McDermott
Will & Emery

Privacy and Data Protection Year in Review

December 23, 2010

A Look at Major Developments of 2010, and a Prediction of What's to Come in 2011 in Rapidly Developing Areas of Privacy and Data Security Law

Privacy and data protection are an exploding area of focus for international and U.S. regulators. Most businesses are now well aware that if their information practices are not already regulated, they likely will be soon. This article gives in-house counsel and others responsible for privacy and data protection in the United States and Europe an overview of the major developments in this area in 2010, as well as a prediction of what is to come in 2011.

U.S. Federal Law Developments – Consumer Protection

Heather Egan Sussman and Carla A. R. Hine

RECAP OF 2010

In December 2010, the Federal Trade Commission (FTC) released its long-awaited report, *Protecting Consumer Privacy in an Era of Rapid Change*. It proposes a new framework for how to protect consumers' privacy both online and offline. The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer or other device, and is intended to guide Congress as it contemplates potential laws and to steer industry toward stronger self-regulation. Some consumer advocacy groups believe the report could be more robust, while businesses are grappling with its potential impact on their bottom line. The report poses a number of questions on which the FTC is seeking public comment by January 31, 2011.

The key takeaways from the FTC's report include the need for covered business to: (1) review privacy notices to make them clearer, shorter and more standardized; (2) strategize on how to simplify consumer choice; (3) ensure procedures are in place for making prominent disclosures and obtaining consent whenever using data in a way that is materially different than promised; (4) evaluate how to reasonably give consumers access to data collected about them; and (5) expect that most commercial entities, regardless of industry, that collect or use consumer data will soon need to adopt a comprehensive privacy and data security program and implement reasonable safeguards to protect classes of consumer data.

Earlier in the year, U.S. Representatives Rick Boucher (D-Va.) and Cliff Stearns (R-Fla.) released draft legislation that would be the first federal law to generally require nearly every company, regardless of industry, to adopt privacy policies in the online and offline space. The general reaction to the bill, however, was less than favorable for many reasons, particularly because it was based on the notice and consent framework, which the FTC and many in industry believe is outdated. The bill is now widely viewed to be dead in the water, both because Rep. Boucher lost his seat in the November elections and because we expect the more evolved privacy framework articulated in the FTC's recently released report likely will shape the near-term future of Congressional action in this evolving area of the law.

For example, U.S. Senator John Kerry (D-Mass.) has announced that he is working on draft privacy legislation that he plans to introduce in early 2011. The legislation reportedly will be based on the Fair Information Practice Principles (FIPPs) and will apply to covered entities that collect significant amounts of personally identifiable information.

WHAT'S TO COME IN 2011

The FTC will continue to refine the framework it proposed in the report based on the comments it receives from stakeholders by January 31, 2011. In the near term, the report will guide the broader discussion in Congress and industry of how to address consumer privacy concerns in the face of rapidly evolving technological environments. The longer-term impact of the report is less clear, though. The proposed framework is not by itself an enforcement mandate, although companies can reasonably expect to be under heightened scrutiny to ensure that they scale their privacy protection measures to the level of risk their privacy practices pose. The year 2011 will see a continuation of the debate among the FTC, Congress, industry and consumers on how to balance privacy protections against the value of consumer data.

Congress has been receptive to consumer privacy protection concerns and it is exploring the possibility of the "Do Not Track" option recommended in the FTC's report, which would allow consumers to opt out of online tracking for purposes of behavioral advertising. Microsoft's recent release of the its new version of Internet Explorer with built-in "Do Not Track" capabilities will give consumers the right to block websites from collecting their online activities. If this solution takes hold, the pressure for a legislative solution may subside.

In addition, we will likely see the release of Sen. Kerry's legislation in early 2011. That bill reportedly will give the FTC rulemaking authority in the area of consumer privacy and security, and it may be that the FTC will then be able to give its 2010 report more teeth. In that case, businesses will be wise to spend 2011 working on integrating the FTC report's key takeaways now to avoid later being caught behind the proverbial eightball from a privacy and security standpoint.

U.S. Healthcare Privacy and Security Developments

Daniel F. Gottlieb and Edward G. Zacharias

RECAP OF 2010

On July 14, 2010, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services issued a proposed rule containing modifications to the privacy standards (Privacy Rule), security standards (Security Rule) and enforcement regulations (Enforcement Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The proposed modifications to the HIPAA regulations include changes required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and other changes deemed appropriate by OCR in order to strengthen the privacy and security of health information and to improve the "workability and effectiveness" of the Privacy Rule, Security Rule and Enforcement Rule. Of particular note, the proposed regulations would implement the HITECH Act provision that makes "business associates," which provide services involving individually identifiable health information to health care providers, health plans and other HIPAA covered entities, directly subject to the HIPAA civil and criminal penalty schemes.

In addition, on July 28, 2010, OCR withdrew its Interim Final Rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) and indicated that it would issue final breach notification standards under the HITECH Act "in the coming months." OCR expects covered entities and business associates to comply with the withdrawn Breach Notification Rule while it works on a final Breach Notification Rule.

WHAT'S TO COME IN 2011

OCR representatives have stated that in early 2011, OCR will issue a coordinated final rule containing modifications to the Privacy Rule, Security Rule, Enforcement Rule and Breach Notification Rule to implement the HITECH Act and make other changes that OCR deems advisable. OCR is considering comments submitted in response to the modifications to the HIPAA regulations proposed in July and its experience under the Breach Notification Rule. The health care industry is eagerly looking for new standards to facilitate research involving individually identifiable health information and hopes that OCR will not finalize its proposal to make subcontractors of business associates directly subject to the HIPAA penalty scheme rather than only contractually liable to the business associates with which they have a downstream agreement. In addition, the health care industry hopes that OCR will not remove the risk of harm trigger for notification of a breach of unsecured protected health information that was included in the Breach Notification Rule and is included in many comparable state laws.

Europe: Privacy and Data Protection

Rohan Massey and Paul Melot de Beauregard

RECAP OF 2010

The European Union has suffered from a number of national scandals arising from breaches of the data protection regime. These scandals include companies unlawfully monitoring employees and customers, national and international data security breaches, as well as the unlawful collection of personal data. Where regulators have been limited in the punishments they are able to enforce, the media have been quick to publicize the shortcomings of major national and international companies resulting in material reputational damage and changes in the faces serving on some boards.

In light of the current media and political environment, the emphasis in Europe has shifted from education on data protection issues to enforcement. To support this new strategy, there have been a number of changes in national legislation, including, for example, a new employee data privacy law that has been intensively discussed in Germany and is now close to implementation. This law will bring, among other things, significant changes in the areas of job applications, video surveillance of workplaces and inspection rights of the employer, which also will heavily influence existing compliance and anti-corruption policies. In the United Kingdom, the level of monetary penalty that can be issued for a breach of the data protection regime has increased from £5,000 to £500,000 (and the UK regulator has already issued a fine of £100,000 against one local authority).

The increased risk of damage to reputation and the threat of a material fine (and, in some cases, director's personal liability) have raised the risk profile of data protection compliance in the EU. 2010 has been for many companies, both those established in the EU and those involved in international data transfer, a turning point in focusing on the idea that data privacy be a fundamental requirement of business rather than a low-risk afterthought.

WHAT'S TO COME IN 2011

The last 15 years have seen an unprecedented change in the way in which personal data is collected, processed and transferred, whether for business or personal use. Technology facilitates the increasing collection of personal data (by, for example, Google Street View) and the way in which we share personal information about ourselves and others (on, for example, social networks). The EU Commission recognizes that the EU data protection regime needs to evolve to keep pace with technology.

The EU data protection directive is currently being revised and we expect to see significant changes to the regime. This is expected early in the new year.

The new EU "Cookies" Directive is to be implemented by mid-2011. This Directive has given the online advertising industry cause for concern, as it provides that unless the cookie is necessary for use of the service, user consent must given or obtained prior to a cookie being placed on the user's machine. This is a significant change to the current regime. No practical guidance has yet been provided to detail how this provision will work in practice, but such guidance is also expected early in the new year.

There are strong indicators that Europe wishes to be seen as the global benchmark for data protection. This is not only true for the political level of the discussion—given the above mentioned scandals, there is also rapidly developing recognition by employees, customers, etc., of the importance of protecting their data. For example, the Google Street View project saw thousands of objections in Germany. This sensitivity in regard to the use of (personal) data will increase and may raise significant practical business problems.

Going forward, this sensitivity and an increasing legal focus on enforcement will require many businesses to undertake internal reviews and to implement data protection compliance programs. For transatlantic groups, the option of building global policies around the European benchmark is likely to become an increasingly cost-effective and efficient compliance solution.

Online Behavioral Advertising

Monique Y. Ho

RECAP OF 2010

We have seen a greater shift away from Run of Network (RON) advertising and contextual advertising and increased movement towards behavioral targeted advertising, which utilizes behavioral segmentation based on past clicks, page views and surfing histories of anonymous consumers to help deliver targeted ads to specific groups. There was also enormous growth in the use of behavioral targeted advertisements and in the acceptance of such advertisements by enterprises and consumers.

In addition, there has been greater self-regulation by industry members, such as ad networks and ad companies, driven by the FTC guidelines and by advertising associations such as Network Advertising Initiative and Interactive Advertising Bureau. At the same time, we have seen an increased backlash from consumers and consumer privacy groups due to use or misuse of behavioral targeted advertising. As a result of the backlash, there has been an increase in calls for regulation and enforcement that would mandate notice (mechanisms for clearly informing consumers about data collection and use practices), choice (enabling users to choose whether data is collected and used), data security (requiring advertisers to provide security for data collected and limiting the retention of such data), and accountability (creating mechanisms for ensuring meaningful compliance).

WHAT'S TO COME IN 2011

We will see continued growth in targeted advertisements with greater availability of behavioral segmentation to allow for better targeting. This means data about online habits will be gathered more precisely so that ads will target very specific characteristics (such as "enjoys playing tennis," "not married" and "likes Italian food"), rather than broad generalizations (including gender, age and education level).

To accomplish this greater segmentation, new platforms will be available that measure with precise accuracy the attributes of the audience of the targeted advertisements, meaning measurements will be taken on impression (whether they saw the advertisement), click (whether they accessed it) and conversion (whether they actually followed through by purchasing, etc.) metrics to give advertisers an increasingly accurate picture of interaction with the specific audience.

We expect there will be an increase in self-regulation and implementation of the regulatory principles, perhaps via a universal icon to be placed near the advertisement, in order to avoid government regulation. In addition, we expect to see increases in alliances, such as the Digital Advertising Alliance, among the large advertising associations to provide uniform industry practices and standards. Ad networks and publishers expect there will be greater enforcement mechanisms discussed across the industry, such as increased monitoring and enforcement of compliance with stated privacy policies. We also expect to see a shift by companies toward adopting clearer, shorter and more uniform privacy policies and disclosures. Similarly, focus may shift from the current opt-out tracking to specific opt ins and there will be greater focus on undisclosed, non-obvious, or unexpected usage and transfer of data collected.

Changes to the Payment Card Industry Data Security Standards

Heather Egan Sussman and Sabrina E. Dunlap

RECAP OF 2010

In October 2010, the Payment Card Industry Security Standards Council (the Council) released updated PCI Data Security Standard (DSS) and PCI Payment Application Data Security (PA-DSS), which contain a number of minor changes for clarification of the existing standards.

While the majority of the changes in PCI-DSS version 2.0 clarify the existing requirements, there were some changes related to application security, including ranking of vulnerabilities according to risk and expanding the scope of vulnerability testing. These changes are viewed as a way to improve the Web security of online merchants and to prevent credit card fraud.

In addition, some of the changes are aimed toward small merchants, by simplifying their compliance efforts through a more straightforward self-assessment questionnaire and validation process. There were also revisions designed to enable organizations to develop a risk-based assessment approach based on a merchant's specific business situation.

The Council is now advocating for the centralization of logging with the new standards, which could help reduce the number of log-based breaches. A number of the PCI-DSS version 2.0 revisions touch on areas such as log management and simplification of existing compliance requirements.

WHAT'S TO COME IN 2011

The revisions go into effect on January 1, 2011. Validation at the current standards will be permitted until December 31, 2011, to allow organizations time to properly implement changes.

Survey of U.S. State Law Developments

Heather Egan Sussman and Sabrina E. Dunlap

RECAP OF 2010

Nevada—Encryption Law (NRS 603A.010)

As of January 1, 2010, any entity doing business in the state of Nevada that accepts payment cards in connection with the sale of goods or services must be compliant with the current version of the Payment Card Industry Data Security Standard (PCI DSS).

In addition, government agencies, institutions of higher education and all business entities that maintain, collect or otherwise deal with personal information must use encryption to ensure the security of electronic transmissions and use encryption when a data storage device (any device that stores information from any electronic or optical medium, including computers, cell phones, magnetic tapes, etc.) moves beyond the "physical or logical controls" of the business or entity.

Nevada was the first state to adopt the PCI DSS in its entirety (Minnesota codified it in part), and compliance with the new law protects businesses from liability for damages resulting from a security breach. The law repealed the existing Nevada encryption law, which required businesses in the state to encrypt personal information sent electronically outside of the business' secure system.

Under this new law, "encryption" means the following:

- Encryption technologies adopted by an "established standards setting body" such as the National Institute of Standards and Technology (NIST), which renders data indecipherable in the absence of associated cryptographic keys "necessary to enable decryption of such data," and

- Appropriate management and safeguarding of cryptographic keys to "protect the integrity of the encryption using guidelines promulgated by an established standard-setting body" such as NIST

Massachusetts—Data Security Regulations (201 CMR 17.00)

As of March 1, 2010, the Massachusetts Data Security Regulations require all entities that own, maintain or store personal information of Massachusetts residents to have a written information security program and implement reasonable administrative, physical and technical safeguards designed to protect that information. The Regulations apply to all entities that handle personal information of a Massachusetts resident, regardless of whether the entity is located in or outside of Massachusetts.

"Personal information" includes a Massachusetts resident's first name and last name (or first initial and last name) in combination with one or more of the following:

- The resident's Social Security number

- The resident's driver's license number or state-issued identification card number

A financial-account, credit-card or debit-card number (with or without the required access code or password) assigned to the resident

The Regulations contain very detailed minimum requirements. For example, covered entities must, among other things, designate an individual in charge of data security, encrypt personal information in transit, and have contract provisions that address protection of personal information given to vendors. Additionally, entities must evaluate their written plans as business practices change, and provide initial and ongoing training to all employees handling personal information.

The Massachusetts Attorney General's Office enforces the Regulations. Failure to comply can result in an enforcement action and substantial fines. The Regulations are widely viewed to be the most comprehensive state law on the protection of personal information because the requirements are so detailed and because they apply to virtually every business, regardless of industry. In addition, the protections "travel," which means that the Regulations apply to businesses that maintain personal information of a Massachusetts resident *regardless of where the information resides*, even if that business does not have an office in Massachusetts.

Connecticut—Insurance Regulation (Bulletin IC-25)

On August 18, 2010, the Connecticut Insurance Commissioner issued Bulletin IC-25, requiring all entities subject to the jurisdiction of the Connecticut Department of Insurance to notify the department of any security breaches involving a Connecticut resident's personal health or financial information within five days of the "information security incident." The Bulletin defines "personal information" as information (regardless of whether computerized or not) that is capable of being associated with a particular individual through one or more identifiers, including, but not limited to, the following:

- A Social Security number

- A driver's license number or state identification card number
- An account number or a credit- or debit-card number
- A passport number
- An alien registration number
- A health insurance identification number

The definition does not include publicly available information that is "lawfully made available to the general public from federal, state or local government records or widely distributed media."

The Bulletin appears to be more burdensome in terms of notice than even the Connecticut data breach notification law (Conn. Gen Stat. 36a-701(b)), effective since 2006. That notification law only requires notice when *computerized* personal information is disclosed, whereas the insurance requirements apply to information in whatever form in which it is collected. The Commissioner reportedly has taken public criticisms of the requirement under advisement and we will watch for a potential modification to the Bulletin in 2011.

New Hampshire—Breach Notification (H.B. 619)

New Hampshire enacted a new breach notification law on January 1, 2010, requiring health care providers and business associates to notify individuals of disclosures of their protected health information, where such disclosures are prohibited under New Hampshire law, even when the disclosures are permissible under HIPAA.

Under the New Hampshire law, individuals can sue for violations of the notification requirement and seek damages of $1,000 per violation. Additionally, if a business associate discloses a person's protected health information, triggering notification under the law, the business associate must cover the costs of notification.

The terms "business associate" and "protected health information" are adopted from HIPAA, but "health care provider" includes the following: any person, corporation, facility or institution either licensed by the state of New Hampshire or otherwise lawfully providing health care services, including, but not limited to, a physician, hospital, office, clinic, health center or other health care facility, dentist, nurse, optometrist, pharmacist, podiatrist, physical therapist or mental health professional, and any officer, employee or agent of such provider acting in the course and scope of employment or agency related to or supportive of health care services.

Unlike the state's general breach notification law, H.B. 619 does not contain a "risk of harm" trigger, such that notice is required regardless of whether it is determined that misuse of the acquired information is likely to occur.

California—Repeal of Privacy Regulations

As a result of the California Office of Administrative Law's (OAL) approval of the California Department of Insurance's plans to repeal portions of its privacy regulations in November 2010, agents and brokers are no longer required to mail privacy policies to customers annually nor must they provide customers with an opt-out form..

This provision of the California Code that was repealed, Section 2689.8(c)(3), required all insurance agents and brokers to mail annual privacy policies to customers and offer customers an "opt-out" form, intended to prevent broker-agents from shopping on renewal, in an attempt to find better policies from other insurance companies.

Proponents of the repeal claim that the changes will make it easier for consumers to shop the insurance market, as customers go to independent agents and brokers to shop multiple insurance companies. Consumers will also no longer receive multiple privacy policies on insurance products they purchase, which some claim is a benefit.

Mississippi—Data Breach Notification (H.B. 583)

On April 7, 2010, Mississippi became the 46th state to enact data breach notification legislation. The new law (H.B. 583), going into effect July 1, 2011, requires that any person who conducts business in Mississippi, and who owns, licenses or maintains personal information of Mississippi residents in the ordinary course of business, provide notice to the owners or licensees' of the information upon discovery of a breach of the security of the data. H.B. 583, similar to many other state data breach notification laws, defines "personal information" as a person's first name or first initial and last name, in combination with any one or more of the following:

- Social Security Number
- Driver's license number or state identification card number
- An account number or credit- or debit-card number in combination with any required security code or password

The law includes a provision stating that notification will not be required if an entity properly investigates the breach and determines that the breach will "not likely result in harm to the affected individuals." The law will be enforced by the state Attorney General, and there is no private right of action under the Mississippi law.

WHAT'S TO COME IN 2011

Michigan: The Michigan legislature is currently considering a bill (HB 4732) that would mimic the Federal Red Flags Rule. The law would require that qualifying entities establish written identity theft prevention programs, designed to identify threats to identity and to prevent and mitigate identity theft.

Kentucky: Pending Kentucky legislation, H.B. 107, would require government agencies to protect all personal data under the Gramm-Leach-Bliley Act. H.B. 107 is titled "An Act Relating to Protection of Private Information," and states its intention to "[c]reate a new section of KRS 65.003 to 65.158 to require that any local governmental entity safeguard the records of any individual or other taxpayer in a manner consistent with federal law relating to the protection and destruction of documents."

Florida: In early 2010, Florida introduced bills (S.B. 586 and H.B. 279) which would require companies to follow federal guidelines when disposing of personal data. Both bills died in committee, and it remains to be seen if they will be raised again in 2011.

For more information, please contact your regular McDermott lawyer, or:

Daniel F. Gottlieb: +1 312 984 6471 dgottlieb@mwe.com

Rohan Massey: +44 20 7575 0329 rmassey@mwe.com

Paul Melot de Beauregard: +49 89 12712 121 pbeauregard@mwe.com

Heather Egan Sussman: +1 617 535 4177 hsussman@mwe.com

Sabrina E. Dunlap: +1 617 535 4014 sdunlap@mwe.com

Carla A. R. Hine: +1 202 756 8095 chine@mwe.com

Monique Y. Ho: +1 858 720 3318 mho@mwe.com

Edward G. Zacharias: +1 617 535 4018 ezacharias@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com