Cross-Border Data Flows and Increased Enforcement

Peter McLaughlin
Foley & Lardner LLP

The term "privacy" is subject to many definitions and descriptions. According to Jim Harper of the Cato Institute, "Properly defined, privacy is the subjective condition people experience when they have the power to control information about themselves and when they exercise that power consistent with their interests and values."[1] Regardless of whether we agree with Harper about the precise phrasing, the definition he posits reflects internationally accepted ideas that the collection, use, sharing, and protection of personal information should be subject to some degree of informed notice to and consent from the affected individual. (For more on this, see the "For further reading" sidebar.) The EU Data Protection Directive takes a somewhat different tack and defines personal data as data relating to an identified or identifiable individual, and then allocates a series of rights to the individual regarding the data, particularly regarding notice, consent, and other principles intended to grant an individual reasonable control over the data relating to him or her. (For more on the directive, see http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.)

Agreement in principle, however, doesn't mean agreement in detail. While companies, search engines, Web sites, and governments collect ever-increasing amounts of personal information, the world's national data protection agencies (DPAs) continue to implement relatively common principles in markedly different ways. (I use DPA as a generic reference to governmental regulators, such as the Information Commissioner's Office [UK], the Office of the Privacy Commissioner [Australia], or the Commission nationale de l'informatique et des libertés [CNIL] in France.) The problem that confronts all involved, from consumers to companies to regulators, is that although principles might be regional or even global, implementation—and thus enforcement—continues to be highly localized. And because the flow of personal information is increasingly global and DPAs wish to protect their citizens, enforcement at a local or national level will impact these data flows more significantly than in the past because of the complexity of complying with so many inconsistent rules. The concern for companies should be that compliance is only going to become more complex and difficult because there's little genuine incentive for government authorities to work toward a consistent standard and enforcement will only increase.

Personal information flows are increasingly international

An increasing number of companies have facilities and employees around the globe, and even those companies located in a single country often have sales from abroad. The ascendance of Google, Yahoo, MySpace, and other Internet-focused firms means that peer-to-peer networks, search engines, social networks, and Internet advertising are moving customer data across national borders and time zones with astonishing speed.

Consider a publicly listed healthcare company based in the US but with operations in 30 countries. The company collects the familiar range of employee data in each country. It has a common set of corporate email address lists on servers around the world, and a corporate "look up" in their computer and phone systems so that employees can contact one another. Employees across borders work together on such projects as virtual teams, whether they work for the same business unit to develop a new product or they work across business units and with core "functions" such as legal, marketing, and HR. IT and HR would like to consolidate the 105 Excel spreadsheets across 34 countries resulting from 11 acquisitions into a single, global database. Although the company has little direct consumer interaction, it frequently supports drug trial operations—it prepares drugs on an individual basis for people it knows only by an anonymous series of numbers. Finally, the company also produces a limited number of medical devices that it sells to hospitals and

clinics around the world and for which it is sometimes necessary to provide remote technical support. Much of their services can be outsourced to a third party.

The enterprise I just described isn't uncommon in the way it wants to move data or the consolidation desired to improve operations. The challenge is that all 27 European Union countries, plus Canada, Japan, Australia, Argentina, and several others, require various combinations of national registrations, regulatory permission, or operational changes to achieve the basic business goals of moving company data to where it needs to be. And each DPA is, like the US Federal Trade Commission, tasked with protecting the interests of its stakeholders, typically citizens with personal data collected by these myriad firms. This gives rise to a local (that is, national) focus on personal information that flows rapidly across national boundaries.

Now consider a younger firm that operates predominantly via the Internet. Perhaps it provides search services and advertising; perhaps it enables distant recruiting or friendships or multiplayer gaming, or the sharing of legally duplicated music or films. Assuming that any of these firms has headquarters in the US, each doubtless collects memberships from and information about any number of people from outside the US. Servers around the world cache and distribute data upon request, the operation of which is only vaguely understood by the firm's customers and perhaps to a similar extent by regulators.

Whether a company is "old economy" or "new," most data flows are intended to be predictable and structured so that queries and data fields are manageable. Unfortunately, US civil litigation discovery rules do not fit that model—you can submit predictable data flows within a regulatory filing and to an individual for consent, but litigation is less predictable and more contentious. Recent modifications to the US Federal Rules of Civil Procedure make clear that the familiar requirements of collecting, preserving, and producing all relevant records now apply squarely to electronically stored information. High-profile cases are an incentive for any litigant to produce what the opponent (and typically the court order) demands.

If we recall the definition of personal data under the EU Directive, though—any data relating to an identified or identifiable person—then it's easier to see how a company with European employees subject to a litigation hold and discovery request can be caught between the demands of a US judge and one or more European DPAs. The Word document I generate at work contains data about me: document creator, modifier, time created, number of modifications, and so on. That data relates to me and the fact and accuracy of that data could be relevant to litigation in the US. Notwithstanding the likelihood that my employer "owns" the document, that I generated the document on company time, and did so through the use of company equipment, under EU privacy law, I might well have a recognizable assertion of a privacy right in the document's metadata. Recipients of the discovery request then find themselves in the suboptimal position of flouting a court's discovery order or the privacy regulations of a country host to perhaps significant operations.

All of which brings us back to privacy, "properly defined" according to Harper, because whether I am a customer, an employee, or an advertising recipient, I have some idea of how I would like information about me to be handled, depending on the context. An individual's privacy rights, though, are largely reliant on applicable law, most of which dates from 2000, 1995, or earlier. A disconnect has arisen, then, because many of the data protection laws were conceived and promulgated without the benefit of today's perspective of information services, data-collecting products, and consolidated employee databases. Regulators, then, see a need to acquire broader enforcement authority and more current legislation to protect their constituents.

Regulators are seeking enhanced powers

Although it was possible to move personal data across borders 10, 15, and even 20 years ago, the flows' nature and scope are now significantly wider. So, privacy regulators are seeking broader mandates to monitor and regulate the collection, use, and sharing of this data by companies and governments in ways that reflect current data flows.

The EU has a data protection supervisor, who is responsible for ensuring consistency of EU Member States' implementation of the EU Data Protection Directive as well as reviewing the manner in which EU institutions handle personal information. In January 2008, this supervisor, Peter Hustinx, stated that data protection enforcement would significantly accelerate in Europe over the coming 24 to 36 months. He also noted that his office was actively engaged to improve the consistency and quality of enforcement by the Member States, in part by encouraging more consistency among the implementing laws. "The stakes will be rising. We need to stimulate much better compliance" with the directive, he said. Furthermore, in recognition of the rapid changes in technology and business practices, Hustinx stated that privacy "is becoming a more

and more relevant issue [in the] digital environment."[2]

Within the EU, the UK has sometimes been regarded as less rigorous than other, continental DPAs. Whether this is fair, the UK has experienced several major data breaches by government and private sector organizations. This brought the UK DPA to recently demand modifications to UK privacy laws so that a significant breach of the UK's Data Protection Act 1998 is potentially subject to criminal penalties.

The UK DPA has also requested changes to its enforcement authority, specifically,

- criminal penalties for those who knowingly or recklessly fail to comply with the privacy law;
- a duty to notify DPAs of data breaches;
- the power to require an independent audit or review of an organization's compliance; and
- a requirement for CEOs to certify their data protection practices, analogous to the Sarbanes-Oxley Section 404 certifications in the US relating to financial controls.[3]

In Europe, then, we see signs of more stringent laws sought and enhanced enforcement penalties planned for miscreants or companies that fail to adequately protect personal data in their trust.

From a US perspective, Canada represents a less demanding environment, with fewer regulatory filings and a principle of accountability so that the party originally collecting the personal information is responsible for ensuring its proper treatment down the line. But Canada, too, is considering data breach amendments to its private sector rules. The Canadian Privacy Commissioner, Jennifer Stoddart, delivered to Canada's House of Commons a report urging the federal government to overhaul the Privacy Act, which governs how the Canadian federal government collects, retains, and uses personal information, and thus Canada is moving forward with a series of reforms to the government-applicable Privacy Act.[4]

In the East, the Australian Law Reform Commission initiated in August 2008 a top-to-bottom review of the country's privacy and confidentiality laws, particularly as these apply to data sharing among government agencies for national security (www.alrc.gov.au/inquiries/index.htm). Nearby in New Zealand, the government has proposed significant changes to the Privacy Act 1993, in the form of a Privacy (Cross-border Information) Amendment Bill, which was introduced in July 2008 (www.parliament.nz/en-NZ/PubRes/Research/BillsDigests/a/e/a/48PLLawBD16301-Privacy-Cross-border-Information-Amendment-Bill-2008.htm).

The New Zealand legislation is interesting in part because, first, it removes any residence restriction on who can submit an information privacy request, and second, it establishes "a mechanism for controlling the transfer of information outside of New Zealand where the information has been routed through New Zealand to circumvent the privacy laws of the country from where the information originated." This statement in the legislation's purpose clause reflects the fact that many countries won't permit personal data within their boundaries to flow to a jurisdiction without equivalent protections. We might infer that entities had been locating operations and computer servers in New Zealand to benefit from a more flexible regulatory regime.

Similarly, the Privacy Commissioner for Hong Kong, Roderick Woo, reiterated in May 2008 his request that the Hong Kong government strengthen the Personal Data Ordinance. Woo's office originally submitted more than 50 recommendations in 2006 (www.pcpd.org.hk/english/infocentre/press_20080522.html).

Business is global, politics is local

Companies operating on any international scale now confront an increasingly complex environment. Firms try to meet the inconsistent demands of different masters because customer requirements or operational efficiencies seek broader, faster information, search results, job data, Facebook updates, or performance review summaries. Meanwhile, national DPAs recognize that their laws and regulations rarely fit well with today's information flows, might not grant citizens sufficient rights given the technical changes, and could result in the DPA being undermined as a protector. Business, then, is trying to operate globally while national regulators focus on imposing national rules with increasing rigor—sometimes with international cooperation on the enforcement side.

Certain DPAs, notably the French CNIL and DPAs in Spain, Hungary, Poland, and the Czech Republic, have been conducting unannounced audits and compliance checks, not unlike the "dawn raids" by other regulatory agencies.[5]

European DPAs have threatened for some time that enforcement of the Data Protection Directive would become more aggressive, perhaps in part because the directive's effectiveness dates back to 1998 (http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm). Although it might have been appropriate to be lenient then, 10 years on, there's less willingness to accept excuses from companies that have made little progress or effort toward compliance with the privacy or data protection laws in countries where they do business. This is an example of privacy regulators adapting the interpretation of current rules to a new technology. Such an interpretation isn't

nefarious per se, but there was little in the precedent to indicate to search engine companies that they would be so governed.

US litigation and the discovery rules have received a great deal of press on both sides of the Atlantic through 2008. For example, in the closing months of 2007, the France's CNIL reported that nearly a dozen French companies and European subsidiaries of American firms had contacted it asking whether litigation-related data transfers to the US were legal under French privacy law.[6] Alex Turk, the chairman of the Article 29 Working Party, has asserted that "We need to find a common legal language on the transfer of personal data, and companies' internal rules on data. …. We have to address the problem of trial discovery. … European countries are being forced to comply with U.S. law [and] there are very large legal questions attached to this."[7]

The challenge that faces any company buying, selling, operating internationally, or even with an Internet presence is that the privacy interests of employees, customers, and others will be increasingly visible. Here, I've tried to highlight that both the corporate and regulatory view have increasingly difficult positions to reconcile: companies (assuming good faith and good intentions) want the data to move so they can conduct business; regulators want to fulfill their mandate to protect the privacy rights of their citizens as granted under national law. The data protection principles are relatively global, but implementation is local—with the increased visibility of international data movement, data breaches, and regulatory fines, the enforcement is likely to only increase. □

Acknowledgments

The views expressed in this article are the author's own and do not necessarily reflect the views of Foley & Lardner LLP or any of the firm's clients.

For further reading

Below are just a few of the core documents addressing international privacy standards. While they hold common principles, the similarities end there:

- "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"; www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
- "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," *Official J. European Communities*; no. L. 281, 1995, p. 31; http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.
- "Personal Information Protection and Electronic Documents Act," 2000, c. 5; www.privcom.gc.ca/legislation/02_06_01_e.asp.
- "Businesses Decry EU Data 'Overprotection'; Hustinx Says BCRs Best Route for Transfers," *BNA Privacy & Security Law Report*, vol. 7, no. 22, 2008, p. 819.
- "EU Privacy Official Hustinx Says to Expect Hike in Data Protection Enforcement Levels," *BNA Privacy & Security Law Report*, vol. 7, no. 5, 2008, p. 157.

References

1. J. Harper, "Understanding Privacy and the Real Threats to It," *Policy Analysis*, no. 520, Aug. 2004; www.cato.org/pubs/pas/pa520.pdf.
2. "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the Follow-Up of the Work Programme for Better Implementation of the Data Protection Directive," Opinion 2007/C 255/1, *Official J. European Union*, Oct. 2007; www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf .
3. "Data Protection Powers and Penalties: The Case for Amending the Data Protection Act 1998," UK Information Commissioner's Office, Dec. 2007; www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf.
4. Proposed Immediate Changes to the Privacy Act, Office of the Privacy Commissioner of Canada, 29 Apr. 2008; www.privcom.gc.ca/parl/2008/parl_080429_02_e.asp.
5. "What a Difference a Few Months Make: A Changing Landscape for EU Data Protection Enforcement," *BNA Privacy & Security Law Report*, vol. 7, no. 12, 2008, p. 439.
6. "Growing Litigation Data Transfers to U.S. Troubles French Data Protection Authority," *BNA Privacy & Security Law Report*, vol. 7, no. 3, 2008, p. 96.
7. "French Data Privacy Chief Is Elected to Lead Article 29 Working Party, Discusses Priorities" *BNA Privacy & Security Law Report*, vol. 7, no. 8, 2008, p. 247.

Peter McLaughlin *is senior counsel with the law firm of Foley & Lardner LLP. He is a Certified Information Privacy Professional by the International Association of Privacy Professionals, and is formerly assistant general counsel and global privacy leader of a Fortune 20 company. He graduated with a JD from Georgetown University Law Center. Contact him at pmclaughlin@foley.com.*

Interested in writing for this department? Please contact editors E. Michael Power (michael.power@ssha.on.ca) and Roland L. Trope (roland.trope@verizon.net).