

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 10, Number 10

October 2010

Accountability: Part Of The International Public Dialogue About Privacy Governance

By Paula J. Bruening, Centre for Information Policy Leadership at Hunton & Williams LLP, Washington.

Dramatic advances in the speed, volume and complexity of data flows challenge existing models of data protection. Powerful analytics yield deeply insightful, real-time inferences about computer users that enhance the online experience and enable companies to offer products and services to the right individual at the right time. Behavioral targeting uses a complex network of vendors to track and analyze an individual's online activity to serve tailored, more effective advertising. Organizations collect and derive data about individuals from myriad sources and often employ service vendors located halfway around the world to carry out internal business processes and provide around-the-clock customer service. Using technologies ranging from surveillance cameras to radio frequency identification, they gather and store data cheaply, often in the cloud, where servers may be located on another continent. And given the rapid pace of development, an organization's impulse to retain that information for future, as yet unanticipated, uses is understandable and often makes good business sense.

The growing power of data holds the promise of economic benefit for businesses and consumers. But to realize that potential, consumers must be confident that their information is used responsibly, and that their privacy is protected. Over the last 18 months, policy-

makers around the world have undertaken efforts to examine and update data governance in a way that would better serve this rapidly changing data environment, providing the best possible privacy protection while encouraging innovation and flexible data use. While policymakers continue to cite traditional principles of fair information practice as relevant and the foundation of good privacy and data protection, they recognize the challenges new technologies and business models pose to the application of those principles.

Data protection that relies primarily on notice and choice has come under particular scrutiny. In a notice-and-choice model, consumers receive information about how an organization will collect, use, and share data about them. On the basis of this notification, consumers choose whether to allow its use. Such a model is seriously challenged by an environment in which organizations can analyze and process information instantaneously at the collection point, and where data collection has become so ubiquitous that individuals could easily be overwhelmed by the privacy notices they receive each day as they shop online, use a mobile communications device, engage in social networking, or visit a building that uses surveillance cameras or sensor technology. In many cases, it is impossible to provide notice, and even when it is, notices are lengthy and complex. Given that data use is necessary for so many activities, both online and offline, choice itself

may be possible and provide real guidance for organizations about how to use information only in limited circumstances.

Accountability requires an organization to remain accountable no matter where or by whom the information is processed.

Faced with these challenges, policymakers are asking a number of questions. How best to protect the privacy of individuals, even when choice is not meaningful or in some instances not possible? How to encourage the innovation in data use that encourages economic growth and still safeguard individuals' interests in the protection and responsible use of their data? For possible answers, policymakers have turned their attention to the fair information practice principle of *accountability*.

Accountability as a principle of data protection is not new. It was first articulated in 1980 as a principle of fair information practices in the Organization for Economic Cooperation and Development's (OECD) privacy guidelines.¹ The accountability principle places responsibility on organizations as data controllers "for complying with measures that give effect" to all eight of the OECD guidelines' principles.

Accountability is also fundamental to privacy protection in the European Union. While not explicitly articulated in the EU Data Protection Directive (95/46/EC), numerous provisions require that organizations implement processes that assess how much data to collect, whether the data may be appropriate for a specified purpose and the level of protection necessary to ensure that it is secure. It is the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),² which requires that Canadian organizations implement the full complement of PIPEDA principles, whether the data are processed by the organization or outside vendors, or within or outside Canada. In the United States, accountability underpins the security requirements of the Gramm-Leach-Bliley Act, which requires that organizations secure their data holdings against theft, loss or unauthorized access, but leaves to their discretion the most effective way to do so.

Accountability Project

Until now, the principle of accountability has often gone undefined, and it has been unclear what conditions organizations must create to establish and demonstrate their accountability. As it has begun to play an increasingly visible role in privacy governance, an international group of experts — including business leaders, data protection authorities, advocates, and government representatives — have convened the Accountability Project. Organized by the Centre for Information Policy Leadership, the Accountability Project seeks to define the contours of accountability, to articulate how it is demonstrated and measured, and to establish why individuals should trust it to protect their data. Their work began as

an inquiry into the essential elements of accountability in early 2009, and will continue into 2011 to more concretely define the fundamentals that characterize the accountable organization.

According to the Project, accountability is designed to provide robust protections for data while avoiding aspects of current data protection that may be of limited effect or that may burden organizations without yielding commensurate privacy benefits. Accountability allows the organization greater flexibility to adapt its data practices to serve emerging business models and technologies and to meet consumer demand. In exchange, it requires that the organization commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure those policies are carried out in a way that protects information and the individuals to which it pertains.

Accountability requires an organization to remain accountable no matter where or by whom the information is processed. An accountability-based approach to data governance focuses on setting privacy-protection goals for organizations based on criteria established in current public policy and allowing organizations discretion in determining how those goals are met. Accountable organizations will adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the demands of their customers.

The essential elements of accountability are:

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

An organization demonstrates its willingness and ability to be responsible and answerable for its data practices. Its practices are based on policies consistent with appropriate external criteria — applicable law, generally accepted principles, and/or industry best practices. Practices are designed to provide the individual with effective privacy protection.

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

The accountable organization deploys and monitors mechanisms and internal programs that ensure its privacy policies are carried out. Mechanisms may include tools to facilitate decision making about data use and protection, training about how to use those tools and processes to ensure employee compliance.

3) Systems for internal, ongoing oversight and assurance reviews and external verification

The organization monitors and assesses whether its internal policies manage, protect and secure data effectively. Risk analysis appropriate to the organization and the industry in which it functions is key to successful monitoring and risk management. The accountable organization engages, as appropriate, an independent entity to verify and demonstrate that it meets the requirements of accountability.

4) Transparency and mechanisms for individual participation

Accountability requires transparency. The accountable organization effectively communicates to indi-

viduals critical information about its data procedures and protections in a posted privacy notice. When appropriate, the information in the privacy notice can provide the basis for the consumer's consent or choice. Individuals should be able to see the data or types of data that the organization collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. In some cases, however, public policy reasons will limit that disclosure.

5) Means for remediation and external enforcement

The accountable organization establishes a means to address harm to individuals caused by the failure of internal policies and practices. When harm occurs due to a failure of an organization's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. The organization should identify an individual to serve as the first point of contact for resolution of disputes and establish a process to review and address complaints.³

Developers envision the ability of an accountability approach to improve data protection in several ways. Ideally, accountability will:

- help organizations improve the quality of data protection by allowing them to use tools that best respond to specific risks and to rapidly update those tools to respond quickly to new business models and emerging technologies;
- enable organizations to better deploy scarce resources allocated to privacy protection. Resources devoted to administrative requirements such as notification of data authorities of minor changes in processing can be redirected to more effective protection measures that most effectively safeguard data;
- heighten the confidence of individuals that their data will be protected wherever it is stored or processed; and
- bridge data protection regimes across jurisdictions, but allow countries to pursue common data protection objectives through very different but equally reliable means.

Accountability does not preclude application of principles of fair information practices. It does relieve the individual of much of the burden of policing the marketplace for organizations using data irresponsibly. Faced with rapid advances in data analytics and increasingly complex technologies, business models and vendor relationships, consumers find it increasingly difficult to make well-informed privacy decisions, even when they can access privacy policies. In an accountability model, when the consumer can provide meaningful consent, the organization is required to act based on that consent. But even when the consumer cannot, accountability demands responsible, disciplined data storage, use and protection.

Factor in International Discussions

Accountability has begun to figure prominently in ongoing discussions about effective data protection.

Accountability has come under close review in the European Union. The Article 29 Working Party launched a consultation on the EU data protection legal framework and determined that the level of data protection in the European Union could benefit from better application of existing data protection principles in practice. In an article released in December 2009 entitled "The Future of Privacy,"⁴ the Article 29 Data Protection Working Party and the Working Party on Policy and Justice noted that, while traditional principles of data protection remain valid, new technologies and the global flow of data present new challenges to data protection. They characterized the new challenges as an opportunity to, among other things, introduce additional principles, including accountability. It also noted the need to strengthen the effectiveness of the current system through modernization, citing particularly the need to reduce bureaucratic burdens.

In July 2010, the Article 29 Working Party released an opinion focusing specifically on accountability⁵ (*see analysis in this issue*). According to the opinion, a principle of accountability "would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the [Data Protection] Directive and demonstrate this on request." The Working Party's objective is to "encourage data protection in practice" by requiring data controllers to engage in risk assessment and adopt measures such as:

- data loss/breach detection/prevention policies and procedures;
- "Privacy by Design" in the development and implementation of new technologies;
- binding policies and procedures that measure compliance; and
- response plans that draw on the organization's experience, mitigate harm and discourage future breaches.

At the Asia-Pacific Economic Cooperation, the Privacy Framework⁶ depends upon accountability to facilitate cross-border data flows. In language similar to that in the OECD Guidelines, the APEC Framework provides that "[a] personal information controller should be accountable for complying with measures that give effect to the Principles stated above."

The Framework commentary specifically discusses accountability in the context of information transfers between different types of organizations, in different locations. It states that controllers should be accountable for ensuring that the recipient of the information will protect it in accordance with the Framework principles. Under the APEC Framework, controllers are accountable for protection of the data even after it is transferred for processing or storage. The requirement assumes that the controller will conduct due diligence to ensure that the recipient is able and committed to fulfilling the obligations to manage and protect the data appropriately.

Finally, the proposed "International Standards on the Protection of Personal Data and Privacy" that are the subject of the Madrid Resolution⁷ also incorporate the

principle of accountability. The principle recognizes both the obligation to observe all of the principles and obligations in the proposed standard, and takes the additional step to require that organizations implement mechanisms and be able to demonstrate their compliance.

Summary

Accountability has become part of the international public dialogue about privacy governance. But to be an effective, credible solution to the privacy issues raised by 21st century data use, it will be necessary to establish the fundamentals that would make an accountability model work in practice.

The Accountability Project is engaged in additional collaborative work to explore the practical questions related to implementing and administering an accountability approach. What must an organization demonstrate to be deemed accountable? How is accountability measured? What triggers an accountability review? How will remediation work in an accountability approach?

Resolution of these and other questions by international policymakers, business, experts and advocates will be critical to accountability's successful adoption as an innovative, effective approach to privacy and data protection.

NOTES

¹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

² <http://laws.justice.gc.ca/en/P-8.6/>

³ For a more comprehensive discussion of accountability, see "Data Protection Accountability: A Document for Discussion," October 2009, <http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf>.

⁴ "The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data." 02356/09EN/ WP 168, December 1, 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

⁵ Opinion 3/2010 on the principle of accountability, July 13, 2010, Article 29 Data Protection Working Party, 00062/10/EN – WP 173, para. 5. http://www.cbpreweb.nl/downloads_int/wp173_en.pdf.

⁶ The APEC Privacy Framework, published 2005, <http://op.bna.com/pl.nsf/r?Open=byul-89js2b>

⁷ "Internacional Standards on the Protection of Personal Data and Privacy: The Madrid Resolution," released October 2009, <http://www.gov.im/lib/docs/odps//madridresolutionnov09.pdf>.

Paula J. Bruening is Deputy Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP in Washington. She may be contacted at pbruening@hunton.com.