Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

December 10, 2015

ENFORCEMENT + LITIGATION

Wyndham Settles with FTC

We have been following the hard-fought case between the Federal Trade Commission (FTC) and Wyndham over an investigation that was launched by the FTC following a series of data breaches of Wyndham's payment card information between 2010 and 2012 (see related post). Wyndham was the first company to challenge the FTC's jurisdiction to regulate data security measures under Section 5 of the FTC Act. The Third Circuit recently backed the FTC's position.

The FTC alleged that Wyndham's security practices "unfairly exposed the payment card information of hundreds of thousands of consumers to hackers in three separate data breaches."

After the years-long battle, and on the heels of the Third Circuit decision, the FTC announced today that the case has settled. Under the settlement, Wyndham does not pay any fines or penalties, but, consistent with FTC settlements in the past, agrees to implement a comprehensive information security program for cardholder data for 20 years, obtain a written assessment of Wyndham's compliance with the program, and certify compliance annually for the next 20 years to the FTC Bureau of Consumer Protection.

Further, Wyndham is required to deliver a copy of the Order of Injunction to "all controlling principals, board of directors members, and LLC managers and members…all officers, employees, agents, and representatives having responsibilities relating to the subject matter of this Order; …and any business entity resulting from any changes in structure…" for the next 10 years.

Finally, Wyndham must submit a compliance report to the commission in one year that it has complied with all provisions of the Order.

The battle was hard fought and the Order is nearly identical to previous orders entered into with businesses who have suffered data breaches in the past. But in this case, there was no fine or penalty paid to the FTC. Nonetheless, it will be interesting to see how the LabMD case may change the landscape.

— Linn Foster Freedman

Mattel Gets Hit with Class Action over Hello Barbie's Invasion of Children's Privacy

We reported last month about the release of Mattel's new Hello Barbie (and the "Hell No Barbie

Campaign), with the capability to "carry on a conversation" with a child using speech recognition software and storage of conversations in the cloud. This week, in Los Angeles Superior Court, two moms filed a class action on behalf of their minor children against Mattel, ToyTalk, and the kidSAFE Seal Program for talking Hello Barbie's invasion of children's privacy. Plaintiffs, Ashley Archer-Hayes (Archer-Hayes) and Charity Johnson (Johnson), allege that Mattel has caused emotional distress and loss of privacy and that Mattel has misled consumers by stating that the doll (and its technology) complies with the Children's Online Privacy Protection Act (COPPA).

Mattel clearly states on its website that Hello Barbie complies with COPPA requirements; however, Archer-Hayes and Johnson disagree. While COPPA restricts collection of personal information from children under the age of 13 without prior, verifiable parental consent, Hello Barbie can record children's' voices without any such checks or balances; Mattel and ToyTalk should have known, say the plaintiffs, that children would play with the doll with other children, who would also be recorded, without any parental consent or the parents' ability to make choices about what happens to that data that is collected from their children. Plaintiff moms say that the companies should have come up with a process that would recognize when someone other than the Hello Barbie's owner was being recorded and delete those recordings.

Plaintiffs' attorney says, "This lawsuit should not be mistaken for a frivolous complaint over a toy. Providing hackers, who know no bounds in their invasive activities, with potential interactive access to any child or adult in proximity of a doll, is a very serious matter, and dictates the very highest safeguards and warnings available." We will watch and see where this one goes as the case (and the holiday sales season) progresses.

— Kathryn M. Rattigan

CYBERSECURITY

Anonymous Hacks Login Information of Paris Climate Summit Attendees

In what has been described as a response to the arrests of protesters on a climate march in Paris this past Sunday in the midst of the United Nations Framework Convention on Climate Change (UNFCC), the hactivist organization Anonymous has announced that its hackers have successfully hacked into the website of UNFCC and posted the names, telephone numbers, email addresses, usernames, and secret questions and answers of summit attendees onto an anonymous publishing site.

The leaked information is of officials attending the climate summit from the United States, Peru, Switzerland, the United Kingdom, and France.

Security experts report that the intrusion used an SQL injection attack, which is a well-known vulnerability, and the password encryption was also weak.

Although the intrusion is embarrassing, the only reported harm from the posting of the information is if the attendees used the same password on other accounts, so the recommendation is to change passwords if that is the case.

— Linn Foster Freedman

DATA BREACH

JD Wetherspoon Announces over 650,000 Customers' Data Lost in Hacking

JD Wetherspoon, a popular chain of pubs in the UK, notified its customers late last week that it has discovered that its website was hacked between June 15 and 17, which exposed the names, birth dates, telephone numbers, and email addresses of 656,723 customers. The credit card information of 100 of those customers, who purchased a voucher online before August of 2014, were also compromised.

Apparently the data located on the website was not encrypted, but the company said the security codes of the credit card information were not stored on the database. The company has stated that the website has been replaced.

This is not the first report of a hacking incident involving a website. Companies may want to review the security of their website hosting provider and consider strengthening contractual provisions to account for a potential security incident.

— Linn Foster Freedman

VTech in Quagmire Following Data Breach of 6.5 Million Kids' Information

In a third update to the data breach of 6.5 million kids' information and 5 million parents' information, VTech Holdings Ltd. (VTech) is facing backlash from plaintiffs' attorneys and regulators.

First, VTech Electronics North America LLC was hit with the now usual class action suits following a data breach--two so far--filed in the Northern District of Illinois. The suits allege that the toy company failed to safeguard sensitive information of millions of American children and their parents. The information compromised included parent names and email addresses, security questions, and children's names, genders, birth dates, and profile pictures.

The suits seek damages caused by the disclosure of the information and for the overpayment of the products.

But that's not all.

Following the notification, VTech is being investigated so far by the attorneys general of Connecticut and Illinois, the privacy commissioner in Hong Kong, and due to the fact that the breach included minor personal information, it is anticipated that other AGs and the Federal Trade Commission will investigate under the Children's Online Privacy Protection Act (COPPA), which regulates what companies can do to market to kids and what minor information can be collected and shared with others. COPPA includes statutory damages of up to $16,000 per violation.

It will be interesting to see the fallout of these investigations, due to the nature of the data involved and the fact that it includes kids' data, as they are one of the most vulnerable, sympathetic, and protected classes that exists.

— Linn Foster Freedman

Public-Private Team of Security Experts Disrupt Dorkbot Malware

This is how it should be—private companies working with law enforcement to disrupt evildoers on the

Internet. Late last week, Microsoft announced that it teamed up with the Department of Homeland Security, Europol, the FBI, Interpol, the Royal Canadian Mountain Police, the Computer Emergency Response Team Polska, security vendor ESET, and the Canadian Radio, Television and Telecommunications Commission to take down the botnet known as Dorknet. Now that's an impressive team.

Dorkbot, malware that steals login credentials from online services such as Facebook, PayPal, Twitter, GMail, Netflix and eBay, has infected an estimated one million computers worldwide since 2011.

This is the kind of public-private partnership that is necessary to combat the sophisticated online attacks that are affecting businesses worldwide. It is effective when security experts from the private industry lend a hand to those combating crime and will hopefully encourage others to do the same.

— Linn Foster Freedman

DATA PRIVACY

The Office of Management and Budget Announces the Establishment of a New Federal Privacy Council

On December 2, 2015, the Office of Management and Budget (OMB), announced a new initiative that is being developed to ensure that government agencies are putting the proper privacy protocols in place. Specifically, Shaun Donovan, the director of OMB, announced the creation of a new federal privacy council. The purpose of the council will be to make policy recommendations, establish best practices, and foster a community of privacy professionals within the federal government.

The Privacy Council will be modeled after the federal Chief Information Officers (CIO) Council—a group of agency CIOs that work together to advise on IT priorities.

“It’s time to stop reinventing the privacy wheel at agencies and do a better job of leveraging the success of each agency’s related efforts,” said Donovan, who made the announcement at the recent federal privacy summit in Washington. “It’s time to shift from reactive programs to proactive strategies. It’s time to professionalize the privacy profession. The privacy council will serve as an ecosystem for strategic thinking on privacy implementation, bringing together the best minds we have to tackle cutting edge issues in the digital area. It will be the place to coordinate and share ideas, best practices and successful practices for protecting privacy across the government. And like the CIO Council, this council will assess and develop recommendations for the attracting and hiring of top talent in privacy programs across the federal government.”

The CIO and OMB councils will work in tandem, as the two areas often overlap. “Privacy and security may be two different disciplines, requiring two separate skill sets but they must be part of one coordinated risk management framework,” he said. “The work of the two councils will complement each other and promote more efficient and effective programs for both privacy and IT security.”

The OMB council will form in early 2016. According to Marc Groman, OMB’s senior adviser on privacy, after creating the governing documents, the council’s first priorities will be to increase the talent pool around privacy; enhance privacy-related training, education, and professional development for current employees; and create a community of practice among privacy professionals.

— Kelly Frye Barnett

WEEKLY PRIVACY TIP #13

Web Trackers: What Others May Know About Your Online Footprint

Web Trackers have been a hot topic in recent news, yet most of us are oblivious not only the extent they are used, but also to the potential for misuse of our personal information currently being aggregated in countless databases around the world.

On the day of this writing, I searched for “cordless drill” on the websites of three very familiar, top 20 global retailers and counted a total of 171 trackers. These trackers are essentially programs that execute when a website page is visited or some action is taken by the user, such as performing a search or clicking on a link or an item of interest. The programs are generally written by companies that benefit financially through targeted advertising or by the sale or use of the aggregation of the data (i.e., “Big Data” —large databases typically analyzed to identify patterns or trends in human behavior). With the exception of a hijacked website, trackers that exist on any given website are the products of the website owner or their invited partners or affiliates.

Most of us have experienced a targeted ad (e.g., for a cordless drill) while on Facebook and concluded that it was in connection to a previous search for that item on another site. Some of us may generally be OK with tracking for that purpose. But would we be OK knowing that a database may contain much more personal information, such as finances, health, religious beliefs, political affiliation, race, ethnic background, or even sexual preferences? Would it concern you even more if these tracker programs were recording our Internet activity over time and establishing long-term profiles of us on an individual basis?

Many of us think that we are surfing the web anonymously, but is that really true? There have been numerous reports and research studies over the past decade which show how personal identity could be obtained by Web Trackers—even when no personal website login information was entered. As social media was becoming extremely popular, representatives from AT&T Labs and Worcester Polytechnic Institute published a research paper making it clear that default settings of many social networking applications caused Personal Identifiable Information (PII), such as our name, location, gender, activities, employer, and even our friends list, to be accessible to tracker programs. More recently, it was discovered that simply surfing the web from a device associated with a major cellular provider exposed personal account information to trackers, essentially connecting “anonymous” web activity to an individual.

In fairness, most of the sites we visit on a regular basis publish and comply with their information privacy policies—generally limiting use of the data to targeted ads and/or broad, non-personal, categorizations of aggregated data. Google, for example, currently has only one tracker (owned by Google) that executes when a search is performed. Based on their information privacy policy, their tracker program would essentially just record the interest in a cordless drill (using the same example as above). While they would also likely record geolocation of the user and other categorical information that would be useful for data analytics and general marketing, they do not associate the activity with an individual. On the other hand, if a typical retail website has fifty or more trackers, most of which are third-party owned, how can you feel comfortable that the actual data recorded and its use will be consistent with the information privacy policy of the site owner?

While concerned end users, security researchers, and lawmakers, will continue to identify unscrupulous behaviors and effect change consistent with our collective privacy interests, I would like to leave you with a few suggestions to help you take matters into your own hands. First and foremost, review and revise any available privacy settings to meet with your comfort level (e.g., limit sharing of name and location information to your friend list) and know the information privacy policies of all your social network applications and any applications/websites that you use to record or share personal information. Find and install tools that make Web Trackers visible to you and, more importantly, allow you to selectively block them from embezzling your personal data. Consider the Ghostery Browser Extension, which is highly rated

by users and free.

Wishing you all a happy holiday season and safe web surfing.

— Fernando P. Monteleone, Jr.

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

---