SMITH ANDERSON
expectexcellence®

DATA USE, PRIVACY AND SECURITY TRENDS OF 2013

11.27.2013
Alicia Gilleskie and Mary Pat Sullivan

The constant evolution of technology continues to bring out corporate efficiencies, and with that, a constantly-changing landscape of “business-as-usual.” These technologies are creating a massive opportunity for companies to collect and use personal information about consumers – whether customers, employees or business contacts.

At the same time, this information is regulated under a complex and growing patchwork of laws, regulations and standards. As illustrated by many well-publicized examples, a lapse in data privacy can have a significant impact on a company’s bottom line and cause irreparable harm to a company's reputation. The following list highlights some of the major topics that companies should consider with respect to data collected and maintained in their operations.

1. Data Security Standards – Which One Applies?

A patchwork of federal and state laws require businesses in the financial, credit card processing and health care industries, as well as companies who collect information about residents of specific states (such as California, Massachusetts, and Nevada), to implement certain data security measures to protect sensitive information. Even if a business is not subject to these specific requirements, the FTC takes the position that failure to take appropriate security measures to safeguard consumer information is an unfair trade practice under federal law, even in cases where companies made no representation that they took security precautions. Accordingly, the FTC has taken numerous enforcement actions against companies for failing to properly safeguard such information.

Many data breaches are preventable (such as those that result from lost or stolen documents, laptops, disks, thumb drives, and other portable devices), and implementing reasonable data security measures is an important step in preventing costly and embarrassing data breaches. Implementing and maintaining an effective data security plan is an ongoing process. It generally includes physical security measures, such as controlling physical access to systems and data through locks and barriers, technical security measures such as firewalls, anti-virus software and password controls, administrative safeguards, such as implementing policies and procedures (including BYOD policies) and training employees on current policies and procedures.

A data security plan should include preventative measures to avoid security breaches, detection measures to quickly identify security breaches and response measures that details how to react to a security breach when it occurs, including how to stop an ongoing breach, investigate the breach and minimize damage caused by the breach. Having an effective data security program is an ongoing process that requires regularly evaluating the effectiveness of ongoing programs and the potential risks, training staff and staying vigilant about following good policies and procedures.

[see article on cybersecurity]

2. Data Breach Response Planning – The Need for a Policy

Data security and managing cyber risk remain at the top of the list of concerns for public company directors and general counsels. Only a minority of general counsels and directors feel confident in the ability of their companies to quickly detect and respond to cyber breaches.[1]

Some data breaches cannot be prevented, but advanced planning can help with a more efficient response when one occurs. Nearly all states have breach notification laws that generally obligate companies to notify affected individuals, and in certain cases, state and federal agencies and the media, in response to an unauthorized access to personal information. To make sure the organization is prepared to react quickly and appropriately, it is imperative to have an "incident response plan" in place.

The incident response plan should address how the organization will investigate and respond to a suspected or actual unauthorized access or disclosure of personal information. It should help employees recognize potential data incidents and direct them to the designated company official through a company-adopted internal notification process. A designated response team should be appointed and the specific responsibilities of its members should be outlined in the incident response plan. Members of the response team often include representatives from legal, information security, human resources, public relations, finance and other management stakeholders. The plan should outline a process for proper documentation, efforts to protect information under attorney-client privilege and retention of records relating to the incident.

The initial response plan should set out steps to contain the breach and end the data compromise. Once contained, there should be an investigation to determine the scope of the breach and related analysis to determine whether any laws or contractual obligations are implicated as a result of the breach. While requirements vary, many of the legal and contractual obligations require some sort of notification to be provided – to affected individuals, state attorneys general, credit reporting agencies, customers and in certain cases, the media. HIPAA and other industry-specific regulations may require notification to industry specific regulators.

The incident response policy should also address organizational efforts to prevent a data breach from re-occurring, including ongoing policy evaluation, re-training and a focus on awareness of the risks. For more information, see our data breach checklist.

3. Online Privacy Statements and Mobile Applications -- No More Boilerplate

There is no federal omnibus privacy statute governing online activities. The law applicable to online privacy comes in a patchwork of state, federal and activity-specific laws.

States such as California have enacted consumer privacy laws that require website owners and operators with online operations involving the collection of personal information from their residents to post a privacy statement that includes certain disclosures to the website user. In addition, the Children's Online Privacy Protection Act of 1998 ("COPPA") requires websites that collect information from children younger than 13 to comply with specific rules. [See further information about COPPA under #3 below.] Further, certain specific marketing and data use activities conducted with personal information collected online require special consents and approvals that online policies should address.

In addition to the state laws that may apply to website operations involving residents of their respective states, the presence of an online privacy policy can draw the attention of the Federal Trade Commission (“FTC”). While the Federal Trade Commission (“FTC”) does not have general jurisdiction over websites, the failure to strictly adhere to the promises and representations contained in online documentation (such as a privacy statement) can lead to an FTC enforcement action under Section 5 of the FTC Act, for unfair or deceptive practices. And with respect to online *security*, the FTC has taken the position that *regardless* of what is stated in a website privacy statement, certain unexpected practices are unfair.

Websites that operate on a national basis and are targeted to individuals need to prepare and post a well-thought-out privacy statement that is strictly tailored to the website’s data collection and use activities. At a minimum, website privacy statements must be accurate, and promises and representations made to the consumer must be honored. The privacy statement must include an accurate description of the types of personal information collected (including through cookies and online tracking) and the ways in which the website owner or operator may use and share that information.

There may also be activity-specific disclosures that can apply, depending on the nature of the data collected or tracking of the individual. For example, California recently amended its California Online Privacy Protection Act to require websites that collect personal information about California residents to disclose how the site responds to browser “do not track” signals, and whether the site allows other parties to collect “personally identifiable information about an individual’s online activities over time and across different websites when a consumer uses the web site or service.” This would apply to behavioral advertising among other things.

The same rules that apply to website privacy statements also generally extend to mobile applications. The FTC has recently focused on mobile app privacy and has brought several enforcement actions against mobile app companies, including for failure to accurately disclose all of the ways personal information would be collected through the app. Companies should expect to see increased enforcement actions regarding mobile app privacy statements. Just as with traditional websites, companies should ensure their mobile app privacy statements are scrupulously accurate.

As e-commerce business models continue to become more complex with respect to data collection and use, organizations would be well-served to familiarize themselves with FTC guidelines regarding online privacy[2] and monitor enforcement actions for trends and problematic practices. Companies should regularly review their online privacy statements to ensure they are accurate, especially as the company’s data collection and use activities change.

Generally, website owners should direct their focus on (i) privacy by design, which focuses on addressing and incorporating privacy issues at all levels of product and business model development, (ii) simplified consumer choice, including providing consumers with the choice about whether the site will collect or share particularly sensitive consumer information (including geolocation data, access address books, etc.) and (iii) transparency by providing short and clear privacy policies that are easily accessible through the website or device. In addition, the FTC considers the use of “just in time disclosures” to be a best practice, which would inform the consumer and obtain the consumer’s consent prior to collecting certain types of unexpected or sensitive personal information (such as location data, or before accessing address books, photos, calendar entries, etc.).

4. COPPA

On July 1, 2013, new rules adopted under the Children's Online Privacy Protection Act of 1998 ("COPPA") greatly expanded parental control over personal information collected online about their children. COPPA is intended to give parents control over the online collection, use and disclosure of personal information of children under the age of 13. Online and mobile websites and services subject to COPPA must post clear and conspicuous privacy policies, provide notice to parents of its privacy practices, obtain parental consent before collecting, using, or disclosing personal information from children and establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

Before these changes, COPPA applied to operators of commercial websites and online services *directed* to children under 13 years old that collect or disclose personal information and third party services (such as an ad network or plug-in) that collects information from such sites. The new regulations expanded COPPA's application to apply also to websites geared towards *general audiences* (not just directed towards kids) that *knowingly* collect personal information from children under 13 years old. Operators who may collect information from children should re-evaluate whether it is subject to COPPA under the new rules.

The new COPPA regulations also expanded the definition of personal information to include geolocation information, photos or videos containing a child's image or audio files with a child's voice, a screen name or user name that functions as online contact information (even if it does not reveal an email address) and a persistent identifier (such as a customer number held in a cookie, and IP address, device serial number, or unique device identifier) that can be used to recognize a user over time and across different websites or online services (persistent identifiers are no longer required to be paired with other individually identifiable information to be subject to the rule).

5. BYOD

Many businesses allow employees to use personal electronic devices, such as smart phones, tablets and laptops for business purposes, commonly called "Bring Your Own Device" or "BYOD". BYOD gives employees greater flexibility to use their preferred devices to work outside the office, but they also raise security, confidentiality and employee privacy concerns for employers.

Companies using BYOD policies should maintain and enforce written policies that govern the use of personal devices. Any BYOD policy should maintain the security and confidentiality of company information accessed through the device. The policy should require the device to comply with the security requirements of any work issued device, including minimum security settings and anti-virus protections, password controls and encryption requirements. It should address whether the information can be backed up to a "cloud" account, whether third party technical support can access company data on the device and whether employees should be prohibited from accessing highly sensitive data from personal devices. Companies should also consider whether to restrict the use of certain applications on the device or whether to segregate company information on the device so that other applications cannot access company information.

Companies should consider how to protect company information if the device is lost or stolen or if the employee is terminated. Employees should be required to immediately report the lost or stolen device and the company should reserve the right to (and already have installed technology to allow it to) wipe its data from the entire device.

BYOD policies also raise a number of other issues for businesses to consider. In particular, employee privacy in relation to BYOD policies is a growing concern. BYOD policies should clearly set forth what data the employer can access on the device (such as text messages, non-work provided applications, etc.), whether the employer can monitor the use of the device or transmission of data, whether certain activities are prohibited on the device (such as viewing pornography, harassment, etc.) and whether the employer can wipe the entire device or only work specific applications. Companies should also consider whether to exclude certain types of employees from using personal devices, such as nonexempt or international employees and how or whether to reimburse the employee for work related costs associated with the device (such as data plans, etc.).

6. Expansion of HIPAA beyond the Core Health Care Community

The September 23, 2013 deadline to comply with the final omnibus rule ("Omnibus Rule")[3] has passed. The Omnibus Rule was published on January 17, 2013 by the U.S. Department of Health and Human Services and modified the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The most sweeping changes to the Omnibus Rule impact Business Associates. The Omnibus Rule expands the definition of "business associate" to include downstream subcontractors of a business associate that creates, receives, maintains or transmits protected health information ("PHI") on behalf of the business associate. A business associate is required to enter into business associate agreements directly with its subcontractors who receive PHI (business associates were already required to enter such agreements with covered entities). All business associate agreements must include certain specified terms (existing agreements, including those with covered entities, will likely need to be updated to comply with this requirement). The Omnibus Rule also requires business associates to comply with *all* of the Security Rules and many of the Privacy Rules. Business associates that fail to comply with these requirements may face significant civil monetary penalties, criminal penalties, as well as any applicable contractual liabilities.

Other significant changes include stricter limitations on marketing communications made in exchange for remuneration, the disclosure of PHI for fundraising purposes and the sale of PHI without *prior* patient authorization.

See *Newly Effective HIPAA Omnibus Rule Makes Sweeping Changes to HIPAA* for more information.

For more details on the new marketing rules, CLICK HERE.

7. Use of Personal Information for Marketing

As technology continues to make it easier for companies to obtain information from consumers and track their habits, companies should ensure that they have the rights to use the information they collect or obtain. Companies operating in certain regulated industries, such as the financial and health care industries, may be required to provide notices to customers before using their information for marketing purposes, and in some cases, obtain the individual's prior authorization or provide the opportunity to opt-out depending on the industry. If your company obtains a mailing list or other consumer information from a third party, you should evaluate whether the third party is authorized to collect the information and disclose it to you for marketing purposes and whether there are restrictions to how you can use or further disclose the information. Remember that any privacy policy or other statement regarding how the information will be protected or used must be scrupulously honored to avoid enforcement actions or civil litigation.

In addition, different forms of marketing communications may be subject to specific rules and regulations. Email messages are governed by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) if the primary purpose of the email is the commercial advertisement or promotion of a commercial product or service, regardless of whether the message is sent as a bulk distribution or to a single recipient. CAN-SPAM requires that the email provide a clear and conspicuous notice of how to opt-out of receiving future emails from the sender and requires the sender to promptly honor all opt-out requests. Email communications subject to CAN-SPAM are prohibited from using deceptive subject lines and must include other certain information, including identifying the message as an advertisement, informing the recipient of your current address and including correct header information (including the “From”, “To” and “Reply To” information).

Additional laws and regulations may apply to telephone solicitations (including the Do-Not-Call Registry which has been extended to mobile phones), commercial advertisements by facsimile and commercial messages sent by text messages. Companies should remember that traditional rules and regulations governing direct marketing may also apply, including without limitation prohibitions on deceptive or misleading advertisements and regulations regarding sweepstakes.

The HIPAA Omnibus Rule also imposes significant new restrictions and consent requirements on the use of PHI for marketing purposes. For more information about the HIPAA marketing rule, CLICK HERE.

---

[1] Kimberly S. Crowe, Corporate Board Member, Law in the Boardroom 21, 2013, *available at* http://www.fticonsulting.com/global2/critical-thinking/reports/law-in-the-boardroom.aspx.

[2]*See* Fed. Trade Comm’n, Mobile Privacy Disclosures: Building Trust Through Transparency (Feb 2013) *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; Fed. Trade Comm’n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012) *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[3] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan 25, 2013) (to be codified at 45 C.F.R. Parts 160 and 164).

PROFESSIONALS

Mary Pat K. Sullivan

PRACTICE AREAS

Data Privacy