oversight of intelligence agency programs involving collection and use of personal data. It said in its April opinion that the following good practices from the various oversight mechanisms currently in place in Member States should be part of the oversight mechanisms in all Member States:

- Strong internal checks for compliance with the national legal framework in order to ensure accountability and transparency;
- Effective parliamentary scrutiny; and
- Effective, robust, and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself, having power to access data and other relevant documentation as well as an obligation to inspect following complaints.

---

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf.

4. Transparency and mechanisms for individual participation.

As discussed above, transparency means both public awareness of what data is being accessed as well as numerical reporting to indicate the scope of government access. The Article 29 Working Party stated: "Some form of general reporting on surveillance activities should be in place."[32]

5. Means for remediation and external enforcement.

Remediation can mean judicial redress. In the US, the legal (and constitutionally-based) doctrine of "standing" and the states secret doctrine make it very hard to challenge national security surveillance in court. The ECtHR has a much broader definition of standing, which might be a model.

[32] The Working Party cited the decision of the ECtHR in Youth Initiative for Human Rights v. Serbia (25 June 2013).