The Shifting Sands of Data Protection and Resulting Privacy Pitfalls

By: Lisa J. Sotto, Aaron P. Simpson and Melinda L. McLellan[1]

With privacy law around the world changing at a dizzying pace, now more than ever vigilance is key for businesses that rely on their robust use of data to thrive in the global economy. Keeping up-to-date on new and revised privacy laws that affect all industry sectors is essential not only to help ensure legal compliance, but to maintain a competitive edge in the marketplace. Proactive attention to the changing legal landscape helps forward-thinking companies avoid potential pitfalls and gives them an advantage over competitors.

The past year has seen a remarkable amount of movement in the privacy and information security arena. In late 2010, the U.S. Federal Trade Commission (FTC) and Department of Commerce issued game-changing policy reports focusing on privacy and information security issues, and six prominent privacy bills have been introduced in Congress since May 2010, in addition to President Obama's recent cybersecurity legislative proposal. Across the pond, the EU Data Protection Directive that was first issued in 1995 is being reviewed for a serious overhaul, and EU Member States are working to implement the EU directive addressing privacy and security concerns associated with the use of cookies to track Internet behavior. The UK has implemented the cookie directive and will require organizations to obtain opt-in consent from website visitors prior to placing certain types of cookies on visitors' hard drives. Elsewhere in the world, Mexico's data protection law came into effect in July 2010, and South Korea enacted a robust privacy protection law in March 2011, to name just two examples.

Given that data generally cannot be confined to a particular jurisdiction, and may, in fact, reside in numerous countries at once, often it is difficult to determine which country's laws apply to a company's data or to the processing carried out with respect to that data. Although multinational groups are making efforts to harmonize global standards, such as the International Standards Organization's Privacy Standards and the Asia-Pacific Economic Cooperation's Privacy Framework, the formalization of such harmonized regulations likely will take years and probably will never replace many national laws and regulations.

In this complex and rapidly-evolving regulatory environment, a thoughtful and informed approach is essential. This article provides in-house counsel with an overview of recent changes to privacy and information security law around the world.

Patchwork of U.S. Laws

Unlike the European Union, Canada, and a number of other countries around the world, the United States does not have an overarching privacy law regime. The U.S. takes a sectoral approach to regulating privacy with more than ten federal privacy laws (and hundreds of state laws) oriented at particular industries or categories of information. On the federal level these laws cover, for example, health privacy (HIPAA), information maintained by financial institutions (GLBA), and children's data collected online for marketing purposes (COPPA). In addition, there are numerous industry-specific self-regulatory regimes such as the Payment Card Industry Data Security Standard, which applies to entities that process payment card transactions and requires them to protect the cardholder data they use. There is no uniform definition of "personal information" in the U.S., so the term varies from law to law. This segmented system may soon shift, however, as federal laws have been proposed that would harmonize the treatment of personal data to some

[1] Lisa J. Sotto and Aaron P. Simpson are partners in the privacy and information management practice of Hunton & Williams LLP in the New York office. Melinda L. McLellan is an associate with the firm in the privacy and information management practice in New York.

extent, and certain federal government agencies have issued reports indicating a need for more comprehensive, cohesive regulation.

U.S. Policy Landscape and Privacy Legislation

In December 2010, the FTC issued a report entitled *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*. The report proposed "a new normative framework for privacy," focusing on themes of simplified privacy choices for consumers and greater transparency on the part of companies that collect and use consumers' personal information. The FTC's report discusses the possibility of instituting a "do-not-track" mechanism that would allow consumers to opt out of companies tracking their behavior online. Notably, the FTC's proposed framework applies to "to all commercial entities that collect consumer data in both offline and online contexts, regardless of whether such entities interact directly with consumers." Its scope goes beyond personal information to cover information related not only to individuals but to computers and other devices as well.

Also in December 2010, the U.S. Department of Commerce issued a Green Paper addressing privacy and information security issues, entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*. The Green Paper included a comprehensive, revitalized set of Fair Information Practice Principles "to protect the privacy of personal information in commercial contexts not covered by an existing sectoral law." It also outlined voluntary, enforceable privacy codes of conduct that leverage innovation and expertise in the private sector to develop trustworthy privacy practices and flexible rules that can "evolve with new technologies and business models." The Green Paper discusses increased global interoperability of privacy frameworks and the creation of a Privacy Policy Office at the Department of Commerce, and recommended the development of a federal commercial data security breach notification law to harmonize the differences among the 46 state data breach notification laws currently in effect in the United States.

With respect to new legislation, privacy has been a hot topic at both the state and federal levels in the past year. In 2011 alone, multiple, prominent bills have been proposed in the U.S. Senate and House of Representatives.

- Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the Commercial Privacy Bill of Rights Act of 2011
- Representative Cliff Stearns (R-FL) introduced the Consumer Privacy Protection Act of 2011
- Representative Bobby Rush (D-IL) re-introduced the BEST PRACTICES Act he originally introduced in the summer of 2010
- Representative Jackie Speier (D-CA) introduced the Financial Information Privacy Act and the Do Not Track Me Online Act
- Senator Jay Rockefeller (D-WV) introduced the Do-Not-Track Online Act of 2011

The Kerry-McCain bill has garnered significant attention due to the prominence of its bipartisan sponsors. At a high level, the Kerry-McCain bill imposes direct requirements on companies with respect to data collection and retention, and grants broad rulemaking authority to the FTC to develop regulations with respect to the collection or use of "covered information." Choosing to regulate "covered" information, as opposed to "personal" information, is significant; the law reaches beyond data that can identify an individual to also apply to data that identifies a computer (such as an IP address). The bill is comprehensive in scope and includes many key elements, such as requirements related to data minimization, data sharing, data integrity, information security, accountability, privacy by design, notice, consent (for behavioral advertising, sensitive information, and unauthorized uses of covered information), access, and the rights of individuals to request that their information be anonymized in certain circumstances.

The bill also contains an important preemption provision indicating that it will supersede state law provisions that pertain to the collection, use or disclosure of covered information or personally identifiable information. Because the bill authorizes the FTC to issue regulations to implement its requirements, those regulations also would preempt conflicting state laws. There are, however, certain types of state laws that would not be preempted by the bill. These include (1) state laws that address the collection, use or disclosure of health information or financial information, (2) state laws that address notification requirements in the event of a data breach, and (3) other state laws to the extent those laws relate to acts of fraud.

The bill provides that knowing or repetitive violations would be enforceable by the FTC as unfair or deceptive acts or practices under section 5 of the FTC Act, and state attorneys general also may bring civil actions. Violators may be subject to civil penalties assessed by state attorneys general of up to $16,500 per day for violations with total violations not to exceed $6,000,000 for any related series of violations (up to a maximum of $3,000,000 for violations of the security and accountability requirements and an additional $3,000,000 for violations of the notice and consent requirements). The bill explicitly does not include a private right of action.

In addition to the Kerry-McCain bill, the two bills introduced by Jackie Speier (D-CA) and Jay Rockefeller (D-WV) regarding online tracking illustrate how prominent the online behavioral advertising issue has become in 2011. These bills direct the FTC to promulgate regulations to establish standards for a "do-not-track" mechanism that would essentially allow web users the ability to direct websites and ad networks to not track their online activity. In contrast, although they are not focused solely on behavioral advertising, both the Kerry-McCain bill and the Rush bill contemplate offering web users the ability to opt out of behavioral advertising but fall short of seeking the creation of a do-not-track mechanism.

Data Protection Legislation in the EU

In general, European laws and regulations governing the protection of personal data are significantly more stringent than their U.S. counterparts. Businesses that operate in both the U.S. and the EU frequently must confront conflicts between the legal regimes, which can require a sophisticated understanding of supra-national, national and even local restrictions on the processing of personal data.

The current EU data protection framework recently has come under review as European data protection authorities seek to adapt their approaches to respond to an increasingly interconnected global economy. The EU Data Protection Directive, which underpins virtually all European data protection laws and regulations, is in the process of being modernized to take account of new technologies, facilitate compliance (especially with respect to cross-border data transfers) and increase the effectiveness of enforcement.

According to EU authorities, the revisions to the Directive will be based on four pillars: (1) the right to withdraw consent to data processing, (2) transparency for individuals so they know what data are collected about them, the purpose of collection and the risks of data processing (specifically with respect to registering for social networks), (3) "privacy by default", which would mean that data protection requirements also must apply if data are processed for a purpose different from that for which they were originally collected, and (4) EU-level data protection irrespective of the location of data processing and the means used to process the data.

Revising the EU Data Protection Directive is expected to be a lengthy process, with a package of proposals possible in autumn 2011 and a new legal framework sometime in the next two to three years. As the negotiations continue, however, companies should stay abreast of new laws and regulations at the national level, as some EU Member States may seek to implement reforms individually ahead of a formal decision at the supra-national level. At this time, enforcement in the EU is Member State-driven. Certain national data protection authorities are more active than others, but in general proactive

enforcement is on the rise. For example, the data protection authority in France (i.e., the CNIL) has announced an aggressive agenda for 2011 and the Information Commissioner's Office in the United Kingdom now has new powers to investigate data protection violations and to impose stiff monetary penalties where appropriate.

Legal Responses to New Technologies

A number of new technologies that are exciting to businesses across the globe have simultaneously aroused the interest of legislatures and consumer protection advocates in multiple countries. Although in most cases laws are not yet in place to address these technologies specifically, such laws are on the way and companies may risk drawing the ire of regulators if they push the currently ill-defined limits too far. For example, cloud computing services offer increased efficiency and potential cost savings, but many argue that significant information security risks still need to be addressed and the FTC has indicated that cloud computing is one of the technologies that has forced government to reconsider public policy in the privacy arena. Geo-location services like Google's Street View attracted the attention of law enforcement authorities around the world, including the former Attorney General of Connecticut who launched a multi-state investigation in conjunction with numerous other state AGs. And 2011 European guidelines applicable to all industry sectors address the data protection implications of smart tags (that use Radio Frequency Identification Devices (RFID)), which increasingly are being used by companies to track shipments and property, possibly even employees.

Online behavioral advertising and the use of cookies to track online behavior are currently in the spotlight and are a driving force behind the slew of data protection laws proposed in the United States over the past year. In the EU, the recently amended e-Privacy Directive requires prior opt-in consent for cookies as opposed to the current method of allowing consumers to opt out through browser settings. EU Member States are in the process of implementing this requirement in their national laws. Although regulators have indicated that they would welcome an effective industry-based solution, it appears the solutions proposed by interested industry groups to date have not been considered sufficient and are likely to be overridden by Member State legislation.

Strategies for In-House Counsel

In-house counsel has a key role to play when it comes to an organization's privacy and information management strategy, particularly in this era of significant change. With respect to governance, counsel should establish policies, procedures and processes to help ensure legal and regulatory compliance while further advancing business goals. With respect to customer relations, counsel can help the organization respond to consumer inquiries regarding privacy and data security, as well as prepare to respond to a possible data compromise event. Counsel also should learn how the business uses information assets (with particular focus on personally identifiable and confidential data), and deploy that knowledge to facilitate business solutions, ensure compliance, and promote training to ensure employees have a comprehensive understanding of policies governing the collection, use and sharing of data. By understanding the existing laws and emerging legal framework relating to privacy and information security, and developing a comprehensive approach and tools to address privacy and information security, in-house counsel can play a vital role in helping companies avoid the privacy pitfalls suffered by so many organizations over the past decade.