August 27, 2015

Data Privacy + Security Insider

DATA BREACH

Ashley Madison Fallout: Class Actions, Pentagon Investigation and Easily Searchable Data

We previously reported that hackers The Impact Team has posted legitimate detailed information about 36 million adultery website Ashley Madison users. In the wake of the shocking posting of the data last week, two class action lawsuits were filed against Ashley Madison parent company Avid Dating Life the day after the posting in Canada for failing to protect the information of its clients and falsely advertising that it would remove all record of use from its databases. The named plaintiff is a widow who joined the site after he lost his wife of 30 years.

Widespread reports are that the data is easily searchable, and has revealed keys to users' email addresses and sexual preferences. Although the company has pledged to try to scrub the data from the Internet, the links have gone viral, which will make it very difficult. Security experts warn and have confirmed that the data has been used to try to blackmail users.

Among those concerned are bankers and military personnel. It has been reported by security firms that have searched the website that over 600 bankers' work email addresses were used to register on the site (although they could be fake as email verification was not required), and several well-known banks have had to issue "no comment" press releases after the banks were publicly named.

After reports that there were over 15,000 .mil email addresses included in the database, the U.S. Department of Defense launched an investigation into the use of military emails by military personnel to sign up for Ashley Madison accounts. Adultery is a crime under the Uniform Code of Military Justice.

In the meantime, Avid Life is working with law enforcement and is offering a $500,000 reward for information leading to the arrest and prosecution of those responsible.

— Linn Foster Freedman

Web.com Suffers Data Breach Affecting 93,000 Customers

The list of companies hit by cyber-attacks continues to grow. This time, Florida-based web hosting company, Web.com, has announced that it suffered a data breach that may have compromised credit card information and other personal information belonging to about 93,000 of its customers.

Web.com provides a variety of online services, including website and Facebook page design, e-commerce and marketing solutions, domain registration and Web hosting. The company claims to have over 3.3 million customers and owns two other well-known Web services companies—Register.com and Network Solutions—neither of which was affected by the breach.

According to the company, the breach was detected on August 13 and has since been resolved. The company uncovered the unauthorized activity through its ongoing security monitoring. It did not specify how the intruders gained access to its systems, but stated that it has contacted law enforcement and hired a "nationally recognized" IT security firm to conduct a thorough investigation. The company is also offering a year of free credit monitoring to those affected by the breach.

"Web.com has very strong and sophisticated security measures in place to protect our computer systems and we regularly review and update our security protocols," the company said in a FAQ published on its site. "Unfortunately, cybercrime is a persistent threat in today's world. Despite our best efforts, no business is immune."

Since the disclosure of the breach, stock in Web.com has tumbled nearly 10 percent.

— Kelly A. Frye

OPM Breach Update

In response to the massive OPM data breach, the government has been searching for a vendor to provide identity protection services for the almost 22 million individuals affected. Bids were due last week, and the chosen vendor will have 12 weeks to send out the notification letters. That means that some individuals might not even know that their data was compromised until close to Thanksgiving, and the information is likely to have been used by then.

Security experts advise that federal government employees and those who sought high security clearance should assume that their information was included in the breach and to take matters into their own hands—place a credit freeze on all accounts now to try to mitigate the risk of identity theft. It is already delayed and waiting until receipt of the notification letter may be too late.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Third Circuit Affirms FTC's Jurisdiction Over Security Practices in Wyndham Case

In a strongly worded opinion, the Third Circuit Court of Appeals on Monday slammed Wyndham Worldwide Corporation's arguments that the FTC did not have jurisdiction to enforce the security practices of businesses following a data breach. The Court noted that it found most of Wyndham's arguments "unpersuasive." This is the first Circuit Court of Appeals case to opine on the FTC's jurisdiction in data security matters.

Wyndham was the first company to challenge the FTC's jurisdiction after it suffered a series of breaches between 2008 and 2010. LabMD took up the gauntlet thereafter and continues its battle against the FTC. The crux of the argument was that Wyndham was a victim of crime, and the FTC did not publish any regulations or guidance on data security in order for the companies to understand that the FTC could regulate their security practices and bring enforcement actions against them for lax security practices. The FTC has strongly disputed the allegations and has expanded its enforcement role over the security practices of companies following data breaches under Section 5 of the FTC Act, arguing that if a company tells consumers in its Privacy Policy that it will keep customers' data secure, and then it doesn't, such is an unfair or deceptive business practice that subjects it to FTC enforcement. The Court rebuffed Wyndham's citing of a dictionary that its practice is only unfair if it is "not equitable" or is "marked by injustice, partiality, or deception" by stating "[A] company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes unsuspecting customers to substantial financial injury, and retains the profits of their business."

After the Court issued its opinion, FTC Chairwoman Edith Ramirez stated in a press release that the decision "reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information."

— Linn Foster Freedman

Three More Darkode Hackers Prosecuted

We previously reported on the prosecutions of Darkode members. Three more members of the computer hacking forum Darkode have pled guilty to accessing protected computers without permission, and for violating the CANSPAM Act. All three (in addition to 9 others prosecuted several weeks ago) were part of a scheme to scan for and infiltrate internet routers that were not protected by adequate security measures. The scheme allowed them to install malware onto routers that then automatically sent messages to cell phone numbers which contained a fake link to a Best Buy card. When a cell phone user clicked on the link, they were directed to a page that then asked for their personal information. The hackers were paid according to how much information was shared through the link.

Twelve members of Darkode have been charged in the scheme. The government says Darkode is one of the most sophisticated English-speaking forums for hackers.

— Linn Foster Freedman

Big Win for Telemarketers: Courts Rule That Consumers Consented to Calls and Texts by Providing Number to the Companies

On August 21, 2015, the 11th Circuit upheld the dismissal of a class action against DCI Biologicals, Inc. (DCI) for its alleged violations of the Telephone Consumer Protection Act (TCPA). DCI is a blood plasma collection center, and a blood plasma donor, Joseph Murphy, alleged that DCI sent him unsolicited text messages using an autodialer. However, the Court found that by providing his cell phone number on the donor information form, he provided prior express consent. The Court said, "Under [the TCPA], and the FCC's interpretation of the prior express consent, Mr. Murphy's provision of his cell phone number constituted his express consent to be contacted by DCI at that number." Perhaps an important factor in this determination was that the form did not ask for a cell phone number and did not require a phone number in order for Mr. Murphy to donate blood plasma. Mr. Murphy voluntarily provided his cell phone number to DCI and DCI's first text message to Mr. Murphy said, "You will receive MMS messages from

DCI Biologicals on short code 76000. Reply STOP to 99000 to cancel." Mr. Murphy never replied and supplied his own cell phone number directly to DCI himself.

At the same time, the 6th Circuit ruled in favor of mortgage debt collector, Homeward Residential Inc. (Homeward), stating that a debtor who provides a cell phone number to a creditor has consented to receiving telemarketing calls. Even though Homeward had called plaintiff, Stephen M. Hill, over 500 times, the court determined that "a debtor consents to calls about 'an existing debt' when he gives his number 'in connection with' that debt." This is a big step forward for companies who face class actions for alleged TCPA violations.

— Kathryn M. Rattigan

IRS Sued In Putative Class Action for Lax Security

Following the IRS' admission that its data breach was actually larger than it originally reported and caused fraudulent tax returns to be filed affecting over 330,000 taxpayers, the IRS was sued this week in a proposed class action for failing to prevent the data breach.

The suit outlines that the IRS was aware that taxpayer information was not properly secured, though the Government Accountability Office and the Treasury Inspector General reports warning the IRS of its inadequate security. The plaintiffs allege that the IRS ignored the reports and stated "As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of sensitive information against unauthorized access or loss."

— Linn Foster Freedman

CYBERSECURITY

Data Detecting Dogs: The FBI's Newest Tool in Fighting Cyber-Crime

The FBI's latest weapon in locating electronic evidence is not a computer program, it's a dog. The FBI is using data-sniffing dogs in raids to cut down on the time it takes agents to locate small hidden data storage devices.

The FBI has used one such specially-trained dog, Bear, in a number of raids to look for hidden electronic evidence. Bear's Kentucky trainers, Tactical Detection K9, worked with scientists to isolate scents that are associated with motherboards in small storage devices. Bear trained for over a year to detect those scents. He can sniff out micro SD devices, thumb drives, external hard drives and other miniscule external storage devices that potentially contain important electronic evidence. Now when federal agents conduct raids to locate tiny data storage devices, some as small as a finger nail, Bear can find the target evidence in minutes.

Just as a body of case law has developed concerning the use of drug-sniffing dogs, we can expect that case law will begin to develop about the use of data-sniffing dogs in the near future.

— Nuala E. Droney

NIST Issues Cybersecurity Practice Guide for Electric Utilities

Yesterday, the National Cybersecurity Center of Excellence issued its NIST Cybersecurity Practice Guide, Draft Special Publication 1800-2 "Identity and Access Management for Electric Utilities."

The Guide is a result of collaboration between NIST and utilities stakeholders, including the energy sector and technology vendors, to design an example solution to help energy companies manage and control access to networked resources, including buildings, equipment, information technology and industrial control systems through a centralized platform.

The solution uses the NIST security standards and framework, and is consistent with the North American Electric Reliability Corporations' Critical Infrastructure Protection standards.

Comments to the Guide are open until October 23. Comments can be submitted online or via email to energy_nccoe@nist.gov.

— Linn Foster Freedman

Roger Williams Law School Hosts Annual Cybersecurity Conference

Roger Williams Law School has announced that it is hosting its annual Cybersecurity Conference on Friday, October 16, 2015 at its campus located in Bristol, Rhode Island.

Numerous speakers from the public and private sectors have confirmed attendance, and it promises to be packed with interesting panels discussing cutting-edge issues in cybersecurity. For more information, visit the conference website.

— Linn Foster Freedman

DRONE PRIVACY

FAA's Commercial Drone Application Process to Be Audited by the DOT

While by law, any aircraft operation in the national airspace requires a certificated and registered aircraft, a licensed pilot, and operational approval, § 33 of the FAA Modernization and Reform Act of 2012, permits the FAA to allow waivers for commercial drone use. On August 20, 2015 the U.S. Department of Transportation (DOT) announced that it will audit the Federal Aviation Administration's (FAA) current processes for commercial drone use applications.

While the DOT Office of the Inspector General understands that the use of drones is beneficial for many commercial avenues, such as agriculture, filmmaking, and the insurance industry, he is concerned that the FAA's processes are too lax since an increasing number of applications for commercial drone use are receiving approval. The FAA has approved over 1,200 applications since last September.

The number of drone related incidents has also increased to an average of about 60 incidents per month–the DOT says that it is these "significant and complex challenges" of safety that warrant this audit. The DOT's audit announcement said, "Some of the incidents did not pose a safety risk, but others have involved reports of pilots altering course to avoid [drones]." The DOT's audit will begin this month.

— Kathryn M. Rattigan

Royal Navy Warship Launches 3D Drone

University of Southampton engineers recently launched a 3D-printed unmanned aerial vehicle from a Royal Navy warship to show the potential use of lightweight drones during sea missions.

The 3D drone weighed 3kg and had a wing-span of 1.5 meters. It was created on a 3D printer in four parts and was assembled without the use of any tools.

The drone flew 500 meters before landing on a beach, using a pre-programmed route. Pretty amazing.

— Linn Foster Freedman

DATA PRIVACY

FTC Issues Statement on Its Enforcement Abilities Under § 5 of the FTC Act

On August 13, 2015, the Federal Trade Commission (FTC) issued a statement on its ability to prosecute 'unfair trade practices' and enforce violations under § 5 of the FTC Act. The guidance said:

"Section 5's ban on unfair methods of competition encompasses not only those acts and practices that violate the Sherman or Clayton Act but also those that contravene the spirit of the antitrust laws and those that, if allowed to mature or complete, could violate the Sherman or Clayton Act. Congress chose not to define the specific acts and practices that constitute unfair methods of competition in violation of Section 5, recognizing that application of the statute would need to evolve with changing markets and business practices."

Without adding any specific examples or discussing its actual approach to exercising its authority under § 5, the FTC seems to be suggesting that it will continue to exercise broad power over any industry that it believes is using 'unfair trade practices.' Businesses beware, particularly in light of the recent Third Circuit ruling in the Wyndham case.

— Kathryn M. Rattigan

SOCIAL MEDIA

Social Networking Service, MeetMe, Inc., Settles Minors' Privacy Violations for $200,000

On August 19, 2015, MeetMe, Inc. (MeetMe), a social networking website and mobile app, agreed to pay $200,000 and to change its privacy policies to settle a lawsuit alleging that MeetMe distributed teenagers' geolocation and personal information, without consent, to predators, stalkers, and advertisers. The allegations were filed by the city of San Francisco, charging MeetMe with violations of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200.

MeetMe has over 122 million users and introduces users to other people who are using the website and

mobile app by sharing users' geolocation so that users can see other MeetMe users who are nearby. MeetMe also shares geolocation and personal information with third party vendors for targeted advertising.

The Office of the City Attorney said, "Our settlement includes groundbreaking steps to protect the safety and privacy of minor teenagers, just as we'd hoped. But MeetMe deserves credit for also seeing the opportunity to expand and better explain privacy protections for the benefit of all of its users, of all ages."

More specifically, MeetMe agreed to stop identifying minors' locations beyond their city and state, and also agreed to limit sharing of minors' proximity to other users to at least one mile away. MeetMe will also start providing "just in time notifications" to allow users more choice about data sharing and will simplify its privacy policy to be written at a 9th grade reading level.

This is a valuable lesson for all websites and mobile apps that are collecting data from their users; implement these provisions from the start and you may be able to avoid payouts like this.

— Kathryn M. Rattigan

First "Right to be Forgotten" Enforcement Action Levied Against Google

The U.K. Information Commissioner issued an order to Google this week requiring it to remove nine search results of an individual's minor criminal offense that was committed close to ten years ago. This is reported to be the first enforcement action since the European Court of Justice held that EU citizens had the right to compel internet search engines to remove links to websites that reference personal information of citizens if the citizen's right to privacy outweighs the public's interest in the right to have access to the information.

The Information Commissioner indicated that the links requested to be removed were subject to data protection rules and the links shouldn't include the personal information of the subject as it was no longer relevant.

Google has not indicated whether it will appeal the order or not.

— Linn Foster Freedman

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.
