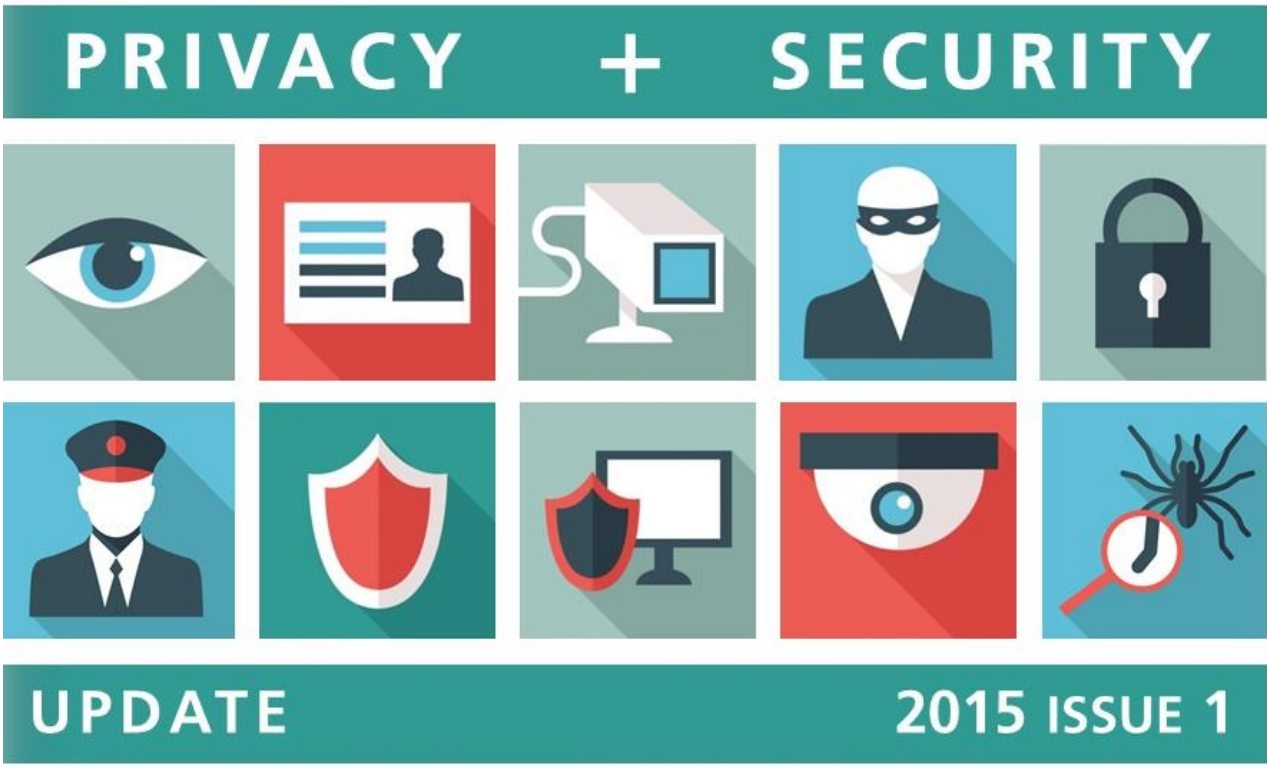


PRIVACY + SECURITY UPDATE

Drones, Data Breaches, Cramming, and Other Privacy + Security Updates

By Daniel J. Solove + Paul M. Schwartz

2015 Issue 1

This post is part of a post series where we round up some of the interesting news and resources we're finding. For a PDF version of this post, and for archived issues of previous posts, click here.

GENERAL DEVELOPMENTS

Privacy Legislation

President Obama Announces New Actions to Protect Privacy (Jan. 12, 2015) [Link]
-- President Obama announced Monday, January 12, 2015, in advance of his State of the Union address, that federal legislation should be passed to safeguard Americans' online privacy to establish a uniform national standard.
-- The Consumer Privacy Bill of Rights -- protect consumers' personal information from theft and place individuals in charge of their data.
-- The Student Digital Privacy Act -- similar to a recent California law that prevents companies from selling student information to third parties for non-educational reasons, such as advertising purposes. The legislation would not apply to higher education.

News

Hadley Robinson, Profile of Judge Lucy H. Koh, Daily Journal (Dec. 4, 2014) [Link]
-- "Experts at the American Law Institute say though there is no official tally, Koh is likely handling more privacy cases than any other federal judge in the country."
-- Key cases include *Adobe Systems Inc. Privacy Litigation* CV13-5226 (N.D. Cal., filed Nov. 11, 2013) (finding injury for data breach); *Google Inc. Gmail Litigation*, MD13-2430 (N.D. Cal., filed April 1, 2013) (denying Google's motion to dismiss for lawsuit alleging Gmail violates the Wiretap Act).
-- Daniel Solove's quote in the article: "Far too often, judges just seem in a hurry to get rid of the cases - they seem too difficult and different - and so many judges dispatch the cases too quickly, without adequately analyzing them. What impresses me about Judge Koh is that she doesn't do that. She engages with the issues and isn't dismissive."

Conferences

Privacy + Security Forum (October 21-23, 2015) – Washington, DC [Link]
-- Goals are to unite privacy and security professionals, as well as practitioners, academics, technologists, and regulators. Educational sessions with rigor and practical takeaways.
-- 50+ speakers
-- PDF Guide to Planned Sessions and Speakers [Link]

IAPP Global Privacy Summit (March 4-6, 2015) – Washington, DC [Link]
-- IAPP's largest event in Washington, DC
-- Numerous sessions and prominent keynote speakers, including Glenn Greenwald.

Books

David Sheidlower, A CISO's Guide to Principles of Data Privacy and Security (2014) [Link]
Free e-book providing a clear, concise, and thoughtful introduction to privacy and security

PRIVACY AND THE MEDIA

Revenge Porn

First Case of a Person Jailed For Posting Facebook "Revenge Porn" [Link]
A California man was sentenced to one year in prison in first successful prosecution under California's "revenge porn" law. The law criminalizes "the unauthorized sharing of nude or sexual images of an individual with the intention of inflicting emotional harm." The defendant in this case posted topless photos of his ex-girlfriend to her employer's Facebook page.

***Wilson v Ferguson,* [2015] WASC 15** [Link]
The Western Australia Supreme Court held that the plaintiff's ex-boyfriend breached her confidence when he posted photos and videos of her naked and engaging in sexual activities on his Facebook page. The court issued a permanent injunction against his posting similar photos and videos of the plaintiff. Damages of $48,404 – $13,404 for loss of income and $35,000 for "embarrassment and distress occasioned by the disclosure of private information."

Books

Amy Gajda, *The First Amendment Bubble: How Privacy and Paparazzi Threaten a Free Press* (2014) [Link]
Discusses how to balance privacy and freedom of the press, including how to define who counts as a "journalist" in the days of blogs and social media.

Articles, Blog Posts, and Scholarship

Danielle Citron, *United States v. Elonis and the Rarity of Threat Prosecutions*, Forbes (Dec. 3, 2014) [Link]
- About 850,000 people are stalked each year – estimate from a 2006 Bureau of Justice Statistics study.
- "[T]hreats and cyber stalking crimes are a low priority for federal law enforcement."
- Average of only 25 federal criminal cases for online harassment each year – "a paltry number given the estimated number of cyber stalking cases a year."

PRIVACY AND LAW ENFORCEMENT

70 Companies and Public Interest Organizations Send Letter to Congress Urging It to Update ECPA (Jan. 23 2015) [Link]
-- 70 civil liberties organizations, public interest groups, and companies sent letters to the House of Representatives and Senate advocating for "speedy consideration" of the bipartisan Email Privacy Act, which Representatives Kevin Yoger and Jared Polis co-sponsored, and the Electronic Communications Privacy Amendments Act, which Senators Mike Lee and Patrick Leahy co-sponsored. These bills would revise the Electronic Communications Privacy Act (ECPA) to provide greater protections for email and data in the cloud.
-- Signatories were Microsoft, Google, Apple, Dropbox, Facebook, Twitter, Yahoo, Amazon, AOL, and Adobe.

NATIONAL SECURITY AND FOREIGN INTELLIGENCE

NSA Releases Limited Info on Privacy Violations (Dec. 24, 2014) [Link]
On Christmas Eve, ~~Santa Claus~~ the NSA released heavily redacted reports showing 12 instances of "intentional misuse" of government surveillance since Jan. 1, 2003. The information release came in response to a FOIA lawsuit filed by the ACLU.

HEALTH PRIVACY

HIPAA: HHS Enforcement

Resolution Agreement, Anchorage Community Mental Health Services (ACMHS) [Link]
HHS OCR $150,000 penalty for data breach resulting from failure to update software with latest patches.

HIPAA: HHS Reports and Guidance

ONC Data Brief, *Individuals' Access and Use of their Online Medical Record Nationwide* (Sept. 2014) [Link]
- Addressing shortcomings in access to online health records. "[O]nly about 3 in 10 individuals were given access to an online medical record."
- "A majority of individuals who accessed their online medical record at least once within the last year considered their online medical record very useful."

Device Loss and Theft Still Pose Greatest Threats to Health Data Security [Link]
According to HHS, more than 50% of the data breaches reported under HIPAA are the result of lost or stolen laptops.

HHS OCR Releases Guidance on Treating Ebola and HIPAA (Nov. 2014) [Link]
- HIPAA still applies if the patient has Ebola; the diagnosis does not change the protection afforded the PHI.
- No special treatment for Ebola patient's PHI, may only release under usual circumstances.

HIPAA: State Common Law

Walgreen Co. v. Abigail Hinchy, No. 49A02-1311-CT-950 (Indiana Ct. App. Nov. 14, 2004) [Link]
-- Reviewing a $1.44 million jury verdict, an Indiana appellate court affirmed that the plaintiff had raised a viable claim of negligence based on using HIPAA as the standard of care.
-- Facts: Upon learning that the plaintiff was pregnant by the pharmacist's boyfriend, the defendant-pharmacist used her access to patient records at Walgreen to examine the plaintiff's prescription history. There, she discovered that the plaintiff had not filled her birth control prescription for two months and sent her abusive text messages to that effect. She also informed her boyfriend of what she learned from the medical records. Walgreen later confirmed that the pharmacist had used its system to access the records, and advised the plaintiff that it would issue a written warning to the pharmacist and requiring her to re-take a HIPPA computer compliance training course. Dissatisfied, the plaintiff sued and prevailed at trial.
-- This case follows on the heels of *Byrne v. Avery Center for Obstetrics and Gynecology*, No. 18904, 2014 WL 5507439 (Conn. Nov. 11, 2014), also affirming the use of HIPAA as the standard of care in a negligence case. [Link]
-- For more analysis of the issue of using the common law to sue for HIPAA violations, see Daniel J. Solove, *Lawsuits for HIPAA Violations and Beyond: A Journey Down the Rabbit Hole* (Nov. 18, 2014) [Link]

Constitutional Law

Stuart v. Camintz, — F.3d —, 2014 WL 7237744, (4th Cir. Dec. 22, 2014) [Link]
On First Amendment grounds, a federal appeals court struck down North Carolina's Woman's Right to Know Act, which compelled doctors to display a sonogram and describe the image of the fetus to a patient before performing an abortion. The court found that the statute amounted to compelled speech and the restriction was ideologically motivated.

State Enforcement

Massachusetts – Beth Israel Deaconness Medical Center Settlement (2014) [Link]
2012 data breach involving doctor's unencrypted personal laptop stolen from an unlocked office. 4000 people's data exposed. $100,000 settlement for inadequate security and failure to provide timely breach notification.

Commonwealth v. Children's Hosp. Corp., No. 14-3955 (Mass. Super. Ct. Dec. 19, 2014) [Link] Boston Children's Hospital entered into an agreement with Massachusetts to settle claims under the Massachusetts Consumer Protection Act and HIPPA. The claims stemmed from the 2012 theft of a doctor's unencrypted hospital-issued laptop that contained the personal health information of 2,100 patients including 1,700 minors. The settlement included a $10,000 contribution to a state-run data-protection education fund and $30,000 in civil penalties.

Wind + PHI = $400,000 Settlement (2014) [Link]
PHI of 1500 patients put in dumpster. Then the wind blows it away throughout a neighborhood. $400,000 settlement with the patients. And all this before possible HIPAA fines.

GOVERNMENT RECORDS

Freedom of Information Act (FOIA)

FOIA Lawsuits Spike in 2014 [Link]
The non-profit/educational organization *The FOIA Project* reported on Dec. 22 that FOIA lawsuits rose in 2014 to a higher count than any year since 2001. 422 lawsuits were filed, driven largely by "new media" outlets, such as Mother Jones, VICE News, and ProPublica, as well as more traditional watchdog groups like the ACLU, EFF, and EPIC.

Books

John Kropf & Neal Cohen, Guide to U.S. Government Practice on Global Information Sharing (2nd ed 2014) [Link]
Useful reference book about the U.S. government's practices regarding sharing personal data with other governments

CONSUMER DATA

Lawsuits

***Perkins v. LinkedIn*, 13-CV-04303-LHK (N.D. Cal. Nov. 13, 2014)** [Link]
-- Plaintiffs alleged that LinkedIn sent out repeated invites to user contacts. Though Plaintiffs may have consented to the initial invitation, they did not consent to the second and third emails. Although the Stored Communications Act and the Wiretap Act claims were dismissed, the court denied LinkedIn's request to dismiss on grounds of standing. The Plaintiff's second amended claim includes violations of publicity rights and California's unfair competition statute.
-- The court rejected defendant's arguments that the plaintiff had not alleged a theory of commercial harm sufficient to establish an injury for the claims of common law right of publicity, UCL, and Section 502. Undertaking a lengthy analysis the court ultimately concluded that:"[I]ndividuals' names have economic value where those names are used to endorse or advertise a product to the individuals' friends and contacts. This is so because an advertisement bearing the imprimatur of a trusted or familiar source, such as a friend or acquaintance, has concrete value in the marketplace. Here, Plaintiffs allege that their names were misappropriated by LinkedIn to create personalized endorsements." The court's findings were partially guided by the company's internal documents extolling the value of the referral emails.
-- Additionally, the court concluded that plaintiffs could be harmed because the emails might provide the impression that plaintiffs were the type of people "who spam their contacts or are unable to take the hint that their contacts do not want to join their LinkedIn network."
-- A Feb. 15, 2015 news story indicates that the parties are close to reaching a settlement.

Electronic Communications Privacy Act (ECPA)

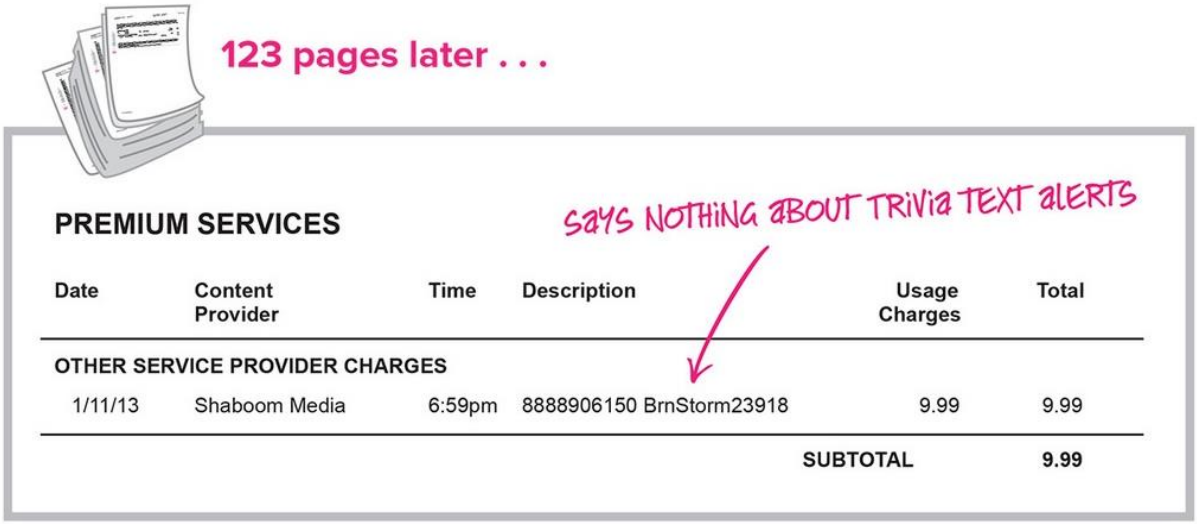
***Campbell v. Facebook Inc.*, No. 13-5996, 2014 WL 7336475 (N.D. Cal., Dec. 23, 2014)** [Link]
Denying Facebook's motion to dismiss a Wiretap Act claim, the court held that Facebook's practice of scanning users' messages for URL's, which it then added to mentioned business's "like" counts, may have constituted an interception which would not qualify as having been done in the ordinary course of business. The court further held that the provision of Facebook's privacy policy that provided the company "may use the information we received about you" for "data analysis" was insufficiently specific to establish express consent.

***Backhaut v. Apple, Inc.,* 2014 WL 6601776, No. 14-2285, (N.D. Cal. Nov. 19, 2014)**
Messages sent to former iPhone users via iMessage were not delivered to their new cellphones; instead, they remained on an Apple server unbeknownst to both sender and intended recipient.

The court held that the plaintiffs had alleged Apple's conduct violated the Wiretap Act by intercepting and preventing delivery of the messages and that this conduct was intentional because Apple did not try to remedy the problem despite knowing of it. The court rejected Apple's argument that its conduct qualified for the Wiretap Act's ordinary course of business exception. Next, the court dismissed plaintiff's SCA claims; agreeing with Apple that the company had not accessed messages in electronic storage and that iPhones are not facilities under the SCA. The court also dismissed several state law claims, leaving only the Wiretap Act claim and a claim under California's Unfair Competition Law.

FTC Act Section 5

FTC v. T-Mobile **(Dec. 19, 2014)** [Link]
The FTC settled with TMobile on allegations regarding mobile cramming. According to the FTC, T-Mobile placed unwanted third-party charges on customer's phone bills for services such as horoscopes and celebrity gossip. The information about these charges was buried in bills that exceeded more than 50 pages in many instances. The carrier will have to pay $18 million in fines and penalties to all 50 states and the D.C. attorney generals. Additionally, it will pay $4.5 million to the FCC. The rest of the amount will be used to pay customers who were affected by third party unauthorized charges. Below is a sample part of a bill the FTC posted in its press release:



FTC v. LeapLab **(Dec. 23, 2014)** [Link]
The FTC recently filed a complaint alleging that a group of data brokers who sold personal financial information collected under the guise of online payday loan applications to third parties that had no legitimate use for the information. These third parties allegedly used the information to fraudulently withdraw millions of dollars from the loan applicants' bank account. The information included highly sensitive personal information such as social security number, bank account number, and routing number. The FTC alleges that only five percent of the

information sold went to legitimate payday loan services, while the remaining information was sold to these allegedly fraudulent companies. The lead defendant, LeapLab, hired the Chief Marketing Officer of a company that was previously under FTC investigation for similar practices (Ideal Financial Solutions, Inc.).

***FTC v. SnapChat* (Dec. 31, 2014)** [Link]
The FTC recently approved a final order settling charges with Snapchat, a mobile application that allowed users to send pictures and videos to other users, which would be automatically deleted after a set number of seconds. Snapchat fell prey to hackers in two highly publicized incidents in 2014, with the January breach involving usernames and passwords being the focus of the FTC investigation. The FTC alleged that Snapchat deceived its users by collecting more private information than Snapchat purported to, while providing less security to data than promised as well. The settlement requires Snapchat to increase its privacy and security measures, to provide users with accurate descriptions of these measures, and to be monitored by an independent privacy professional for the next 20 years.

Telephone Consumer Protection Act (TCPA)

***Palm Beach Golf Center-Boca, Inc. v. John G. Sarris*, D.D.S., P.A., No. 13–14013, 2014 WL 5471916 (11th Cir. Oct. 30, 2014)**
A federal appeals court overturned a lower court's ruling that plaintiffs lacked standing under the TCPA because no one had actually seen the junk faxes sent in contravention of the statute. The court of appeals held that the transmission of the faxes themselves constituted a concrete injury, because the plaintiff's fax machine was rendered otherwise unavailable for legitimate business for the duration of the transmission. Further, the TCPA statutory scheme allows private individuals to pursue civil action against violators.

Communications Privacy

FCC Imposes $35k Penalty For Local Station's Broadcast of Private Phone Conversation [link]
The FCC announced that it has entered into a consent decree with a Salt Lake City television station, resolving its investigation into an incident in which the station called a consumer on the telephone and, without prior warning, recorded the call and broadcast the conversation as a part of a news segment. As part of the decree the station agreed to pay a $35,000 penalty and admitted to hampering the agency's investigation and violating 47 C.F.R. § 73.1206. *See* Order, *Newport Television, LLC*, DA 14-1676, 2014 WL 6722317 (FCC Nov. 28, 2014).

Children's Online Privacy Protection Act (COPPA)

Covington & Burling, *Carnegie Mellon Grades Privacy of Android Apps* (2014) [Link]
Carnegie & Mellon developed a website, privacygrade.org, which grades Android applications based upon their privacy policies. Grades are established from a model that evaluates one's expectations regarding an application's performance and how the application really acts. An A+

indicates no privacy risk, whereas a D, the highest grade, reflects many concerns. Of the 1 million applications reviewed, researchers gave about 1,000 of them—most of which were children's games—a D rating.

FTC Warns Chinese Toymaker About Geolocation Tracking [Link]
The FTC has warned China-based toymaker BabyBus that its "statistical plug-ins" may be in violation of COPPA. The downloadable applications collect precise geolocation data and are child-directed, i.e., parental consent is not required for operation. The company said that it will comply with the COPPA rules although the plug-ins are not against local laws in China.

Computer Fraud and Abuse Act (CFAA)

***DeSoto v. Bd. of Parks & Recreation*, No. 14-0822, 2014 WL 6680681 (M.D. Tenn. Nov. 25, 2014)**
A technician for plaintiff's former employer attempted to unlock the device, resulting in 10 incorrect password attempts and triggering a security feature that wiped the device. The 10th access attempt was in violation of an administrative order and agreement between the parties in unrelated litigation. The court held that the employer's access of the Blackberry could not be unauthorized access under the CFAA because it owned the device.

***Total Safety v. Rowland*, No. 13-6109, 2014 WL 6485641 (E.D. La. Nov. 18, 2014)**
The court, in declining to grant summary judgment, adhered to the Fifth Circuit's broad interpretation of the CFAA. Noting that "in the civil context, under the terms of a broad confidentiality agreement, a former employees' actions may exceed authorized access."

***Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, — F.3d —, 2014 WL 7247400 (6th Cir. Dec. 22, 2014)**
The Sixth Circuit held that "damage" for purposes of the CFAA could be established by showing a defendant submitted fraudulent bids. Defendant's conduct occupied bidding slots, rendering them inaccessible to legitimate bidders.

***St. Jude Medical S.C., Inc. v. Janssen-Counotte*, No. 14-0877, 2014 WL 7237411 (W.D. Tex. Dec. 17, 2014)**
The court held that in order to state a claim under the CFAA, a plaintiff needn't own the computer which was accessed without authorization. The defendant used a thumb drive on a laptop owned by her then-employer, who was not a party to this case.

Drones

***Huerta v. Pirker* -- NTSB Rules That Model Planes are "Aircraft" Under FAA Rules** [Link]
In *Huerta v. Pirker*, the NTSB held that a model airplane constituted an "aircraft" under 14 C.F.R. § 91.13(a), which defines "aircraft" as "a device that is used or intended to be used for flight in the air."

Drone Crashes on White House Grounds (Jan. 25, 2015) [Link]
-An off-duty employee of the National Geospatial-Intelligence Agency lost control of a drone he was flying from an apartment near the White House. The employee, who had been drinking alcohol, went to bed without locating the drone. The drone was located on White House property the next morning.

Articles, Blog Posts, and Scholarship

IAPP, *FTC Casebook* (2015) [Link]
"The FTC Casebook collects and provides access to more than 180 privacy and data security enforcement actions—full-text searchable, tagged, indexed and annotated."

DATA SECURITY

FTC Section 5

LabMD v. FTC, No. 14-12144 (11th Cir. Jan. 20, 2015)[Link]
"Because we hold that the FTC's Order denying LabMD's motion to dismiss was not a "final agency action," as is required of claims made under the APA, those claims were properly dismissed. And because we conclude that LabMD's other claims —that the FTC's actions were ultra vires and unconstitutional — are intertwined with its APA claim for relief and may only be heard at the end of the administrative proceeding, we affirm the District Court's order dismissing the case for lack of subject-matter jurisdiction."

Other LabMD Case Developments (2015)
-- LabMD has filed a separate suit against Robert Boback, CEO of Tiversa. Boback testified in front of the House Oversight Committee that he misled the FTC, falsely representing that LabMD patient information was found outside of its network, helping the FTC make its complaint against LabMD. LabMD alleges that Boback turned over stolen patient data to the

FTC. LabMD's suit seeks millions of dollars for fraud, defamation, and a slew of other related charges. [Link]
-- In 2014, testifying witness Richard Wallace refused to testify without a grant of immunity. Wallace was expected to testify to providing an FTC attorney with false information that would contradict the complaint filed against LabMD. On January 5, 2015, the Court lifted the stay after granting Wallace immunity. The evidentiary hearing will resume March 3, 2015. [Link]
-- From Daniel J. Solove & Woodrow Hartzog, *Should the FTC Be Regulating Privacy and Data Security?* (Nov. 14, 2014): "In the LabMD case, LabMD is contending that the U.S. Department of Health and Human Services (HHS) -- not the FTC -- has the authority to regulate data security practices affecting patient data regulated by HIPAA. With Wyndham, and especially LabMD, the drama surrounding the FTC's activities in data protection has gone from 2 to 11. The LabMD case has involved the probable shuttering of business, a controversial commissioner recusal, a defamation lawsuit, a House Oversight committee investigation into the FTC's actions, and an entire book written by the LabMD's CEO chronicling his view of the conflict. And the case hasn't even been tried yet!" [Link]
-- FTC Complaint against LabMD [Link]

F. Paul Pittman, *FTC Shows Willingness to Credit Responsive Data Security Efforts in Exercising Enforcement Authority*, JD Supra Business Advisor, Dec. 1, 2014 [Link]
The FTC recently decided not to pursue enforcement action against Verizon because Verizon had taken affirmative steps to address its data security issues. Verizon allegedly engaged in unfair or deceptive practices by failing to adequately secure consumer equipment. The author suggests that this might be a signal to companies of the FTC's willingness to work with them in implementing secure adequate security measures, as opposed to just seeking to punish them.

News, Reports and Studies

Ponemon Institute, *Corporate Data: Protected Access or a Ticking Time Bomb* (Dec. 2014) [Link]
- Of end users, "71% say they have access to company data that they should not be able to see."
- Of end users, "47% say the organisation doesn't enforce its policies relating to the misuse of or unauthorised access to company data."
- Of IT professionals, "80% say their organisation doesn't enforce a strict least-privilege data model."

NY Times Special Section on Security (Dec. 2, 2014) [Link]
-- From *Hacked vs. Hackers*: "A bleak recap: In the last two years, breaches have hit the White House, the State Department, the top federal intelligence agency, the largest American bank, the top hospital operator, energy companies, retailers and even the Postal Service. In nearly every case, by the time the victims noticed that hackers were inside their systems, their most sensitive government secrets, trade secrets and customer data had already left the building." [Link]
-- From *Hacked vs. Hackers*: "If the tech sector cannot persuade foreign customers that their data is safe from the National Security Agency, the tech industry analysis firm Forrester Research predicts that America's cloud computing industry stands to lose $180 billion — a quarter of its current revenue — over the next two years to competitors abroad." [Link]
-- *Betting on Security Start Ups:* Lots of money flowing into data security companies; big growth in the industry [Link]
-- *Betting on Security Start Ups: "*A decade ago, most large information technology customers would spend 2 to 6 percent of their budget on security, estimates Asheem Chandna, a partner at Greylock Partners, a venture capital firm. These days, it is more like 5 to 15 percent, creating an estimated $80 billion-a-year market for security products and services." [Link]

2014 IBM Chief Information Security Officer Assessment (2014) [Link]
-- 80% of CISOs said that the number of data security threats is rising.
-- "Close to 60 percent of security leaders interviewed said that the sophistication of attackers was outstripping the sophistication of their organization's defenses."

Data Breach Facts

Nearly a Billion Records Were Compromised in 2014 [link]
"In first nine months of 2014, after 1,922 confirmed incidents, criminals managed to compromise 904 million records. Many of the incidents reported in 2014 were record setting, including twenty of them that resulted in the compromise of more than a million records each."

3M, Visual Data Breach Risk Assessment Study (2014) [Link]
-- 67% of employees expose data beyond the workplace

Data Breaches

Home Depot Breach – the Gory Details [Link]
-- Home Depot spent $43 million dealing with its data breach in one quarter
-- Money spent on "spent on investigations, providing identity theft protection services to consumers, increased call center staffing and other legal and professional services." 56 million payment card details and 53 million email addresses stolen. 44 lawsuits filed. Hackers gained access via the login of one of Home Depot's vendors.

Sony Data Breach [Link]
Hackers have gained access to data on Sony employees, including sensitive information such as Social Security numbers, medical information, and even salaries. Emails were also compromised, including emails sent by C-Suite officials. The information was leaked online. The company's computer systems were severely affected.

Fortune 500 Cyber Attack Timeline (2011 to 2014) [Link]
-- big increase in number in 2014

Data Breach Litigation

***In re Target Corp. Customer Data Sec. Breach Litigation*, No. 14-02522 (D. Min.. Dec. 2, 2014)**
A judge ruled that corporate plaintiffs, namely banks, in the ongoing litigation over Target's famed data breach can continue to pursue their claims. Rejecting Target's motion to dismiss the court pointed out that "Although third-party hackers' activity caused harm, Target played a key role in allowing the harm to occur." The retailer's role included disarming some of its security features and ignoring system warnings while the attack was underway. The judge has yet to rule in the companion class action brought by consumers affected by the Target data breach.

***In re Target Corp. Customer Data Sec. Breach Litigation*, No. 14-2522, 2014 WL 7192478 (D. Minn. Dec. 18, 2014)**
-- Ruling on Target's motion to dismiss for want of standing and failure to state claim under various state laws, Judge Paul Magnuson held that consumer plaintiffs had adequately plead injury but delivered mixed judgments on their state-law claims. The case, consolidated before Judge Magnuson by the Judicial Panel on Multidistrict Litigation, has 114 named plaintiffs and the affected group of consumers is estimated to be around 110 million.
-- Rejected Target's contentions that plaintiffs did not allege injuries that are actual or imminent, the court found alleged injuries in "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."
-- Rejected Target's arguments that, to establish an injury, plaintiffs are required to allege fraudulent credit card charges were unreimbursed.
-- Plaintiffs plausibly alleged "a threat of ongoing or future harm."
-- Allowed most state consumer protection law claims to proceed and a number of claims based on state breach notification laws

***In re Adobe Systems, Inc. Privacy Litigation* , No. 13-cv-05226-LHK (N.D. Cal. 2014)** [Link]
-- Allowed class certification based on plaintiffs' shared risk of future harm. The court ruled that the theft of personal information including email passwords and credit card information satisfied the test in *Clapper v. Amnesty International* (2013) where the Supreme Court required that injury be "immediately impending" to gain class action certification

-- "Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. Plaintiffs' personal information was among the information taken during the breach. Thus, in contrast to *Clapper,* where there was no evidence that any of respondents' communications either had been or would be monitored under Section 702, here there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken."

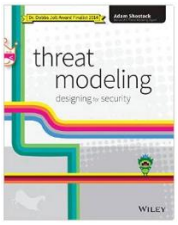
Data Security Statutes

4 New Federal Cybersecurity Laws (2014) [Winston & Strawn Post: Link]
-- At the end of 2014, four new federal cybersecurity laws were signed into law
-- The Cybersecurity Enhancement Act of 2014 (S.1353) provides guidelines and practices to follow when developing complex and secure software systems.
-- The National Cybersecurity Protection Act of 2014 (S.2519) requires the DHS National Cybersecurity Communications Integration Center to share information regarding cybersecurity risks with the rest of the federal government and to provide risk management support to federal and non-federal bodies with respect to cybersecurity risks.
-- The Cybersecurity Workforce Assessment Act (H.R. 2952) gives the Secretary of DHS the responsibility of monitoring the Department's readiness and ability to accomplish its cybersecurity goals and one year thereafter establish a workforce strategy to increase DHS' readiness, training, and recruitment of its cybersecurity workforce.
-- Amendment to the Federal Information Security Management Act of 2002 (S. 2521) mandates evaluation of federal information security standards as well as agency compliance with protections against security threats.

Massachusetts Data Security Law Enforcement

Massachusetts Office of the Attorney General, *TD Bank to Pay $625,000 to Address Data Breach Involving Thousands of Massachusetts Residents*, (Dec. 8, 2014) [Link]
Two unencrypted computer server backup tapes that contained the personal information 90,000 Massachusetts residents (260,000 consumers nationwide) went missing in March 2012. TD Bank did not notify customers and the Attorney General until October 2012. TD Bank also failed to adhere to state data security laws that require reasonable measures to ensure data security such as encryption and risk assessment concerning the tapes. TD bank was also faulted in not taking adequate measures in hiring a third-party to transport the tapes. TD Bank was ordered to pay $625,000 and to implement encryption of personal information and reasonable risk assessment and monitoring measures.

Books



Adam Shostack, Threat Modeling: Designing for Security (2014) [Link]
Practical and comprehensive guide to anticipating and addressing threats when designing software and technology

EDUCATION PRIVACY

Higher Education Privacy Conference (HEPC) (May 11-12, 2015) – Washington, DC [Link]
-- The HEPC will be held on Monday, May 11, 2015 in Washington, DC. The HEPC focuses on privacy and information management in higher education. The event will begin with a panel entitled: *Education Privacy: A New Regulatory Paradigm?* Panelists include Kathleen Styles, CPO Dep't of Education, Jules Polonetsky (FPF), Dipayan Ghosh (White House), and Steven McDonald (RISD).
-- The rest of the day consists of breakout discussion groups on topics such as cloud providers and incident prevention and response.
-- An additional day-long workshop – *Building a Privacy Program for Higher Education* – will be held on Tuesday, May 12, 2015. This workshop is separate from the conference.

EMPLOYMENT PRIVACY

Americans with Disabilities Act (ADA)

***EEOC v. Honeywell*, No. 14–4517, 2014 WL 5795481 (D.M.N. Nov. 6, 2014)**
In denying the EEOC's request for a preliminary injunction to prohibit Honeywell from implementing an employee wellness program that entailed biometric testing for beneficiaries, the court observed that "great uncertainty persists" in regard to how protections for employee medical privacy under the ADA, 42 U.S.C. § 12112(D)(4)(A), and GINA, 42 U.S.C. § 2000ff-5, interact with the ACA's authorization of employer wellness programs. The EEOC charges that Honeywell's biometric testing "constitutes an involuntary medical exam that is not job related," and that their collection of spouses' medical information violates GINA. Honeywell counters that its program is permissible either under the ADA's safe harbor provisions or because it is in line with congressional intent of the ACA, and that the biometric exam does not constitute a "genetic test."

Butler v. La. Dep't of Pub. Safety & Corr., No. 12-0420, 2014 WL 6959940 (M.D. La. Dec. 4, 2014)
In the course of denying a plaintiff's motion for partial summary judgment on ADA claims, the court held that if he could establish that a psychiatric evaluation ordered by his superior was arranged with doctor who was, at that time, already an expert specially retained for litigation it would establish that the evaluation was not job-related and consistent with business necessity. Thus, it would establish a key element of a claim under 42 U.S.C. § 12112(d), which prohibits employers from subjecting employees to invasive and unnecessary medical examinations.

NLRB Enforcement of the National Labor Relations Act (NLRA)

***Purple Commc'ns, Inc. & Commc'ns Workers of Am., AFL-CIO*, 361 NLRB No. 126 (Dec. 11, 2014)**
In a 3-2 ruling the NLRB held that employees that are already authorized to use an employer's email system have a presumptive right to use the system for NLRA protected activities during non-work hours.

Tennessee Employee Online Privacy Act of 2014
-- Effective Jan. 1, 2015
-- Prohibits employers from requiring disclosure of passwords to employee or applicant personal Internet accounts
-- Prohibits employer from forcing employee or applicant to add employer to contact list or access account in employer's presence so employer can review it
-- Exception for investigations of work-related misconduct
-- Exception if employer is providing the account, such as employer's own Facebook, Twitter, or LinkedIn page

Fourth Amendment

***Gustafson v. Thomas*, No. 11-5852, 2014 WL 7177593 (N.D. Ill. Dec. 16, 2014)** [Link]
In a case concerning whether a government-employer's installation of covert video cameras in a room commonly used by female employees to change violated the Fourth Amendment, a court denied defendant's motion for summary judgment on the issue of qualified immunity. The rights were clearly established at the time of the violation.

INTERNATIONAL PRIVACY LAW

Canada

R. v. Fearon, 2014 SCC 77 (Dec. 11, 2014) [Link]
The Supreme Court of Canada held that police may search cellphones without a warrant incident to an arrest. The decision stands in contrast to the decision by the U.S. Supreme Court in *Riley v. California*, 134 S. Ct. 2473 (2014), which the Canadian Court expressly rejected, holding that U.S. police must first obtain a warrant before searching a cell phone during an arrest.

Office of the Privacy Commissioner of Canada, *Joint Open Letter to App Marketplaces*, Dec. 9, 2014 [Link]
In an open letter addressed to the top seven mobile application marketplaces, the Privacy Commissioner of Canada, along with 23 other privacy related organizations from 19 different countries (noticeably *not* including the US), requested that privacy practice information such as privacy policies should be a mandatory requirement for an application to be allowed into the respective marketplaces. These privacy practices should be provided in a manner that allows the user to make an informed and meaningful choice whether to download the application or not. The letter suggests that app marketplace should participate in the informed choice of users, instead of standing back and forcing the responsibilities on app developers and users.

European Union

Scott Goss, *Data Protection Law Errors in Google Spain LS, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*, Future of Privacy Forum (2014) [Link]
-- "The mark of a controller is one who 'determines the purposes and means of the processing of personal data.' (Art. 2, Dir. 95/46 EC). In creation of the index, rather than 'determining', search engines are identifying the activities of others (website publishers) and heeding their instructions (use or non-use of robots.txt). I believe such processing cannot, as a matter of law, rise to the level of 'controller' activities."
-- "The question is not whether the search results are 'incomplete or inaccurate' representations of Mr. Costeja Gonzalez, but whether the search results are inaccurate as to the purpose of the processing. The purpose of the processing is to copy, sort, and organize the information on the internet. In this case, queries for the characters 'Mario Costeja Gonzalez,' displayed articles that he admits were actually published on the Internet. Such results, therefore, are by definition not incomplete or inaccurate as to the purpose of the data processing activity. To put it simply, the Court applied the relevancy test to the wrong party (Mr. Costeja Gonzalez) as opposed to Google and the purpose of its index."

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 Ariel Glickman, 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