Robinson+Cole

Data Privacy + Security

June 18, 2015

Data Privacy + Security Insider

DATA BREACH

The U.S. Office of Personnel Management Suffers Largest Breach in U.S. Government History

The United States Office of Personnel Management (OPM) disclosed that it was the target of what has been described as the largest breach in U.S. government history, affecting the personal information of up to 14 million current and former federal employees, a far higher figure than the 4 million the agency initially disclosed. Officials believe that the intrusion originated in China and suspect that it was state sponsored, claims the Chinese government has steadfastly denied. A foreign government can use the stolen personnel records to blackmail, impersonate, or otherwise exploit those affected as a way to gain access to U.S. secrets or entry into government computer networks. The American Federation of Government Employees believes the hackers stole Social Security numbers; military records and veterans' status information; addresses; birth dates; job and pay histories; health insurance, life insurance, and pension information; and age, gender, and race data.

Officials also discovered that deeply personal information submitted by U.S. intelligence and military personnel for security clearances—such as mental illnesses, drug and alcohol use, past arrests, bankruptcies, and more—is in the hands of hackers also linked to China. Officials say that the hack into the security clearance database is separate from the breach of federal personnel data announced last week and that it is unclear whether the security database breach happened when OPM's computer networks were breached in 2013, an attack that was discovered in July 2014.

The recent breach comes only a few months after OPM's Office of the Inspector General harshly criticized OPM for its lax security in a November 2014 report on the agency's compliance with the Federal Information Management Act. The report found "significant" deficiencies in OPM's IT security program. Specifically, it noted OPM's lack of encryption and the agency's failure to tract its equipment. It also found that OPM failed to maintain an inventory list of its servers and databases and had no knowledge of all the systems that were connected to its networks. OPM also failed to use multifactor authentication for workers accessing the systems remotely from home or on the road.

–Kelly A. Frye

Medical Informatics Engineering Discloses Data Breach

Electronic health record (EHR) vendor Medical Informatics Engineering and its subsidiary,

NoMoreClipBoard, a personal health record (PHR) product, notified its EHR clients and PHR individuals that it has been the victim of a sophisticated cyber-attack resulting in the unauthorized access to its system and data. The web-based electronic medical record system information that was breached involves patient data, including names, mailing addresses, e-mail addresses, dates of birth, some Social Security numbers, lab results, dictated reports, and medical conditions.

The exposed PHR information, stored through NoMoreClipBoard, includes names, addresses, usernames, hashed passwords, security questions and answers, e-mail addresses, dates of birth, health information, and Social Security numbers—the complete treasure trove of a consumer's most sensitive information. Those individuals notified of this breach should take special care in proactively protecting themselves, including changing their passwords and security questions that may have been used for other sites or purposes.

The companies are offering affected individuals credit monitoring and identity protection services for 24 months.

–Linn Foster Freedman

ENFORCEMENT + LITIGATION

First Suspected Domestic Corporate Espionage Hacking Incident Happens on the Baseball Diamond

This story should tell you something: hacking doesn't only happen in department stores and hospital databases. Now, the Federal Bureau of Investigation (FBI) is investigating front office officials for Major League Baseball's (MLB) St. Louis Cardinals. These front-office officials allegedly hacked into the internal networks of one of its rival teams, the Houston Astros, to gain access to information about player personnel. The information included internal discussions about trades, proprietary statistics, and scouting reports and was part of a large collection of "baseball knowledge." This baseball knowledge was organized using a computer program that took all the different statistical variables about players and weighted "them according to the values determines by the team's statisticians, physicists, doctors, scouts, and coaches." While not much has been revealed so far about this FBI investigation, subpoenas have been served upon the Cardinals and the MLB itself. An MLB spokesman said, "[We] have been aware of and [have] fully cooperated with the federal investigation into the illegal breach of the Astros' baseball operations database." The MLB commissioner will likely wait until after the investigation is concluded to determine whether disciplinary action is necessary against the team.

–Kathryn M. Sylvia

Advocate Health Data Breach Class Action Suit Dismissal Upheld by Appellate Court

In August 2013, four computers of Advocate Health and Hospitals Corporation (Advocate Health) were stolen from one of its offices. The computers contained the names, dates of birth, Social Security numbers, health insurance information, diagnoses, Medicare and Medicaid information, and diagnosis codes of approximately 4 million patients.

Several class action cases were filed against Advocate Health following the breach, and the cases were dismissed by the trial courts for lack of standing, as the plaintiffs had failed to establish an injury in fact. The dismissals were appealed.

On June 2, 2015, the Illinois Appellate Court affirmed the dismissal of the suits, stating “[H]ere, plaintiffs’ allegations of injury are clearly speculative, and, therefore, they lack standing to bring suit.” The Court further held that the allegations of injury set forth in the complaints, including an increased risk of identity theft, are speculative and conclusory, as the plaintiffs did not allege that they actually were the victims of identity theft. Illinois law requires the showing of a “distinct and palpable injury” in order to move forward with a claim.

This holding is consistent with other standing cases that have been decided in both federal and state court cases and expands the precedent in this area.

–Linn Foster Freedman

Adobe Settles Proposed Class Action Data Breach Case with Award of $1.18 Million for Plaintiffs' Attorneys

Adobe Systems, Inc., has agreed to settle the proposed class action lawsuit filed against it following the breach of its system in 2013. The breach compromised the personal and payment card data of millions of its customers. There were no allegations of actual damage or identity theft as a result of the security breach.

The settlement awards $5,000 to each named plaintiff and attorneys' fees of $1.18 million. Adobe has agreed to implement additional security measures and to submit to an independent security audit to ensure it has implemented the security measures. Sounds like a lot of attorneys' fees for no claimed damages.

–Linn Foster Freedman

LinkedIn Settles Class Action Suit

Last week, LinkedIn agreed to pay $13 million and change some of the site's features to settle a class action lawsuit filed against it in 2013 alleging that it used the Add Connections feature to access users' e-mail contacts to send invitations to users' contacts without their consent.

The allegations of the suit include that LinkedIn accessed and collected e-mail addresses from users' contacts and then sent e-mails that looked as if they were from the user to the contacts, who were not LinkedIn users, to persuade them to sign up to LinkedIn. LinkedIn argued that permission was granted by users when they signed up for LinkedIn.

In addition to the monetary settlement, LinkedIn has agreed to enhance the user permission process for the use of contact information, including a new screen stating that LinkedIn will “import your address book” if a user elects to use the service, which will “upload detailed information about your contacts to our LinkedIn servers.”

Of course, LinkedIn will mine that data and use it for its own marketing purposes (a brilliant strategy that is widespread). Do you want LinkedIn to upload your entire address book? And how do your contacts feel about having their complete contact information uploaded to LinkedIn for marketing purposes? When I explain these features to my friends and colleagues, some of them are appalled but have unwittingly agreed to them because they never read the terms of use and just hit “I agree.” When you agree, you are agreeing to all of that fine print.

I was in Seattle speaking at a cybersecurity conference, and I offered to find a restaurant for dinner for my co-panelists. I accessed a popular app on my smartphone to find the hot spots in Seattle. A screen came up that said “oops! Your location services are not on, so go to settings and turn them on to use this app” or something like that. Of course, to protect my privacy, I never have my location-based services on. I did not want the app to have my exact location for that purpose, so I chose to go to another site that did not require that I tell them exactly where I was at that exact time. I found a great restaurant and we ate well. The point is, I had the choice of sharing or not sharing my data and location and I made it. Be aware of your choice when using apps.

Many apps have the same feature. It is important to read the pop-up screens and terms of use so you know how these apps are using your data.You have the clear choice of how you want your data, including your entire address book, used by companies. Don't just click “I agree.” Know what you are agreeing to before you grant your permission.

–Linn Foster Freedman

Oral Argument Scheduled in Microsoft Foreign Data Demand Appeal

The U.S. Second Circuit Court of Appeals scheduled oral argument for September 9, 2015, on Microsoft’s appeal of a district court opinion upholding the validity of the U.S. government’s search warrant for customer data stored on computers of Microsoft’s affiliates outside the United States. The customer data sought is in Ireland at a data center operated by a Microsoft subsidiary. The data involves evidence relevant to a pending drug and money laundering case in New York.

The U.S. government’s position is that the Stored Communications Act permits the government to seize private e-mails and other user-generated data stored in data centers outside the United States without having to obtain an order from the courts of the foreign country. Microsoft disagrees. However, Microsoft was unable to persuade a U.S. magistrate judge or a U.S. District Judge in the Southern District of New York of its position. Microsoft has appealed the case to the Second Circuit. The case is being watched closely by the cloud computing community, who are concerned that foreign companies will stop working with U.S.-based cloud providers. The concern is that the data of foreign companies and governments on non-U.S. servers will be subject to the U.S. government’s reach if the servers are owned by a U.S. cloud provider.

More than a dozen *amicus* briefs in favor of Microsoft’s position were filed by a diverse group of companies and organizations, including cloud computing, software and other technology companies, the Chamber of Commerce, and the ACLU. The case is also being closely monitored by foreign governments and companies.

See “Microsoft versus the Federal Government; Round Three” for more discussion of the case. *See In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation 14-2985*.

–Kathleen M. Porter

DIGITAL ASSETS

Connecticut General Assembly Fails to Pass Digital Assets Act

In its most recent legislative session, which ended this month, the Connecticut General Assembly failed

to pass Connecticut's proposed version of the Uniform Fiduciary Access to Digital Assets Act (UFADA). Fiduciaries are charged with the responsibility to collect, protect, and preserve the assets of a deceased or incapable individual. In modern life, electronic and digital assets are increasingly as important and valuable as physical assets. However, most agreements that govern online account access do not permit a fiduciary to access or utilize the account. Lack of access can lead to a substantial financial loss. Equally important in many respects is the sentimental value of certain digital assets. Social media accounts are often terminated or frozen upon the death of the account holder. Denying access to these accounts can cause greater emotional distress for an already grieving family.

Unfortunately, the law continues to lag far behind the reality of modern economic and social life. Any fiduciary acting on behalf of the individual has the power and duty to manage and control assets to the same extent the individual could manage and control the assets. Traditional brick-and-mortar banks and brokerage firms have ample experience dealing with fiduciaries. They have adopted policies and procedures that mitigate the risk of improper use or access by a fiduciary. The law and the courts have been successfully managing these risks for centuries. However, industry providers of electronic and digital accounts seem paralyzed by fear of the risk of privacy breaches if a fiduciary access is required. Significant progress needs to be made to ensure that fiduciaries have the power to manage, protect, and control all of an individual's assets, including digital and electronic assets, while still addressing privacy concerns.

–Kelley Galica Peck

HIPAA

Health Care Worker Sent to Jail for HIPPA Violations

When we train employees on HIPAA, we always remind them that HIPAA violations carry significant penalties—both civil and criminal. Our favorite line is "Keep your day job." Stealing patient information is never worth the consequences.

Stacy Laulu, a previous employee of Providence Alaska Medical Center (Medical Center) learned that lesson the hard way. She was recently sentenced to serve two 24-month prison terms concurrently for unauthorized disclosure of two patients' health information.

Laulu was employed as a financial counselor at the Medical Center. Her husband was a close friend of Stuart Seugasala and a co-defendant with Seugasala in a previous federal drug case. Saugasala kidnapped and sexually assaulted a victim and shot another individual, both of whom became patients at the Medical Center. The HIPAA violation occurred when Laulu looked into the patients' records to see what the victims had told the police and the extent of their injuries and texted the information to Seugasala at his request.

Saugasala was convicted of the crimes against the two patients, and Laula was convicted and sentenced for the HIPAA violations. Justice served.

–Linn Foster Freedman

To get more thoughtful and timely discussions of legal news and perspectives on various 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

---