McDermott
Will & Emery

Privacy and Data Protection 2011 Year in Review

December 30, 2011

A Look at Some of the Major Developments of 2011 Around the Globe, and a Prediction of What's to Come in 2012 in the Areas of Privacy and Data Protection

Privacy and data protection continues to be an exploding area of focus for regulators in the United States and beyond. This article gives in-house counsel and others responsible for privacy and data protection an overview of some of the major developments in this area in 2011 around the globe, as well as a prediction of what is to come in 2012.

UNITED STATES

Developments at the Federal Trade Commission

Heather Egan Sussman and Sabrina Dunlap

SETTLEMENT REGARDING ONLINE ADVERTISING

Among the many interesting settlements at the Federal Trade Commission (FTC) this past year, the FTC announced in March 2011 that it had reached a settlement with online advertising company Chitika, Inc., to resolve its complaint against the company involving its online consumer tracking practices. According to the FTC complaint, Chitika serves as an intermediary between websites and advertisers, by buying ad space on websites and contracting with advertisers to place ads with cookies on those sites. Chitika also engages in the practice of "behavioral advertising" by placing cookies on the browsers of consumers who visit the websites displaying the advertisements it has placed. Chitika then tracks the consumer's activities on the web, including searches made and sites visited by the consumer. Chitika then displays targeted ads to that consumer based on the tracked activities.

The FTC alleged that while Chitika disclosed in its privacy policy that it collects data about consumers' preferences, the privacy policy also stated that consumers could opt out of having cookies placed on their browsers and receiving targeted ads. The FTC alleged that the opt-out lasted only 10 days. After that brief opt-out period expired, Chitika re-placed tracking cookies on browsers of those consumers, and targeted ads to them again. The FTC complaint alleged that Chitika's claims about its opt-out mechanism were deceptive and violated federal law.

Chitika ultimately agreed to settle the matter and refrain from making misleading statements about the extent of data collection about consumers and the extent to which consumers can control the collection, use or sharing of their data. The agreed Consent Order requires that every targeted ad include a hyperlink that takes consumers to a clear opt-out mechanism that allows a consumer to opt out for at least five years. It also requires that Chitika destroy all identifiable user information collected when the defective opt-out was in place. In addition, the settlement requires that Chitika alert consumers who previously tried to opt out that their attempt was not effective, and they should opt out again to avoid targeted ads.

After a period of public comment on the proposed settlement, the FTC finalized the matter in June 2011. A few pointers for companies that engage in online marketing practices can be gleaned from the Decision and Order. First, if a company wishes to engage in behavioral advertising, it must adequately disclose the practice in the online privacy policy. Second, it appears the FTC does permit a company to put an expiration date on a consumer's opt-out election. However, that expiration date must be reasonable. Here, the FTC found 10 days was too short and instead agreed upon an expiration period of five years. It remains to be seen whether some shorter time period would also be deemed reasonable by the FTC, but there may be updated guidance on this issue in 2012, as described below.

GUIDANCE REGARDING ONLINE ADVERTISING

Following on the heels of the Chitika settlement, in May 2011, the FTC requested public comments on its advertising guidance, "Dot Com Disclosures: Information About Online Advertising." The guidance, originally published in 2000, advises businesses

how federal advertising law applies to online advertising and sales. However, there has been tremendous change in the online world since the FTC first published the guidance—mobile marketing has seen rapid growth, the "app" market for mobile devices and tablets took off, and online social networking now includes many millions across the globe. As a result, the FTC invited public comment on the guidance, indicating that the agency was particularly interested to hear what marketers, consumer advocates and other stakeholders believe are the technical and legal issues that the agency needed to address given the growth in online use and online marketing over the years.

The public comment period closed in August 2011, and it is not yet clear when the FTC will publish the revised guidance. The original guidance addressed issues of transparency in marketing, and means by which marketers could provide clear and conspicuous disclosures to consumers making online purchases. Any updated guidance will likely focus on how much online marketing has changed, the need for improved transparency in online marketing practices, and how companies can find appropriate ways to make adequate disclosures to consumers using online services.

PROPOSED COPPA AMENDMENTS

The FTC recently proposed changes to its online privacy rule for children, the Children's Online Privacy Protection Act (COPPA), to expand coverage of its protection, and accepted comments until November 28, 2011. The proposed changes are available at www.ftc.gov/os/2011/09/110915coppa.pdf. COPPA, which was implemented in 2000, gives parents control over what personal information websites can collect from children under the age of 13, and limits the amount of data websites can collect and use about children.

One of the most significant proposed changes to COPPA is the expanded definition of covered "personal information," which would now include screen and user names, as well as persistent identifiers such as Internet Protocol addresses and tracking cookies. In addition, the FTC proposed eliminating one of the ways in which businesses can obtain parental consent—the "e-mail plus" mechanism, which allowed sites to obtain consent by receiving e-mails from parents, then sending them a delayed response confirming the parental consent. Under the proposed amendments, companies would have to find alternatives to the e-mail plus mechanism for consent, including using video conferencing or government-issued identification numbers for verification.

COPPA will continue to apply to those who operate websites directed at children and collect personal information, and those who have actual knowledge that they are collecting personal information from a child under 13. But the FTC clarified its position in the proposed changes that COPPA applies to a wide range of current technologies that could be considered "online services," including mobile apps, network-connected games and some text messaging. While the FTC did not expand the technical application of COPPA by significantly expanding the definition of personal information or by including all online services (not just websites), such as mobile apps, the changes to COPPA will likely expand the scope of covered businesses.

The proposed changes related to parental consent and the expanded definition of personal information will likely have the largest impact on current business practices, because companies will now have to find new ways of obtaining consent, and the use of certain identifiers that previously were not considered personal information could now bring companies under the domain of COPPA. More discussion on COPPA will likely occur in 2012, as the FTC is expected to release revised regulations that will reflect on comments received to date.

Developments in Health Care – HIPAA Audit Program Initiated

Daniel Gottlieb

On November 8, 2011, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) published on its website the details of its pilot program to perform up to 150 audits of compliance with the privacy, security and breach notification standards (collectively, the Standards) adopted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) between November 2011 and December 2012 (Pilot Audit Program). The details of the Pilot Audit Program are available at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

The Pilot Audit Program will include only HIPAA-covered entities, *i.e.*, health care providers, health plans and health care clearinghouses, and not their business associates. OCR stated, however, that business associates would be included in future

audits. OCR implemented the Pilot Audit Program pursuant to Section 13411 of the HITECH Act, which requires OCR to conduct audits of covered entities and business associates to ensure they are in compliance with the Privacy and Security Rules and the Breach Notification standards. The audits will be conducted by KPMG, which was awarded the contract to develop the Audit Program and conduct the audits.

OCR stated that it "will audit as wide a range of types and sizes of covered entities as possible; covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses may all be considered for an audit." While business associates will not be included in the initial 150 pilot audits, they will be included future audits after completion of the Pilot Audit Program.

All audits conducted during the Pilot Audit Program will include a site visit and result in a formal report. Covered entities selected for audit will receive a notification letter from OCR approximately 30 to 90 days prior to the site visit. OCR has provided a draft notification letter, available at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/sample-ocr_notification_ltr.pdf. The letter will provide contact information for the auditor, explain the audit process and include an initial document request. The document request will require the covered entity to provide documentation of its efforts to comply with the Standards, which are expected to include, at a minimum, copies of the entity's privacy, security and breach notification policies and procedures and the security risk assessment required under the HIPAA security standards. Covered entities and business associates selected for an audit will have 10 business days to provide the requested documentation to OCR. The onsite visits may take anywhere between three and 10 days. During the site visits, auditors will interview personnel and observe the entity's practices. Thereafter, OCR will generate a draft report, and the covered entity will have 10 business days to review it and provide written comments to the auditor. The auditor will then complete a final audit report within 30 business days and submit it to OCR. The final report will include the auditor's findings, the corrective steps the entity is taking to correct any deficiencies and a description of any best practices of the covered entity.

OCR stated that the Pilot Audit Program is primarily intended to improve its understanding of compliance efforts with particular aspects of the Standards, to determine what types of technical assistance should be developed and to determine what types of corrective actions are being developed. OCR will share best practices identified during the Pilot Audit Program and issue guidance on common compliance challenges, but it will not publish a list of the audited covered entities or any findings of an audit that could identify an audited entity.

In circumstances where an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited entity that could lead to civil money penalties. For more information about the civil money penalties authorized under HIPAA, see McDermott *On the Subject* "HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act Requirements," available at www.mwe.com/info/news/ots1109f.htm.

While OCR will only select a very small percentage of covered entities to be audited under the Pilot Audit Program, the Pilot Audit Program is representative of OCR's stepped-up efforts to enforce and ensure compliance with the Standards. For more information on OCR's increased enforcement activity, see McDermott *On the Subject* "OCR Exercises its Enforcement Discretion," available at www.mwe.com/info/news/ots0311a.htm. Accordingly, it would be prudent for covered entities to revisit their policies and procedures for compliance with the Standards and ensure that they have completed and documented at least one security risk assessment consistent with the HIPAA security standards.

Litigation and Arbitration Trends

CLASS ACTION LITIGATION AND THE HARM THRESHOLD

Jason Crow and Heather Egan Sussman

More than 150 consumer class actions were filed in 2011 alleging invasions of online privacy. These claims were brought under a mix of state and federal statutes that provide attorney fees and statutory damages. Federal claims were typically brought under the Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), and Stored Communications Act (SCA). State claims typically were brought under consumer protection statutes (*e.g.*, Ch. 93A in Massachusetts), as well as common law theories, such as breach of contract, invasion of privacy and unjust enrichment.

Common fact patterns emerged, and many of these cases alleged the following:

- Violations of terms of use agreements
- Leasing, selling and improper disclosure of personal information from social media websites
- Improper use of internet browser tracking technologies, *e.g.*, Flash cookies (a cookie that regenerates itself when deleted), browser history sniffing code and online behavioral analysis

Common theories of harm included the following:

- Increased risk of identity theft
- Time and effort to monitor/fix credit
- Emotional distress
- Personal information as property

Despite the large number of invasion of online privacy class actions filed, plaintiffs have struggled to quantify the harm they have suffered. In fact, defendants often prevailed because plaintiffs were unable to plead sufficient economic or emotional harm (*e.g.*, *Bose v. Interclick*, *Low v. LinkedIn*, *Del Vecchio v. Amazon*, *In re Facebook Privacy Litigation* and *Krottner v. Starbucks*). For example, in *Bose v. Interclick*, 2011 U.S. Dist. LEXIS 93663 (SDNY), the court dismissed Bose's class action CFAA claim and held that she failed to show that Interclick, an internet advertising company, caused damage to her "computers, systems or data that could require economic remedy" when it installed a Flash cookie and browser history sniffing code on her personal computer. Interclick's software had gathered and transmitted Bose's browsing habits to an online advertising network. The court reasoned that Bose failed to establish how she was deprived of the economic value of her personal information simply because it was collected by a third party and failed to demonstrate how Interclick's software caused damage, a slowdown or a shutdown to her computer. The court, however, denied Interclick's motion to dismiss Bose's state law claim brought under New York's consumer protection statute, reasoning that Interclick's conduct may have "injured" Bose's privacy rights by misleading her into believing her information was private when in reality it was being tracked without her knowledge.

The struggle to meet the harm threshold has similarly been an issue for plaintiffs in traditional security breach cases, but the U.S. Court of Appeals for the First Circuit issued a significant decision in October 2011, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011). In that case, the First Circuit reversed the lower court's dismissal of plaintiffs' negligence and implied contract claims, and held that plaintiffs' "reasonably foreseeable mitigation costs," such as credit card replacement and identity theft insurance costs, "constitute a cognizable harm under Maine law."

In 2012, plaintiffs likely will continue to file lawsuits over privacy practices that rely on a mix of harm theories and federal and state law, despite plaintiffs' traditional difficulties demonstrating actionable harm, for several reasons. As *Bose v. Interclick* demonstrates, whether plaintiffs can show harm resulting from the collecting and sharing of personal information, or use of online behavior tracking devices, is still in flux and depends on the circuit and state in which the case is heard. In addition, there are unresolved issues regarding the applicability of federal statutes. For example, major amendments to the ECPA in 1986 did not contemplate technologies like Flash cookies and browser sniffing. Finally, the *Anderson* decision could pave the way for more cases to be filed and survive motions to dismiss in 2012.

FLASH COOKIES

Eric Hagen

In 2010 and 2011, a flurry of class action lawsuits alleging unlawful use of so-called Flash cookies was filed against numerous online companies. The complaints have asserted that defendants' websites used Adobe Flash files called locally stored objects, or "Flash cookies," to bypass users' privacy controls and track their online activity without their knowledge or consent. The class action plaintiffs have asserted violations of various federal and state electronic data privacy and computer crime laws.

The first such complaints were filed within a year after a U.C. Berkeley study claimed that some popular websites were using Flash cookies to "respawn" HTTP cookies that users tried to delete. The researchers asserted that websites using these resilient Flash cookies could perpetually track users' online activity unbeknownst to the users.

Some courts have dismissed these data privacy claims, for reasons that include failure to allege adequate facts or sufficient injury. But that does not necessarily mean those cases are over. In some instances, plaintiffs have been granted the opportunity to

amend their complaints, while in at least one other case, the plaintiffs continue to prosecute surviving common law claims for consumer fraud and trespass to chattels.

Meanwhile, some of these class actions reached final settlements in 2011, and other settlements are pending. At least two of closely watched cases settled for as much as $2.4 million, with a significant portion to be paid to nonprofits engaged in consumer data privacy protection. In addition, the settling defendants agreed to implement certain measures to prevent Flash cookies from respawning web browser cookies that users have intentionally deleted. These measures include requirements that the accused website's privacy policies adopt rigorous notice requirements that provide a means for users to opt out of online behavioral advertising that employs Flash cookies.

ARBITRATION OF CONSUMER CLASS ACTION CLAIMS

Heather Egan Sussman and Sabrina Dunlap

Despite the increase in class action lawsuits in 2011, there was one major development related to *limiting* class actions—the Supreme Court of the United States decision *AT&T Mobility LLC v. Concepcion*, 562 U.S. ___ (2011). In April 2011, in what many hailed as a win for businesses, the Supreme Court held that the Federal Arbitration Act (FAA) preempts any state authority that strikes down as "unconscionable" consumer contracts with arbitration clauses containing class action waivers.

The background to this decision is Section 2 of the FAA, which makes agreements to arbitrate "valid, irrevocable, and enforceable, *save upon such grounds* as exist at law or in equity for the revocation of any contract" (9 U.S.C. §2, emphasis added). Prior to the *AT&T* decision, the California Supreme Court had considered the emphasized statutory language, and used the doctrine of unconscionability as such "legal grounds" to strike down class action waivers in consumer contracts.

In *AT&T*, the Supreme Court of the United States held that the California Supreme Court decision interfered with the clear intent of the FAA to promote arbitration, and held that when a state law would impair the purpose of the FAA, the FAA must preempt the conflicting state law. Importantly, the Supreme Court did not rule that *all* arbitral class action waivers are enforceable. Rather, the Supreme Court held only that arbitral class action waivers are not, in and of themselves, void as unconscionable.

As a result, courts still must evaluate the particular arbitration agreement at issue on a case-by-case basis to determine whether the terms are fair. The arbitration agreement at issue in the *AT&T* decision, however, provides an example of one that would be deemed fair and enforceable. The highlights of that arbitration agreement include the following:

- Venue was in the county where the consumer resides.
- Consumers could elect to have the arbitration be in-person, telephonic or decided based on written submissions.
- AT&T agreed to pay all costs for non-frivolous claims.
- Arbitrators had the power to award any form of individual relief, including issuing injunctions and presumably awarding punitive damages.
- AT&T waived any right to seek reimbursement of its fees and costs.
- In the event that a consumer received an award greater than AT&T's last written settlement offer, AT&T was to pay a $7,500 minimum recovery and double the amount of the consumer's attorney's fees.

In light of this decision, businesses at risk for consumer class actions should consider whether the cost of a generous arbitration provision like AT&T's outweighs the risk of consumer class actions. One important factor in this analysis is the difference between the number of consumers who are likely to pursue individual claims to their conclusion, and the likelihood that a plaintiff's lawyer will assert claims on behalf of a large number of consumers without their active participation. In any case, businesses should consider reviewing existing contracts with outside counsel and determine whether revisions are appropriate in light of the *AT&T* decision.

SEC Issues Guidance on Cybersecurity Disclosure Obligations

Amy Leder, David Cifrino and Heather Egan Sussman

On October 13, 2011, the Division of Corporation Finance of the U.S. Securities and Exchange Commission (SEC) issued "CF Disclosure Guidance: Topic No. 2 – Cybersecurity" (the Guidance), available at www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, regarding a public company's obligation to make certain disclosures concerning cybersecurity risks and cyber incidents. Although the Guidance is not a rule, regulation or statement of the SEC, public companies should nevertheless ensure that their disclosures and their disclosure controls and procedures comply with the Guidance to the extent applicable to their material cybersecurity risks and any cyber incidents.

The Guidance notes there are two separate triggers for cybersecurity disclosures. First, public companies must evaluate cybersecurity risks, regardless of whether a cyber attack has occurred, and assess whether disclosure of those risks is appropriate. A second trigger for disclosure is the occurrence of specific events, including cyber attacks and other cyber incidents. This could mean disclosing information about material investigation costs and other effects, such as when a cyber attack or breach could expose a company to a lengthy government investigation or costly third-party claims, cause significant business interruption and result in lost revenues and impairment of certain assets, undermine the value of services, harm reputation or lead to substantial costs of remediation.

The Guidance describes in further detail the Staff's expectations regarding how and when companies should make specific types of disclosures, including in the financial statements and in the Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), Description of Business and Legal Proceedings sections of annual and quarterly reports.

In the wake of this Guidance, an uptick in public company disclosures will likely occur in this area, with respect to both specific cyber incidents that have occurred and risks that such an incident might occur. As with any other risk, the SEC cautions that such disclosure "should be tailored to [the issuer's] particular circumstances and [should] avoid generic 'boilerplate' disclosure." A company is not required to give a roadmap of its weaknesses, but it may have to disclose if it has a particular weakness given its business model. As a result, companies must balance carefully the need to make a disclosure with the need to protect their cybersecurity vulnerability. Although the SEC cautions against boilerplate disclosures, common themes are likely to emerge nevertheless in cybersecurity disclosures made in issuers' SEC filings in the industries and sectors where cybersecurity issues are most prevalent.

Other Federal Law Developments

PENDING FEDERAL BREACH NOTIFICATION LAWS IN THE SENATE

Jennifer Geetter

Personal Data Privacy and Security Act of 2011

On June 7, 2011, Senator Patrick Leahy (D-VT) introduced S. 1151, entitled the Personal Data Privacy and Security Act of 2011, co-sponsored by Senators Charles Schumer (D-NY) and Ben Cardin (D-MD). Senator Leahy previously introduced significant privacy and security legislation (2005, 2007 and 2009), but each time the bill did not advance. The bill was referred to the Committee on Judiciary, which held a hearing, and on November 7, 2011, the Committee's written report was filed, but it is unclear whether the Senate will resume consideration in 2012.

If enacted, S. 1151 would establish new federal criminal offenses for the unauthorized access to personal information. The bill would also mandate that many federal agencies and private businesses that collect, maintain, use or disclose personal information establish adequate privacy and security processes and programs, and provide notice to individuals regarding breaches of their data.

For entities that collect, access, transmit, use, store or dispose of *sensitive* personal data on 10,000 or more individuals, the bill requires implementation of a privacy and data security program. Business entities would be expected to conduct risk assessments periodically to identify vulnerabilities and make adequate upgrades, and to train employees in the requirements of the program. The bill charges the FTC with responsibility to develop regulations, including provisions exempting certain businesses from compliance, such as financial institutions already regulated by the Gramm-Leach-Bliley Act and entities subject to HIPAA.

Entitles not exempted may find that their existing information security programs are inadequate to meet the requirements of the bill, because the bill appears to more broadly define sensitive personally identifiable information and require audit trail provisions that exceed commonly implemented industry standards. The bill imposes steep penalties for non-compliance, including civil and criminal penalties.

Data Security and Breach Notification Act of 2011

On June 15, 2011, Senators Mark Pryor (D-AR) and Jay Rockefeller (D-WV) introduced S. 1207. It was referred to the Committee on Commerce, Science and Transportation and scheduled for two mark-ups in fall 2011, which were both cancelled. Although the bill appeared to have support from Chairman Rockefeller, it is unclear whether the Senate will resume consideration in 2012. Of all the bills under consideration, this one arguably has the most elements in common with the European Union's existing Data Protection Directive.

The bill proposes to cover for-profit and not-for-profit entities, and seeks to establish a national standard that would preempt the current patchwork of state regulation. The bill governs any covered entity that "owns or possesses data containing personal information, or contracts to have any third-party entity maintain such data" and "information brokers," which are defined as entities whose business it is to "collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity," and that then sell or provide that information to nonaffiliated third parties, such as informatics companies.

This legislation would direct the FTC to promulgate regulations, with joint enforcement by the FTC and state attorneys general. Like the Leahy bill, this legislation contains both breach notification provisions and information security program requirements, including detailed parameters for the required security policies. Regulated businesses would be required to report to the FTC the security polices and processes that they have implemented to safeguard personal information. The bill permits entities to provide notice of breaches to individuals in a variety of ways. Entities may be exempt from the notice provisions, however, if the entity determines that the breach does not present any reasonable risk of identity theft, fraud or other unlawful conduct. In addition to notice of breaches, affected individuals would be entitled to receive consumer credit reports and credit monitoring assistance for a two-year period. The bill also provides for individuals to access personal data maintained about them and establishes a process to dispute information. This bill, too, contains steep enforcement penalties

Data Breach Notification Act of 2011

On June 7, 2011, Senator Dianne Feinstein (D-CA) introduced S. 1408, entitled Data Breach Notification Act of 2011. Senator Feinstein has previously introduced similar legislation in four prior consecutive sessions of Congress, but it has never come out of Committee. S. 1408 was referred to the Committee on Judiciary, and a hearing was held this fall, from which no written report has resulted. No further activity has occurred, and it is unclear whether the Senate will resume consideration in 2012.

Of all the bills under consideration, this one arguably is the most streamlined and focuses mainly on establishing one federal breach notification standard. In particular, this bill only contains breach notification provisions and does not require any programs and policies. However, the notification provisions are more detailed than the other bills. For example, covered entities would be required to notify individuals of security breaches unless the entity determined that there was "no significant risk" that the breach would harm an individual whose sensitive personal data was involved in the breach. An entity making this conclusion would have to undertake a formal risk assessment supporting this finding and submit the results of the assessment to the FTC. If the information involved in the breach was encrypted or rendered indecipherable through best practices, there would be a statutory presumption of no significant risk of harm. Under certain scenarios, the entity must also notify the Secret Service within 14 days. If a security breach involves 5,000 or more individuals from one state, there must also be notice through a media outlet. Enforcement would be lead by the U.S. Attorney General and state attorneys general when the federal government declines to enforce. Unlike other bills, S. 1408 would not designate the FTC as the primary enforcer. In addition, this bill would preempt state and federal law relating to notification by a business entity of a security breach.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Evan Panich and David Gacioch

In May 2011, Senator Patrick Leahy (D-VT) unveiled a plan to amend the Electronic Communications Privacy Act (ECPA), which Congress first enacted in 1986. The ECPA prescribes the circumstances under which government entities can access an individual's e-mail, wireless communications (including SMS text messages) and cell site location information (CSLI), which law enforcement entities can use to pinpoint a suspect's location.

As written, the statute does not require the government to obtain a warrant to access e-mails and wireless communications more than 180 days old. Instead, the statute allows the government to access electronically stored information armed only with a court order. A judge may issue such an order without a showing of probable cause. Additionally, the statute allows the government to delay notifying the subject of this intrusion for up to 90 days.

Senator Leahy's amendment (S. 1011) would accomplish three goals. First, it would eliminate the distinction between e-mails more recent than 180 days old and older than 180 days old. Under the proposed scheme, the government would need to obtain a warrant to access *any* e-mail or wireless communication. Second, the amendment would eliminate the ECPA's delayed notice provisions and require the government to disclose the warrant to the individual within three days, but would allow the government to seek a court order to delay notice for up to 90 days upon a showing that disclosure would jeopardize an ongoing investigation or national security. Third, the amendment would require the government to obtain a warrant to access an individual's CSLI.

These amendments likely stem from recent judicial decisions challenging the validity of the ECPA. *See, e.g., United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that the ECPA is unconstitutional to the extent that it allows the government to obtain access to e-mails without a search warrant); *see also In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 2011 WL 3678934 (E.D.N.Y. Aug. 22, 2011) (finding that warrantless access of CSLI is unconstitutional).

In 2012, Congress may act on Senator Leahy's proposed amendment, but some officials in the U.S. Department of Justice oppose it. For example, Associate Deputy Attorney General James Baker has said that for Congress to require the government to obtain a warrant to access all stored e-mail content would have "collateral consequences to criminal law enforcement and the national security."

Additionally, the Supreme Court of the United States will hear an appeal from the U.S. Court of Appeals for the District of Columbia Circuit deciding the constitutionality of warrantless GPS tracking. Although not directly related to the ECPA, the decision will likely definitively determine the constitutionality of the government's use of CSLI in electronic surveillance.

WHITE HOUSE CYBERSECURITY LEGISLATIVE PROPOSAL

Evan Panich and David Gacioch

In May 2011, the White House announced a legislative proposal to enhance protections against cyber crime. The White House has two proposals for helping to protect individuals. First, the White House points to the patchwork of state law relating to data breach and seeks to enact a single federal legislative scheme outlining businesses' obligations in notifying their consumers when intruders gain access to consumers' personal information. Second, the President would enhance criminal penalties for cyber criminals and amend the federal Racketeering Influenced and Corrupt Organizations (RICO) statute to apply to cyber criminals.

The White House also has advanced proposals aimed at forging partnerships between the public and private sector in combating cyber crime. The Administration has encouraged Congress to adopt a statutory scheme by which private sector businesses can seek the assistance of the Department of Homeland Security for investigatory assistance when a business's security is breached. Conversely, the proposed legislation would incentivize private sector organizations to share information regarding potential cyber threats with the government.

Finally, the legislative proposal seeks to enhance the standards for cyber security within federal agencies' computing infrastructure in a number of ways, including centralizing management of government computer security, recruiting highly qualified cybersecurity professionals, installing intrusion prevention systems and incentivizing cloud computing.

Cybersecurity legislation that incorporates many of the White House proposals is currently under consideration by the House and Senate. The House is currently considering two pieces of cybersecurity legislation (H.R. 2658 and H.R. 3523). The House Intelligence Committee approved one such bill on December 1, 2011 (H.R. 3523). Members of the House Homeland Security Committee introduced another on December 16, 2011 (H.R. 2658). It is expected that the full House will continue to consider this legislation in the coming months. Meanwhile, Senate Majority Leader Harry Reid (D-NV) hopes to bring a yet-undrafted cybersecurity bill to the Senate floor in early 2012.

Developments at the State Level

DEVELOPMENTS IN CALIFORNIA

Elisabeth Malis and Jorge Arciniega

In August 2011, California passed a senate bill (SB 24) updating California's security breach notification law, by establishing new content requirements for breach notification letters to California residents and requiring notification to the state attorney general when a breach affects more than 500 California residents. HIPAA-covered entities in compliance with the federal HITECH Act are deemed to have complied with these new content requirements. In addition, entities reporting a security breach that elect to notify affected individuals through the state's media, rather than directly, must now also notify the California Office of Privacy Protection and Consumer Services Agency. The amendments take effect January 1, 2012.

In February 2011, the California Supreme Court held that it is a violation of California law for businesses to request and record a credit card holder's ZIP code in connection with a credit card transaction (*Pineda v. Williams-Sonoma*, 51 Cal. 4th 524 (Cal. 2011)). Plaintiff filed a putative class action against retailer Williams-Sonoma alleging that it violated California's Song-Beverly Credit Card Act of 1971 (one of the state's consumer protection statutes) when a cashier asked for, and later recorded, plaintiff's ZIP code during a credit card transaction, and plaintiff believed that providing such information was a condition to completing the purchase. The Credit Card Act prohibits businesses from asking for cardholders' "personal identification information" during credit card transactions and then recording that information. The California Supreme Court reversed the lower courts' holdings that ZIP codes were not "personal identification information" and held that the retailer's request and recording of ZIP code information violates the Credit Card Act.

DEVELOPMENTS IN TEXAS

Elisabeth Malis and Jorge Arciniega

Texas passed a law (H.B. 300) in the fall of 2011 that will take effect on September 1, 2012. The law imposes new employee training and notification obligations related to protected health information (PHI), exceeding the requirements of the HIPAA Privacy Rule. The law provides patients with increased rights and remedies over electronic health records, and increases penalties for non-compliance. Significantly, the law incorporates an expanded definition of the term "covered entity" in Texas's existing health privacy law, such that it could have a broad effect on many non-HIPAA-covered entities. The definition of "covered entity" under the law includes any entity that engages in assembling, collecting, analyzing, using, evaluating, storing or transmitting protected health information, as well as any entity that comes into possession or obtains or stores PHI.

The law also amends the existing breach notification law, Business & Commerce Code, Section 521.053, and purports to expand coverage to all citizens of the United States. In particular, the new law provides that if an entity conducting business in Texas suffers a breach, it must not only provide notice to affected consumers who live in Texas, but also to those who live in a state that does not currently require notification. If the individual lives in a state that currently does require notification, then the entity can comply with Texas law by providing notice to the affected consumer pursuant to his or her state's law. To the extent a company doing business in Texas suffers a breach after August 2012, therefore, it should evaluate with counsel whether and to what extent it should send notices to all affected U.S. consumers regardless of the state of residence, to avoid the harsh penalty scheme of the Texas law.

EUROPEAN UNION

EU Data Protection Directive – Draft Revised Legislation

Amelia Cross and Alison Wetherfield

Proposed changes to EU data protection law that will affect global business are expected to be formally proposed in late January 2012. A spokesperson for the European Commission in the United Kingdom has warned that a leaked draft of the new data protection directive, published online in December 2011, should not be considered a definitive version.

The new laws are likely to mandate the following:

- Enhanced rights of data subjects to control their own data that will be enforceable in the online environment
- Data minimization rules (*i.e.*, collecting only essential data and storing such data only for as long as is necessary)
- Privacy by design (*i.e.*, weaving privacy throughout an entire organization in order for it to work effectively, for example by proactively embedding privacy into the design specifications of information technology and accountable business practices)
- The right to be forgotten (*i.e.*, the deletion of personal data from social networking and other sites)
- Protection of children against abusive profiling or tracking on the internet
- Introduction of privacy impact assessments for risky processing to ensure that data controllers properly manage data protection risks
- Appointment of a data protection officer for certain enterprises
- Extension of data breach notifications (*i.e.*, mandatory requirement to notify customers of data security breaches) to all sectors
- Strengthened competences for national data protection authorities

In addition, for binding corporate rules, it is likely that a streamlined approval process will be introduced whereby companies will have a single point of contact, and once approval is obtained from a single data protection authority, there will be mutual recognition by all other European data protection authorities.

E-Privacy Directive – Cookies

Rohan Massey

May 25, 2011, was the deadline for EU Member States to implement local laws reflecting the requirements of the revised E-Privacy Directive (2009/136/EC). Of the changes required, the most contentious related to the use of cookies. Under the original E-Privacy Directive (2002/58/EC), a provider must provide clear and comprehensive information about any cookies being used and provide the option for people to opt out of the cookies being used or stored on their devices. The revised position is that unless the cookie is necessary for performance of the service, the user's consent must be obtained in order to store a cookie on a subscriber's device.

There has been much debate as to when and how consent must be obtained to comply with the new Directive. Although there is no one-size-fits-all solution, it is clear that for consent to be effective the user should be given clear and comprehensive information about the cookies and its purpose, as well as details of any data sharing with third parties prior to the cookie being placed. The more invasive the use of cookies, the greater the prominence that should be given to obtaining the consent. Providers should therefore audit the cookies they use, revise privacy policies to highlight the use and where possible obtain an active indication of the user's consent prior to use.

By December 2011, only 11 of the 27 Member States had implemented the revised Directive, and some, including the United Kingdom, had granted a 12-month period before beginning enforcement. This does not mean that providers should relax. These

laws will likely be enforced vigorously in 2012, and as the regulators have the power to levy fines in excess of $500,000 for non-compliance, this is a compliance issue that warrants serious consideration.

Developments in France

Jilali Maazouz and Sébastien Le Coeur

PHONING – PACITEL LIST

As of September 2011, consumers who do not wish to be contacted by telephone can register their landline and mobile phone numbers for free on the PACITEL list. The companies to which the consumers have given their phone numbers will still be allowed to contact them.

The PACITEL list is managed by an association created at the initiative of five major professional associations that currently represent 80 percent of the companies using phoning. These professional associations will ensure that their members abide with the PACITEL list, failing which said members will face sanctions from these associations and the government services.

COOKIES STATUTE OF AUGUST 24, 2011

The transposition in French law of the "Telecom Package" directives reinforces the obligation to inform web users regarding cookies. Unless relevant information has already been provided, any subscriber or user of an electronic communication service must be informed in a clear and comprehensive manner by the data-controller of the purpose of any action to gain access by electronic transmission to information already stored in his or her electronic communications terminal equipment, or to place information in the equipment, as well as the means available to oppose such actions.

This access or storage can only take place if the subscriber or user has expressed agreement after being provided with this information; such agreement may result from appropriate settings of his or her connection device or any other device placed under his or her control.

These provisions do not apply if access to information stored in the terminal equipment of the user or the storage of information in the terminal equipment of the user has the sole purpose of enabling or facilitating electronic communication, or is strictly necessary for the provision of an online communication service at the express request of the user.

In practice, the website should be able to offer multiple choices to the user:

- Accept the aforementioned cookie
- Refuse the cookie and be asked again next time
- Refuse the cookie and memorize this refusal with the installation of a "refusal cookie"

Developments in Germany

Paul Melot de Beauregard

In Germany a bill for an Employee Data Protection Act (*Beschäftigtendatenschutzgesetz*) was launched by the federal government in summer 2010, to regulate the data protection of employees and implement the main tenor of the case law of the German Federal Labour Court. But currently, after the counterstatement of the second chamber (*Bundesrat*) with numerous amendments and the first reading in the first chamber (*Bundestag*), the legislative procedure stagnates. The main point of issue is the challenge to achieve an appropriate equilibrium between the interests of the employees in a comprehensive data protection on the one side and the interests of the employers in the effective possibility to prevent corruption and criminal offenses on the other side.

Some core issues of the bill so far include the following:

- Health checks should only be allowed if they are relevant to a decisive vocational requirement and the employee agrees.

- Employers should not be allowed to use personal data of employees from the internet, especially from social networks. Exceptions should only apply for web pages for purposes of the employee's own presentation (*i.e.*, websites where an employee may present him- or herself, such as LinkedIn).
- Secret video surveillance should be prohibited in general.
- Fighting corruption without information of the employee should only be possible if a concrete suspicion concerning a criminal offense or a severe violation of duty exists and the facts cannot be revealed in any other way.

The German Federation of Trade Unions (*DGB*) assumes that due to the delay and the controversial parliamentary debate there will be a lowering of the level of protection for employees. On the other hand, the German Employers' Association (*BDA*) fears that such legislation would bring more risks for employers, in particular in regard to terminations and the extensive options for employees to declare them unlawful. However, it appears to be very likely that the Employee Data Protection Act will come into force in the coming months.

Developments in Italy

Veronica Pinotti

NEW RULES ON THE PROCESSING OF LEGAL ENTITIES' DATA

In July and December 2011, Italy adopted new rules amending the scope of application of the Personal Data Protection Code. Under such new rules, all information relating to private and public bodies or associations is excluded from the definition of personal data. As a consequence, private and public bodies as well as associations are no longer considered "interested parties" for the purpose of the application of the Italian Data Protection Code.

Before the above amendments to the Data Protection Code, Italy was one of a small number of EU Member States where the protection of personal data was extended not only to natural persons, but also to legal entities. The new rules aim at reducing the administrative burden on companies and limiting the privacy protection of private and public bodies whose data can now be processed without having to obtain permission.

UNLAWFUL PROCESSING OF MOBILE NUMBER DATA AND THE DEFINITION OF SENSITIVE DATA

In February 2011, the Italian Supreme Court (*Corte di Cassazione*) issued a highly criticized judgment in a matter of unlawful processing of personal data concerning the publication on the internet of mobile number information without the data subject's consent.

The judgment has been criticized as the court went far to state that the mobile numbers published on the internet constituted "sensitive data." Such unprecedented interpretation appears difficult to reconcile with the wording of the Data Protection Code, which requires that "sensitive data" should be able to reveal "racial or ethic, religious, philosophical or other beliefs, political opinions, membership of political parties, unions, associations or organizations of a religious, philosophical, political or trade union, as well as personal data disclosing health and sex life." It remains to be seen whether such interpretation will be confirmed in the future court's ruling.

Ukraine – New Comprehensive Privacy and Data Protection Law

Amelia Cross and Alison Wetherfield

The law On Protection of Personal Data, which is based on the framework of the 1995 EU Directive, has been in force since January 1, 2011. The law requires state registration of any database owned by individuals or legal entities and used for business purposes containing personal data of, for example, customers, clients, end consumers and employees.

The fundamental principle of the new law is that a data subject's prior documented consent is required for all stages in data collection, storage and processing, which clearly poses an extreme administrative hurdle before a database can be registered. The

regulator's strict adherence to the recognized forms when processing submitted information coupled with the fundamental principle has resulted in delays to the statutory time limits for the registration of databases.

Companies are under increasing pressure to become compliant with the new law as existing databases must be registered by January 1, 2012, which coincides with the introduction of the increase in liability for violating the law to U.S.$2,000 per violation and up to five years imprisonment for the company's CEO. Interpretation of some provisions of the law has also proved problematic, even for the regulator. An English translation of the law is available at www.zpd.gov.ua/zpd.gov.ua_eng/R/indexResources.html.

LATIN AMERICA

Mexico – New Federal Regulations

Matthew Turnell and Heather Egan Sussman

Mexico's Regulations of the Federal Law for the Protection of Personal Data (*Reglamento de la Ley Federal de Protección de Datos Personales en posesión de los particulares*) took effect on December 22, 2011. The final regulations, which follow prior drafts released in July and October 2011, provide guidelines for implementing Mexico's Federal Law for the Protection of Personal Data, which became effective in July 2010. The 2010 privacy law regulates the collection, processing and disclosure of personal data held by private companies, and provides for both civil and criminal penalties for violations. The law adopts eight general principles that must be followed in the handling of personal data: legality, consent, notice, quality, purpose limitation, fidelity, proportionality and accountability. The 2011 regulations cover matters such as the territorial scope of the law, consent requirements for handling personal data, privacy notice requirements, use restrictions on persona data, safety measures for handling personal data, requirements for data transfer and data owners' rights to obtain personal data. An unofficial English translation of the regulations, supplied by local counsel in Mexico as a courtesy, is available at http://www.mwe.com/info/pubs/Regulations Data Protection Law (Eng).pdf.

Peru – New Comprehensive Privacy and Data Protection Law

Matthew Turnell and Rohan Massey

In July 2011, Peru adopted its Law on the Protection of Personal Data. The law, the first of its kind in Peru, regulates the processing of personal data in Peru. The law establishes eight guiding principles for the processing of personal data: legality, consent, purpose, proportionality, quantity, security, enforcement and adequate protection of cross-border data flow. The law also creates a National Personal Data Protection Authority under the Ministry of Justice to enforce the law. The law grants data subjects rights to access, correct, update, include, eliminate and object to data, and also creates a right to compensation for violations of the law. Individuals may also appeal to the National Personal Data Protection Authority to enforce their rights under the law. The law establishes fines for violations of the law, which are categorized as "mild," "serious" and "very serious." Fines are capped at 10 percent of the violator's annual gross income. Regulations implementing the law have yet to be drafted. An English translation of the new law is available at http:www.mwe.com/info/pubs/Peru Data Protection Law July 28_EN _2_.pdf.

Costa Rica – New Comprehensive Privacy and Data Protection Law

Heather Egan Sussman and Rohan Massey

In September 2011, Costa Rica enacted a new privacy law entitled *Protección De La Persona Frente Al Tratamiento De Sus Datos Personales* (Law No. 8968), becoming the latest Latin American country to enact a comprehensive privacy regime. Prior to enactment of this new law, Costa Rican privacy law centered around the constitutional principle of "Habeus Data," which essentially means that the data subject is the owner of data about him- or herself. The new law creates a regime that formalizes "Habeus Data" and that incorporates foundation principles similar to those of the 1995 EU Directive. For example, the law creates a newly formed Agency for the Protection of Inhabitants' Data known as "Prodhab" under the Ministry of Justice, which is responsible for overseeing administration of the new privacy and data protection regime. Covered persons and entities must

register all databases that process personal information for business purposes and pay an annual fee of U.S.$200 for operating such databases. The law distinguishes between "data controllers" and "processing of personal information," and requires notice to data subjects and consent regarding the processing of personal data, as well as a means for revoking that consent. Similar to the EU regime, the Costa Rican privacy law requires special treatment of sensitive data; places limits on data transfers; and requires reasonable security to protect against unauthorized use, access, disclosure and destruction.

Going forward, the Prodhab is expected to draft and publish regulations further implementing and clarifying procedures under the new law. In the meantime, individuals who allege they are aggrieved by violations of the new law can file complaints with the Prodhab, which has the authority to undertake a procedure for review and sanctions.

ASIA-PACIFIC

China – First Law to Expressly Regulate Personal Information Protection

Henry Chen

In July 2011, China's Ministry of Industry and Information Technology (MIIT) released draft voluntary regulations intended to protect citizens against the misuse of personal information by Internet Information Service Providers. The draft regulations, entitled Provisions on the Administration of Internet Information Services (Provisions), establish users' rights and set guidelines for the distribution of internet services.

The Provisions stipulate that, among other requirements, Internet Information Service Providers must collect only personal information relevant to internet services, inform users about the terms of the information collection before obtaining consent and protect users' information from distribution to third parties. In addition, the Provisions establish guidelines for behavior between competing Internet Information Service Providers. According to the new regulations, providers cannot slander or spread false information about competitors, nor can they force users to uninstall services offered by competitors or limit the use of competitors' services. For all Internet Information Service Providers, failure to adhere to these Provisions could result in fines of RMB 10,000 to 30,000 (approximately U.S.$1,540 to U.S.$4,620).

Importantly, the Provisions currently stand only as draft standards; they are voluntary regulations that lack the full strength of legal enforcement. They could be modified any time by the MIIT, which has not yet formalized the regulation. Still, the Provisions represent an important stepping-stone toward future progress in Chinese privacy legislation, because the Provisions represent China's first internet service regulations to *explicitly* address the issues of competition and personal information protection. With its increased focus on privacy, it appears likely that China will soon see new legislation for personal information protection.

India – Clarifying Existing Privacy and Data Protection Law

Heather Egan Sussman and Rohan Massey

In April 2011, India issued final privacy regulations that sought to clarify and enhance the scope of the country's existing privacy regime as set forth in section 43-A of the Information Technology Act, 2000. The new regulations, entitled the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules), establish a framework obligating covered entities (bodies corporate) to take the following actions:

- Establish a privacy policy regarding the collection and processing of personal data
- Obtain consent for processing sensitive data (which includes a mere password), collect sensitive data only in certain circumstances and use data only for the purpose for which it was collected for the time period necessary to accomplish that purpose
- Give data subjects the right of access to review data collected about them, to correct or amend inaccurate data and to withdraw previously supplied consent

- Appoint a grievance officer, whose name and contact information must be posted on the website of the body corporate
- Maintain reasonable security measures to prevent unauthorized disclosure
- Limit transfers to third parties and other jurisdictions, except in certain circumstances

Many felt the final regulations were not entirely clear, however, and following release of the Privacy Rules, there was substantial confusion regarding scope, particularly regarding the seemingly onerous consent requirements. As a result, the Ministry of Communications and Information Technology released a statement in August 2011, clarifying that outsourcing firms in India handling personal data for companies outside of India need not get written consent from data subjects in other countries in order to process their information in accordance with the law. In addition, for body corporates covered by the law, written consent included consent by any electronic means.

South Korea – New Comprehensive Privacy and Data Protection Law

In March 2011, South Korea become the latest country in the Asia-Pacific region to enact a new comprehensive privacy and data protection law, entitled the Personal Information Protection Act (PIPA). Many provisions of PIPA will reportedly take effect later in 2012.

AFRICA

Angola – New Comprehensive Privacy and Data Protection Law

Heather Egan Sussman and Rohan Massey

The Angolan Data Protection Act (Law No. 22/11) was reportedly enacted in June 2011. It is modeled generally after the 1995 EU Data Protection Directive but is more closely aligned with Portugal's national regime. In addition to Angola, the African countries of Kenya, Malawi, Mozambique and South Africa are considering draft legislation to implement comprehensive privacy regimes. Some drafts have reportedly been circulating for years, but strong industry opposition has delayed enactment. Given what appears to be the increasing global trend toward establishing comprehensive regimes in line with the European Union, more privacy developments may well be seen in these countries and in others in Africa in 2012. A copy of the Angolan law provided by McDermott's local counsel firm is available at http://www.mwe.com/info/pubs/Law_22_11_Data_Privacy_Law.pdf.

For More Information

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

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

Rohan Massey: +1 011 44 20 7577 6929 rmassey@mwe.com

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

Jorge Arciniega: +1 310 551 9306 jarciniega@mwe.com

Paul Melot de Beauregard: +1 011 49 89 12712 330 pbeauregard@mwe.com

Henry Chen: +86 21 6105 0586 henrychen@mwechinalaw.com

David Cifrino: +1 617 535 4000 dcifrino@mwe.com

David Gacioch: +1 617 535 4478 dgacioch@mwe.com

Jennifer Geetter: +1 202 756 8205 jgeetter@mwe.com

Eric Hagen: +1 310 788 4165 ehagen@mwe.com

Amy Leder: +1 212 547 5514 aleder@mwe.com

Jilali Maazouz: +33 1 81 69 15 00 jmaazouz@mwe.com

Veronica Pinotti: +1 011 39 02 786273 02 vpinotti@mwe.com

Alison Wetherfield: +44 20 7577 3489 awetherfield@mwe.com

Jason Crow: +1 617 535 4018 jcrow@mwe.com

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

Sébastien Le Coeur: +33 7 61 67 34 54 slecoeur@mwe.com

Elisabeth Malis: +1 310 788 1557 emalis@mwe.com

Evan Panich: +1 617 535 4161 epanich@mwe.com

Matthew Turnell: +1 617 535 4019 mturnell@mwe.com

Amelia Cross: +44 20 7570 1420 across@mwe.com

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