Robinson+Cole

Data Privacy + Security

September 3, 2015

Data Privacy + Security Insider

ENFORCEMENT + LITIGATION

Maryland AG Settles with Visionworks over Security Practices

Using the Maryland Consumer Protection Act, Maryland Attorney General Brian Frosh has announced that eye care retailer Visionworks, Inc. has agreed to pay the state of Maryland $100,000 and enhance its security measures following an investigation into two security incidents that occurred in 2014. When it was upgrading its Annapolis, Maryland and Jacksonville, Florida stores to fully encrypted servers, Visionworks allegedly left the old servers, containing customers' names, addresses, dates of birth, purchasing history, health insurance information and three days' worth of encrypted credit card data unsecured as they were "misplaced" by accident. They believe the servers were taken to landfills.

Frosh stated that Visionworks expressly and implicitly represented to consumers that it would protect their personal information, including their health information, which was required by HIPAA and the Maryland Personal Information Protection Act. When it failed to secure the servers and properly dispose of them, the AG alleged that Visionworks "committed unfair and deceptive trade practices" which violated the Maryland Consumer Protection Act.

In addition to the $100,000 penalty, Visionworks has also agreed to provide credit monitoring and identity theft insurance to any consumer who contacts it or the AG's office. It further agreed to enhance its security practices with respect to storage and disposal of personal information, use encryption technology to safeguard personal information, and "not misrepresent the extent to which it protects personal information."

Although we are used to seeing cases and settlements over security practices with the FTC for unfair and deceptive practices following a data breach (and the Wyndham case) has certainly paved the way for more FTC enforcement actions and settlements), seeing settlements with state AGs is less common. However, we anticipate seeing more AGs use the same theory to launch investigations and push for settlements using broad state consumer protection powers. The message to businesses is clear: enhance security measures to avoid enforcement actions at both the federal and state level.

— Linn Foster Freedman

MAC Zip Code Privacy Suit Settled

MAC Cosmetics, Inc. (MAC) has settled a proposed class action suit filed in Massachusetts federal court, which alleged that it illegally obtained customers' zip codes at the point of sale. MAC has agreed to set up a fund totaling $365,000 to issue gift cards to approximately 86,000 former MAC customers who purchased MAC products starting in the fall of 2009. The case alleged that the customers were asked for their zip codes to complete the transaction of purchasing MAC products in stores in Massachusetts, and after the zip codes were given, MAC used the zip codes to cross reference customer names with the zip code to obtain the customers' full address. Thereafter, MAC allegedly sent the customers unwanted advertisements. MAC disputes the allegations.

The kicker is that the proposed attorneys' fees agreed to will be $107,000 and the lead plaintiff will also receive $2500. The settlement has to be approved by the judge before it becomes final. The named plaintiff and her attorneys are making the rounds and already settled similar suits with Urban Outfitters Inc. and Free People LLC earlier this year.

— Linn Foster Freedman

Online Entertainment Network Machinima Settles with FTC

California based Machinima, an online entertainment network that promoted Xbox One, has settled an investigation with the FTC surrounding its advertising practices. The FTC alleged that Machinima paid "influencers" to post YouTube videos endorsing Xbox One and other online games. However, the "influencers" failed "to adequately disclose that they were being paid for their seemingly objective opinions," according to the FTC.

According to the complaint, a small group of influencers were paid between $15,000 and $30,000 for producing YouTube videos at the beginning of the Xbox One marketing program. Thereafter, Machinima promised to pay a larger group of influencers $1 for every 1,000 video views up to a maximum of $25,000. Machinima did not require the influencers to disclose they were being paid for the YouTube videos.

The FTC's blog post announcing the settlement stated: "The law says reviewers should disclose their connection to a company. Why? Because a connection could affect the credibility a consumer gives to the review." In its press release, the FTC stated "When people see a product touted online, they have a right to know whether they're looking at an authentic opinion or a paid marketing pitch. That's true whether the endorsement appears in video or any other media."

The settlement is clear in explaining the FTC's requirements for paid endorsements in marketing campaigns, and online marketing companies may wish to consider the settlement when developing online marketing campaigns that use paid endorsements.

— Linn Foster Freedman

DATA SECURITY

Security Frameworks 101: Which Is Right for My Organization?

These days information security is on the minds of virtually all technology professionals and business executives alike. But how does an organization ensure that its security profile is adequate. It can certainly help to subscribe to a security framework.

What is a security framework and which should I consider for my organization? A security framework can simply be described as a collection of policies, standards, procedures, controls, tools, and/or guidelines to assist in furthering an organization's security composition. Which one is right for your organization is not as simple a question to answer. Let's look at a few of the more prevalent frameworks.

COBIT, first released in 1996, has been applied across a wide range of industries – to generally improve the effectiveness of IT. COBIT 5, published in 2012, has components that specifically address IT governance, risk management, information security, regulatory compliance, and audit assurance. COBIT has been a popular choice for publicly traded companies required to comply with the Sarbanes-Oxley Act of 2002.

The ISO 27000 series, published in 2013, also provides a very broad information security framework that can be applied to all types and sizes of organizations. By many reports, ISO 27000 is currently the fastest growing security standard applied, in terms of the number of certifications obtained by organizations and consultants.

The NIST Cybersecurity Framework is the result of a February 2013 Executive Order, by President Barack Obama, titled "Improving Critical Infrastructure Cybersecurity". NIST is an agency of the United States Department of Commerce and its framework represents 10 months of collaboration with more than 3,000 security professionals. Like many frameworks, it is comprised of leading practices from various standards bodies that have proved to be successful when implemented. NIST can generally be applied across industries and there are many writings about its applicability to healthcare and financial services. Of course it is widely utilized by government agencies.

HITRUST CSF, released in 2009, was developed with healthcare and information security professionals and is the first security framework targeted specifically for healthcare information. The framework leverages existing, globally recognized standards, including HIPAA, ISO, NIST, and COBIT. Subscription to the framework includes a very interesting tool, called MyCSF, which provides very prescriptive requirements based on the size and type of healthcare organization. The tool also facilitates both a self-assessment and an assessment validated by a certified assessor or auditor.

While this writing does not attempt to be exhaustive in regards to identifying available frameworks, hopefully it provides some useful insights into the benefits of frameworks in general – to help an organization manage its information security program.

— Fernando P. Monteleone, Jr.

New Survey Shows Continued Lack of Executive Confidence in Cybersecurity and Increases in Data Loss

A new survey released by Raytheon and websense, called "Study-Why Executives Lack Security Posture Confidence While Knowing that the Metrics They Use to Gauge it are Ineffective," "reveals that confidence in [executives'] enterprise security posture is lacking." The results of a survey of 100 security executives were that less than a third (31%) of the executives feel "very confident" in the organization's security posture, and "only slightly more than a quarter feel that their communications on security metrics and posture to senior management is effective." The survey revealed that the overwhelming majority (65%) are only "somewhat confident" in their organization's security posture.

Further, those responding to the survey indicated that almost 9-in-10 organizations had at least one

breach in the last year that resulted in data loss or compromise and nearly 1-in-5 have had three to five breaches in the last year resulting in the loss or compromise of data. Data breaches and compromises are not going away.

The authors submit that counting breaches from year to year and using the count as a metric is ineffective and does little to protect the organization from the next breach, particularly when even one breach is costly and damaging. Instead, the survey posits that organizations must look inward and that it is more important to detect how long a threat or attack was inside the organization and measure the effectiveness of the defense to the attack. The conclusion: "it is time for organizations to consider a qualitative approach as part of a comprehensive security program." Agreed. And we would add that the responsibility of a comprehensive security program does not rest with the IT department. A coordinated effort, with C-Suite engagement and robust communication between the two, is essential to combat threats and minimize risk.

— Linn Foster Freedman

Back to Basics: Low Tech Tips to Alleviate High Tech Headaches

It's easy to get lost in the abyss of technical jargon when discussing Electronically Stored Information (ESI). However, good information governance, which is one of the cornerstones of data privacy and security, doesn't have to be complicated. Adherence to a few simple "good housekeeping" principles will go a long way toward minimizing the creation of extraneous data, organizing existing data, and eliminating outdated data, all of which will make any data breach response or e-discovery process that much easier.

- Have a written record retention policy…and enforce it. A record retention policy is only as good as the people behind it. Make sure your organization has an up-to-date policy (one from 1999 isn't going to do the trick), and encourage a culture of compliance.
- Out with the old: The temptation to keep data past its useful life is high. What if you need to remember what was said at that meeting back in 2007? While those notes may help jog your memory they take up valuable space and could expose you to liability or embarrassment (think, Sony emails).
- Draw a map: It's important to know where your data is. If you don't, have your IT department map out all possible repositories of data and identify what type of information resides there. In the event of a breach, this will give you an immediate sense of what was compromised. In e-discovery, it can greatly reduce the scope of collection. And if you don't have one, it's one of the first things your lawyers will be asking you do if either of the above situations occur.
- BYOD policies are your friend: Personal devices being used for business purposes is the new normal. Develop policies surrounding the practice so you know where your data is and can ensure that it is secure.
- Litigation holds are not forever: Litigation holds are serious business, but they don't have to endure years beyond the conclusion of a dispute. Consult with your attorneys to determine when it's appropriate to lift the hold and purge that dated information.

— Andrea Donovan Napp

DATA BREACH

OPM Data Breach Update--$133 Million Contract Awarded to Vendor

The Office of Personnel Management (OPM) and the Defense Department announced this week that a Portland, Oregon based vendor has been selected to assist with breach notification and credit assistance for the almost 22 million individuals affected by the OPM data breaches. The cost? $133 million. Although the services that will be provided to the affected individuals include credit and identity monitoring, identity theft insurance, and identity restoration services for three years, it does not appear to include assistance with credit freezes which, according to Brian Krebs (and this writer), is the only real way to protect oneself (Read Krebs' post here). Think of how far that $133 million would have gone toward enhancing security measures at OPM BEFORE the intrusion. The lesson? Invest in security measures now before you are a victim of an intrusion to save lots of money later.

— Linn Foster Freedman

TELEPHONE CONSUMER PROTECTION ACT

E-faxes Regulated in the Same Way as Conventional Faxes under the TCPA

The Federal Communications Commission (FCC) announced on August 28, 2015, that "e-faxes" are considered the same as conventional faxes when it comes to consumer protections and violations of the Telephone Consumer Protection Act (TCPA) and the Junk Fax Protection Act (JFPA). In its declaratory ruling, the FCC said, "Unwanted fax advertisements can annoy consumers, costing them time and money by way of interfering transmissions, and unplanned uses of paper and toner, as well as wear and tear on equipment… Based on our clarification, consumer will enjoy the same protections from unwanted e-faxes as they do from conventional faxes." The FCC also clarified that this interpretation of the statute focuses on *the sender's means of transmission* and not the ultimate destination.

Additionally, the FCC explained, in support of its ruling, that "e-faxes are just like paper faxes." Even though they do not necessarily result in the same waste of paper or toner, e-faxes "can increase labor costs for businesses, whose employees must monitor faxes to separate unwanted from desired faxes." Businesses: add e-faxes to your list of hazardous promotional materials.

— Kathryn M. Rattigan

DRONES

Support from the LA City Council for More Public Safety Protections against Drone Use

The Los Angeles (LA) City Council (the Council) decided it would join the widespread efforts for more drone legislation, and endorse a series of federal and state legislation related to the use of drones and public safety protections. On August 31, 2015, the Council voted unanimously to support state legislation criminalizing drone usage that interferes with firefighting, medical evacuations, and search-and-rescue operations, and to indemnify emergency responders that damage privately-owned drones in the line of duty. The Council also voted unanimously to support federal legislation requiring drones to have safety features such as "geo-fencing" (or technology that restricts the drones' ability to fly to specific heights and locations) as well as "collision-avoidance software." Lastly, the Council asked the LA fire and police departments to help prepare draft ordinances that would regulate drones within five miles of an airport. This will surely only be the beginning of many more state and federal proposals for drone regulations and privacy protections against drone use.

— Kathryn M. Rattigan

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com