PRIVACY AND SECURITY DEVELOPMENTS

By Daniel J. Solove + Paul M. Schwartz

Issue 2014 No. 1

We spend a lot of time staying up to date so we can update our casebooks and reference books, so we thought we would share with you some of the interesting news and resources we're finding. We plan to post a series of posts like this one throughout the year.

For a PDF version of this post, click here.

GENERAL DEVELOPMENTS

Privacy Legislation

ZwillGen, *List of Privacy Laws Taking Effect in January 2015* (2014) [Link]
- California Digital Eraser Law
- Amendment to California's Anti-Paparazzi Law
- Amendment to California's Revenge Porn Law (adding a private right of action)
- Delaware Data Destruction Law

California Attorney General, *California Privacy Legislation Enacted in 2014* [Link]
List of 10+ statutes pertaining to privacy and data security enacted by California in 2014

Covington Privacy Blog, *Ten Ways the 2014 Election May Affect Privacy and Data Security Law* (2014) [Link]

Studies and Reports

IAPP Study, *Benchmarking Privacy Management and Investments of the Fortune 1000* (2014) [Link]
- "38% of respondents said they would likely increase their privacy budget in the next year."
- The "Fortune 1000 spends roughly $2.4 billion on managing privacy."
- IAPP grew from 10,000 members in 2012 to projected 20,000 members by the end of 2014.

Pew Internet Research Project, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, (Nov. 12, 2014) [Link]
- 91% of adults in the survey "agree" or "strongly agree" that consumers have lost control over how personal information is collected and used by companies.
- 64% believe the government should do more to regulate advertisers, compared with 34% who think the government should not get more involved.
- Only 36% "agree" or "strongly agree" with the statement: "It is a good thing for society if people believe that someone is keeping an eye on the things that they do online."

Daniel J. Solove, *People Care About Privacy Despite Their Behavior* (Nov. 12, 2014) [Link]
Post about the Pew study

Other Stuff

Oliver Stone Movie About Edward Snowden [Link]
Oliver Stone starts filming in Munich in January. Joseph Gordon-Levitt will play Snowden.

Terms of Service: A Graphic Novella on Big Data [Link]
Features Daniel Solove, Scott Peppet, Paul Ohm, danah boyd, Alessandro Acquisti

New Books and Scholarship

David Rose, *Enchanted Objects: Design, Human Desire, and the Internet of Things* (2014) [Link]
Extols the virtues and promise of the Internet of Things.

Jim Dwyer, *More Awesome Than Money: Four Boys and Their Heroic Quest to Save Your Privacy from Facebook* (2014) [Link]
Story of four undergrads who tried unsuccessfully to build a social media site called Diaspora where people could control their personal data.

Sue Halpern, *The Creepy New Wave of the Internet*, NY Review of Books (2014) [Link]
Reviewing four books about privacy and personal data, including the two books above.

PRIVACY AND THE MEDIA

***Austin v. Preston County. Comm.*, Case No. 1:13-cv-135 (N.D.W. Va. 2013)** [Link]
Employee of county animal shelter created a Facebook page for the shelter, but did so through her personal Facebook account. She wrote posts critical of the shelter, and the shelter asked for her password. She refused to provide it and was fired. She sued. The court dismissed her First Amendment claim because she was speaking as an employee, not as a public citizen.

Although a state statute prohibits firing an employee for not providing a social media account password to a personal account, this page was the shelter's page even though she created it from her personal account.

Daniel J. Solove, *Should Celebrities Have Privacy? A Response to Jennifer Lawrence* (Nov. 17, 2014) [Link]

PRIVACY AND LAW ENFORCEMENT

FBI Complains About "Going Dark"
The FBI expressed concern that without having technological abilities to intercept and decipher encrypted communications, it would be "going dark" and not be able to conduct legally-authorized investigations of crimes with warrants or court orders.

***United States v. DiTomasso*, 2014 WL 5462467 (S.D.N.Y. Oct. 28, 2014)** [Link]
Holding that AOL's terms of service waived users' 4th Amendment rights. The policy stated that AOL monitors for criminal activity and that it reserves the right to reveal criminal activity to law enforcement. The court held that "a reasonable person familiar with AOL's policy would understand that by agreeing to the policy, he was consenting not just to monitoring by AOL as an ISP, but also to monitoring by AOL as a government agent."

NATIONAL SECURITY AND FOREIGN INTELLIGENCE

PCLOB Event, *Defining Privacy* (Nov. 12, 2014) [Link]
A group of privacy and security experts spoke at this event, including Professor Solove. The C-SPAN recording of the event is archived online at the link.

U.S. Marshals Use of "Dirtboxes" on Passenger Planes [Link]
A "dirtbox" is a piece of equipment that mimics a cell phone tower, tricking cell phones into reporting in with user data. The DOJ is said to have been allowing the U.S. Marshals Service to use dirtboxes to ping passenger airliners since 2007 to track suspected criminals.

HEALTH PRIVACY

HIPAA

HHS OCR, *Bulletin: HIPAA Privacy in Emergency Situations* [Link]
In light of the Ebola scare, this bulletin provides guidance about HIPAA's rules for sharing PHI in emergency situations.

HIPAA Criminal Enforcement Ramping Up [Link]
Christopher Lykes, a South Carolina state employee who unlawfully accessed 228,000 patient health records, was sentenced to 3 years probation and 300 community service hours. Other criminal sanctions imposed under HIPAA included Huping Zhou who improperly accessed PHI of celebrities being treated by the UCLA Healthcare System. Zhou was the first person imprisoned for violating HIPAA. In 2013, Helene Michel was sentenced to 12 years in prison for ID theft, Medicare fraud, and HIPAA violations. A pending HIPAA criminal case involves charges against Joshua Hippler, who allegedly disclosed PHI for personal gain.

***Byrne v. Avery Center for Obstetrics and Gynecology*, No. 18904, 2014 WL 5507439 (Conn. Nov. 11, 2014)** [Link]
Bryne received medical care from the Avery Center, while in a personal relationship with Andro Mendoza. Bryne warned the Avery Center not to release her medical records to Mendoza. Mendoza later filed a paternity suit, and the court issued a subpoena to the Avery center to appear with Bryne's medical records. The Avery center mailed a copy of the medical forms to the court. Byrne claimed that the disclosure of the medical forms was not done properly under HIPAA and that she should have been notified of the subpoena.

As a result of the disclosure, Bryne filed suit for breach of contract, negligently releasing her medical file without authorization, negligent misrepresentation of the Center's privacy policy, and negligent infliction of emotional distress.

The Connecticut Supreme Court held that HIPAA could be used as a basis in establishing the standard of care for negligence. According to the court, "to the extent it has become the common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records pursuant to a subpoena."

Daniel J. Solove, *Lawsuits for HIPAA Violations and Beyond: A Journey Down the Rabbit Hole* (Nov. 18, 2014) [Link]
Post about *Byrne v. Avery Center*

***Murphy v. Dulay*, 768 F.3d 1360 (11th Cir. 2014)** [Link]
A Florida statute requires a patient pursuing a medical negligence claim to execute a written authorization releasing the patient's health information to the defendant for independent analysis prior to filing the action. The statute was challenged as pre-empted by HIPAA. The court rejected the claim that the Florida statute violated HIPAA's privacy protections, relying on the Florida statute's requirement that all authorizations "shall be construed in accordance with [HIPAA requirements]." Fla. Stat. §766.1065(3). In the course of the analysis the court rejected claims that the Florida statute's pre-suit disclosure authorization violated the revocability, legitimate purpose, specificity and prohibition on compound authorization HIPAA protections.

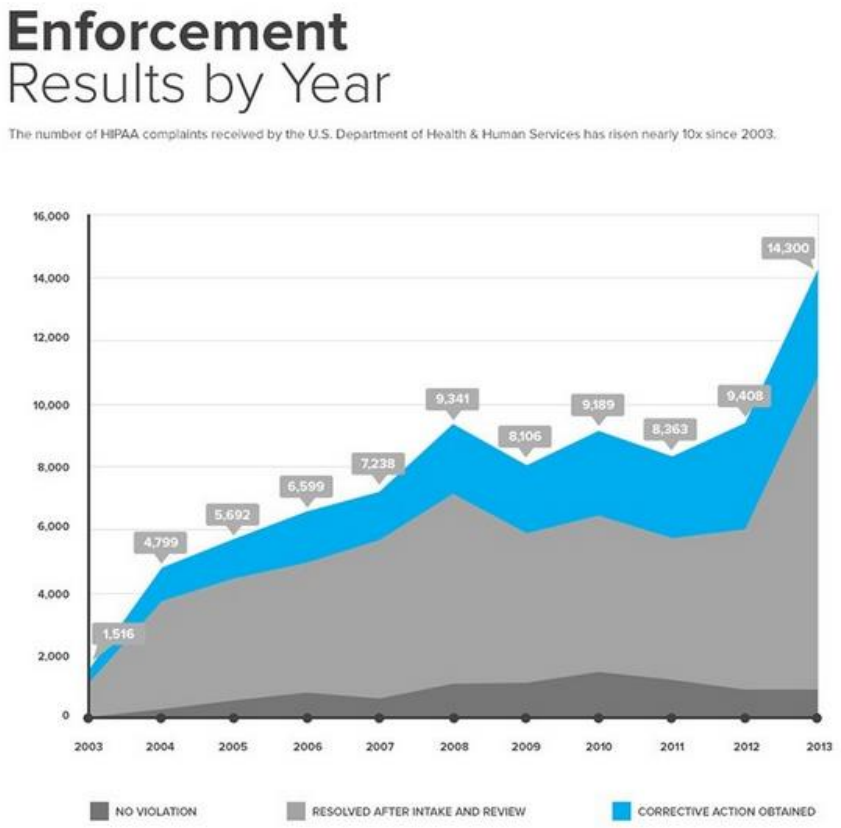
Other Resources of Note

HIPAA Privacy and Security Infographic [Link]

Interesting Facts

- Stolen protected health information (PHI) is worth 50 times more than credit card numbers or SSNs because of its usefulness for Medicare fraud. [Link]

- According to a study, 68% of healthcare breaches caused by loss or theft of devices. [Link]
- The number of HIPAA complaints has risen 10x in the past 10 years [Link]



Studies and Reports

ONC Study, *Trends in National Perceptions Regarding Privacy and Security* (2014) [Link]

- 75% very or somewhat concerned about the privacy of a medical record
- 69% very or somewhat concerned about the security of a medical record
- 8% withhold information from healthcare provider due to privacy/security concerns

Articles, Blog Posts, and Scholarship

Kirk J. Nahra, *Moving Toward a New Health Care Privacy Paradigm* (Nov. 2014) [Link]
Discussing growth of non-HIPAA-regulated heathcare data and how it is and ought to be regulated.

GOVERNMENT RECORDS

Symantec, *Internet Security Threat Report* (2014) [Link]
• Government's odds of being attacked are 1 in 3.1.
• 76% of federal employees surveyed stated their agency had a "formal, enterprise-wide information governance strategy," but only 22% said their agency's strategy is effective.

EPIC v. FBI [Link]
The D.C. District Court ruled in favor of EPIC in a case seeking to compel the FBI to comply with FOIA requests for information about its biometric database, Next Generation Identification (NGI). As the successor system to the FBI's Integrated Automated Fingerprint Identification System (IAFIS), NGI "will offer state-of-the-art biometric identification services and provide a flexible framework of core capabilities that will serve as a platform for multimodal functionality" including fingerprint, voice, iris, and facial recognition. The main issue in this case was the attorneys' fees, but the court validated a previous ruling that made a 2010 report about NGI available to the public. The report suggested a 20% failure rate in NGI's facial recognition technology. The court said that "the general public has a genuine, tangible interest in a system designed to store and manipulate significant quantities of its own biometric data, particularly given the great numbers of people from whom such data will be gathered."

New Privacy Training Requirement for Federal Contractors [Link]
DoD, GSA, and NASA issued a final rule amending the Federal Acquisition Regulation (FAR) to allow government agencies either to offer in-house privacy training or to require contractors to conduct privacy training for personnel who handle PII. The idea is to allow the government to shift training cost to contractors. The rule does not appear to address security training. Under the rule, privacy training must include these seven components at a minimum:
• Protection of privacy, in accordance with the Privacy Act;
• Handling and safeguarding of PII;
• Authorized and official use of a Government system of records;
• Restrictions on the use of personally-owned equipment to process, access, or store PII;
• Prohibition against access by unauthorized users, and unauthorized use by authorized users;
• Breach notification procedures; and
• Agency-specific privacy training requirements.

FINANCIAL DATA

Fair Credit Reporting Act (FCRA)

FCRA Complaint Filed Against LinkedIn [Link]
Class action filed against LinkedIn. LinkedIn allows users to post their employment history without any safeguards as to the accuracy. Complaint states that this violates the Fair Credit Reporting Act because "any potential employer can anonymously dig into the employment history of any LinkedIn member, and make hiring and firing decisions based upon the information they gather, without the knowledge of the member."

Gramm-Leach-Bliley Act (GLBA)

New GLBA Rule from CFPB on Notice [Link]
Under this new rule, GLBA-regulated financial institutions can post their annual privacy notices as opposed to having to mail them. If an institution changes its policy or if a person requests, a hard copy must be mailed.

CONSUMER DATA

Contract Law

***Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014)** [Link]
The Ninth Circuit refused to enforce an arbitration clause found on Barnes & Noble's website because, although the link to the clause was provided at the bottom of each web page, the link was not adequately conspicuous to put the user on notice of the clause. The court suggests that perhaps the user would be put on constructive notice if the link was placed in closer proximity to buttons/areas that the user is required to click-on.

***Knutson v. Sirius XM Radio*, 2014 U.S. App. LEXIS 21373 (9th Cir. 2014)** [Link]
The Ninth Circuit refused to enforce an arbitration clause found in a Welcome Kit provided by Sirius XM Radio because the clause was not displayed in a form that appeared to be a contract. Since the clause did not appear to be a contract, and since there was no evidence that Knutson had read the Welcome Kit that contained the clause, the court found that Knutson was not put on notice of the terms.

FTC Act Section 5

***FTC v. Acquinity Interactive, LLC*, No. 13 C 5380, 2014 LEXIS U.S. Dist. 720 (N.D. Ill. 2014)** [Link]
The FTC reached a settlement with defendants agreeing to pay a total of $9.3 million for sending unsolicited, deceptive text messages to people promising free gifts in exchange for

personal information. This information was sold to advertisers, used to place charges onto consumers' cell phone bills, and used to solicit paid subscriptions for which defendants received referral bounties. The FTC alleged violations of the FTC Act Section 5 and the Telemarketing and Consumer Fraud and Abuse Prevention Act.

***In re TRUSTe,* No. 132-3219 (Nov. 17, 2014)** [Link]
TRUSTe stated on its website that companies with TRUSTe privacy seals would be recertified each year. The FTC alleged that from 2006 through 2013, TRUSTe did not recertify in more than 1000 cases. After becoming a for-profit company in 2008, TRUSTe did not require companies using its seal to update statements in their privacy policies that TRUSTe was a non-profit entity. TRUSTe settled with the FTC, agreeing to refrain from misrepresenting its certification process and to provide model language to companies about its for-profit status. TRUSTe must pay $200,000.

Telephone Consumer Protection Act (TCPA)

***Marks v. Crunch San Diego, LLC*, No. 13-0348, 2014 WL 5422976 (S.D. Cal. Oct. 23, 2014)**
In a private civil action under the TCPA, the Southern District of California held that a device that was not currently capable of randomly generating phone numbers did not fall within the act's prohibitions.

Video Privacy Protection Act (VPPA)

***Ellis v. Cartoon Network*, No. 14-0484 (N.D. Ga., Oct. 8, 2014)** [Link]
The court dismissed a VPPA lawsuit against Cartoon Network for disclosure of its app users' viewing history and "Android ID" to a third party data analytics company. The court held that that an Android ID was not personally identifiable information (PII), despite the fact that the analytics company had reverse engineered viewers' identities from the data. Agreeing with other district courts, the court held that "personally identifiable information is that which, in its own right, without more, link[s] an actual person to actual video materials." Because at least one additional step is necessary to link the identification number to a specific person, the information is not PII.

***Sterk v. Redbox*, 2014 WL 5369416 (7th Cir. Oct. 23, 2014)** [Link]
In a VPPA class action the Seventh Circuit held that, under the circumstances, Redbox's disclosure of personally identifiable information along with video rental history to a third-party vendor did not violate the Act. The information's disclosure in the course of customer service requests and training for such requests fell within the Act's "ordinary course of business exception."

FCC Enforcement

***TerraCom Inc. & YourTel America, Inc.*, FCC No. 14-173, 2014 WL 5439575 (Oct. 24, 2014)**
[Link]
The FCC fined two wireless providers $10 million for storing customer data on publicly accessible servers. The improper storage came to light when a reporter discovered the data, which included names, addresses, social security numbers, and diverse license information

Computer Fraud and Abuse Act (CFAA)

***Aquent LLC v. Stapleton*, No. 13-1889, 2014 WL 5780293 (Nov. 5, 2014)**
In *Aquent LLC v. Stapleton*, the Middle District of Florida denied the defendant's motion to dismiss for failure to state a claim under the CFAA. The court adopted a broad view of the CFAA's protections; holding that the employee had exceeded authorized access when she accessed company data for non-business purposes, in contravention of her employment contract.

***Rajaee v. Design Tech Homes, Ltd*., No. 13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014)**
[Link]
The court rejected a plaintiff's argument that his former employer violated the Stored Communications Act (SCA) and the Computer Fraud and Abuse Act (CFAA) when remotely wiped the contents of his personal iPhone, through its connection to the company's Microsoft Exchange server. The defendant's actions allegedly caused plaintiff to lose "more than 600 business contacts collected during the course of his career, family contacts (many of which are located overseas and some are related to family business), family photos, business records, irreplaceable business and personal photos and videos and numerous passwords." The court granted summary judgment to the defendant, holding that the SCA does not protect data stored on an iPhone and that the plaintiff had not plead a loss which could sustain a CFAA claim because the CFAA does not protect the value of data itself. The court then dismissed, without prejudice plaintiff's remaining common-law claims so that they could be re-filed in state court.

Industry Self-Regulatory Principles

Global Automakers & Alliance of Automobile Manufacturers, *Privacy Principles for Vehicle Technologies and Services* (Nov. 12, 2014) [Link]
19 automakers agree to privacy principles for personal data of consumers. The principles include transparency; choice; respect for context; data minimization, de-identification and retention; data security; integrity and access; and accountability.

American Farm Bureau Federation, *Privacy and Security Principles for Farm Data* (Nov. 13, 2014) [Link]
Principles include education; ownership; collection, access, and control; transparency and consistency; choice; portability; terms and definitions; disclosure, use, and sale limitation; data retention and availability; contract termination; and liability and security safeguards.

DATA SECURITY

Standing

***Sterk v. Redbox*, 2014 WL 5369416 (7th Cir. Oct. 23, 2014)** [Link]
Rejected Redbox's argument that plaintiffs lacked Article III standing because the disclosure of their information was a "mere technical violation" of the VPPA and thus did not constitute injury in fact. The court held that violation of the plaintiff's VPPA-created rights did in fact constitute an injury in fact because it was an "invasion of a legally protected interest."

FTC Section 5

Amicus Briefs Filed in *FTC v. Wyndham Worldwide Corp.*, on Appeal to 3rd Circuit
A number of privacy groups recently filed amicus briefs before the Third Circuit in support of the FTC's Section 5 authority to regulate companies that unfairly claim to protect data in a reasonable and appropriate manner. The district court, *FTC v. Wyndham Worldwide Corp,* 2014 U.S. Dist. LEXIS 47622 (D.N.J. 2014), previously ruled in the FTC's favor in April. The appeal stems from three data breaches of over 600,000 customer payment accounts resulting in over $10.6 million in fraud loss.

Parties' Briefs
Wyndham's Opening Brief [Link], Joint Appendix Vol. 1 [Link], Joint Appendix Vol. 2 [Link]
FTC's Brief [Link]

Amicus Briefs Filed in Support of the FTC
EPIC [Link]
EFF and CDT [Link]
Public Citizen Inc., Center for Digital Democracy, and Consumer Action [Link]

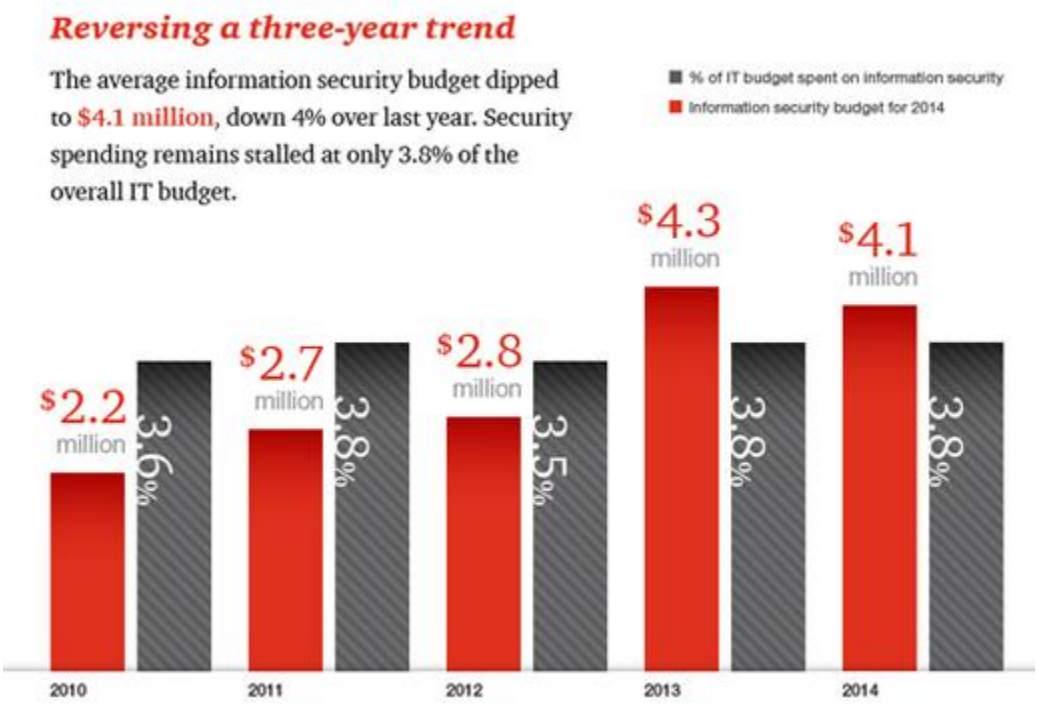
Amicus Briefs Filed in Support of Wyndham
US Chamber of Commerce, American Hotel & Lodging Association, and Federation of Independent Business [Link]
Electronic Transactions Association [Link]
Washington Legal Foundation and Allied Educational Foundation [Link]

Reports and Studies

Ponemon RSA Study, *Consumer Perceptions on Security* (2014) [Link]
• 77% of consumers lack trust in mobile app security
• 1 in 2 individuals notified of a data breach within the past 2 years

Poll, Spiceworks Voice of IT (on behalf of CloudEntr) (2014) [Link]
• 77% of IT professionals said that the workforce was the weakest link in data security
• 89% of IT officials plan to increase workforce data security education

PwC, *The Global State of Information Security Study* (2014) [Link]
Despite an increase in data breach incidents and an increase in risk and cost, security budgets shrank in the past year.



PwC, U.S. State of Cybercrime Survey (2014) [Link]
• "42% of respondents said security education and awareness for new employees played a role in deterring potential attacks. "
• Companies with workforce data security training had average annual financial losses from incidents that were $500,000 less than companies without such training.

Interesting Facts

Hackers have broken into 37% of energy companies [Link]

Data Security Statutes

Cal. Civ. Code §§ 1798.81.5, 1798.85
California recently amended several provisions of its data security laws. California expands the scope of entities that are required to implement reasonable security procedures appropriate to the nature of information collected to include not only "businesses that own or license personal information", but also any entity that "maintains" such personal information. This presumably includes "cloud" storage businesses. This does *not* apply to breach notification laws, where only those that own or license the data are bound. California also now requires businesses to provide identity theft prevention or mitigation services to all persons affected by a data security breach for at least 12 months, provided that the business (1) owned or licensed the personal information involved in the breach and (2) that the business was responsible for the breach in question. California also added a provision that permits a business to sell, advertise for sale, or offer for sale an individual's social security number if the business is required to do so by law. [Good analysis at Proskauer Privacy Law Blog]

Other News of Note

Home Depot Data Breach [Link]
Home Depot recently released a data security breach notification outlining the details of a breach that involved 56 million customer credit and debit card accounts, as well as 53 million customer email addresses. Hackers gained initial entry into Home Depot's network by using the log-in credentials of a third party vendor. Once inside, hackers exploited a weakness Microsoft Windows to access the sensitive information.

U.S. Postal Service Hacked [Link]
On November 10, 2014, the postmaster announced that the records of 800,000 U.S. Postal Service employees were breached. The breach affected the names, dates of birth, SSNs, addresses, employment dates and emergency contact information of up to 800,000 employees. The names, addresses, phone numbers, and email addresses of customers who called or emailed the USPS Customer Care Center between January 1 and August 16, 2014, may also have been compromised. Chinese government hackers are suspected.

First Cybersecurity Professional In Congress [Link]
Congress will be getting its first self-styled cybersecurity professional next term, when Congressman-Elect Will Hurd (R, TX-23) is sworn in. The one-time computer science major, former CIA undercover officer, and current adviser to a cybersecurity firm hopes to focus on the importance of cybersecurity to both national security and private industry.

PCI-DSS

PCI Council, *Best Practices for Implementing Security Awareness Program for PCI-DSS* (2014) [Link]
Guide for developing a security awareness program and training

Verizon, *2014 PCI Compliance Report* [Link]
• Only 11.1% of organizations complied with all PCI requirements

Reports and Studies

California Breach Report (2014) [Link]
Big increase from 2013 due to large breaches such as Target,

Symantec, *Internet Security Threat Report* (2014) [Link]
• 71% of phishing attacks involved fake financial institutions
• "Approximately 1 in 3 organizations in the Mining, Public Administration and Manufacturing sectors were subjected to at least one targeted spear-phishing attack in 2013."
• 16% of websites had "critical vulnerabilities that could allow attackers to access sensitive data, alter the website's content, or compromise visitors' computers."

EDUCATION PRIVACY

Industry Guidance

National Association of Secondary School Principals (NASSP), *Student Data Privacy* (2014) [Link]
The NASSP has proposed recommendations to protect student privacy at schools. Recommendations are directed to federal and state policymakers, as well as to district policymakers. Included among the recommendations are:
• "Develop clear policies about what student information is collected, how that data is used, to whom the data is disclosed, and each party's responsibilities in the event of a data breach."
• "Educate district staff about online educational services (paid and free) and how to determine whether they comply with FERPA and state and district regulations."
• "Identify a district privacy officer who is responsible for monitoring and complying with federal, state, and district policies on data privacy and for guiding school leaders and teachers in their use and protection of data."

Useful Information and Resources

Tracy Mitrano Interview of Steve McDonald on FERPA [Link]
Tracy Mitrano, Director of the Internet Culture, Policy, and Law Program (ICPL) at Cornell University interviewed Steve McDonald, General Counsel at the Rhode Island School of Design. McDonald is one of the leading experts on FERPA.

INTERNATIONAL PRIVACY LAW

Canada

***Wakeling v. United States of America*, 2014 SCC 72** [Link]
A man accused of trafficking ecstasy from Canada to the U.S. argued on appeal that the Royal Canadian Mounted Police violated his privacy when they handed over wiretap evidence to U.S. authorities. The Supreme Court of Canada upheld the lower courts' ruling that legally obtained wiretap data can be disclosed to foreign authorities without a court order in accordance with international policing procedures.

European Union

Eduardo Ustaran, *The Privacy Challenges of the New European Commission*, Chronicle of Data Protection (Hogan Lovells, Nov. 4, 2014) [Link]
Identifies challenges to the new regulatory framework for data protection. Argues that the Commission will "probably need to accept a degree of vagueness and flexibility in order to

accommodate the all too obvious level of dissent among Member States." Many agree that a "one-stop shop" (one national data protection authority) is not achievable, but the Commission should try to adopt some of its principles in building the new regulations.

Asia

Hogan Lovells, *Data Privacy Regulation Comes of Age in Asia* (2014) [Link]
Overview of recent state of privacy regulation in Asia, with useful maps.

ABOUT THE AUTHORS

Daniel J. Solove *is the John Marshall Harlan Research Professor of Law at George Washington University Law School, the founder of* ***TeachPrivacy****, a privacy/data security training company, and a Senior Policy Advisor at Hogan Lovells. Along with Paul Schwartz, Solove is a Reporter on the American Law Institute's Restatement Third, Information Privacy Principles. He is the author of 9 books including Understanding Privacy and more than 50 articles. Follow Professor Solove on Twitter @DanielSolove.*

Paul Schwartz *is the Jefferson E. Peyser Professor of Law at UC Berkeley School of Law and a Director of the Berkeley Center for Law and Technology. Schwartz is also a Special Advisor at Paul Hastings, where he works in the Privacy and Data Security Practice. He is the author of numerous books and articles on information privacy and information law. With Daniel Solove, he is the co-author of* *Privacy Law Fundamentals* (a short reference book) and *Information Privacy Law* (a casebook).

The views here are the personal views of Professors Solove and Schwartz and not those of any organization with which they are affiliated.

The authors would like to thank Bryan Lee, Grant Nelson, Amy Roller, Sonia Shaikh, and Adam Shaw for their assistance with this post.

Please join one or more of Professor Solove's LinkedIn groups:

Privacy and Data Security

HIPAA Privacy & Security

Education Privacy and Data Security

Image Credits: Fotolia + DJS Mashup