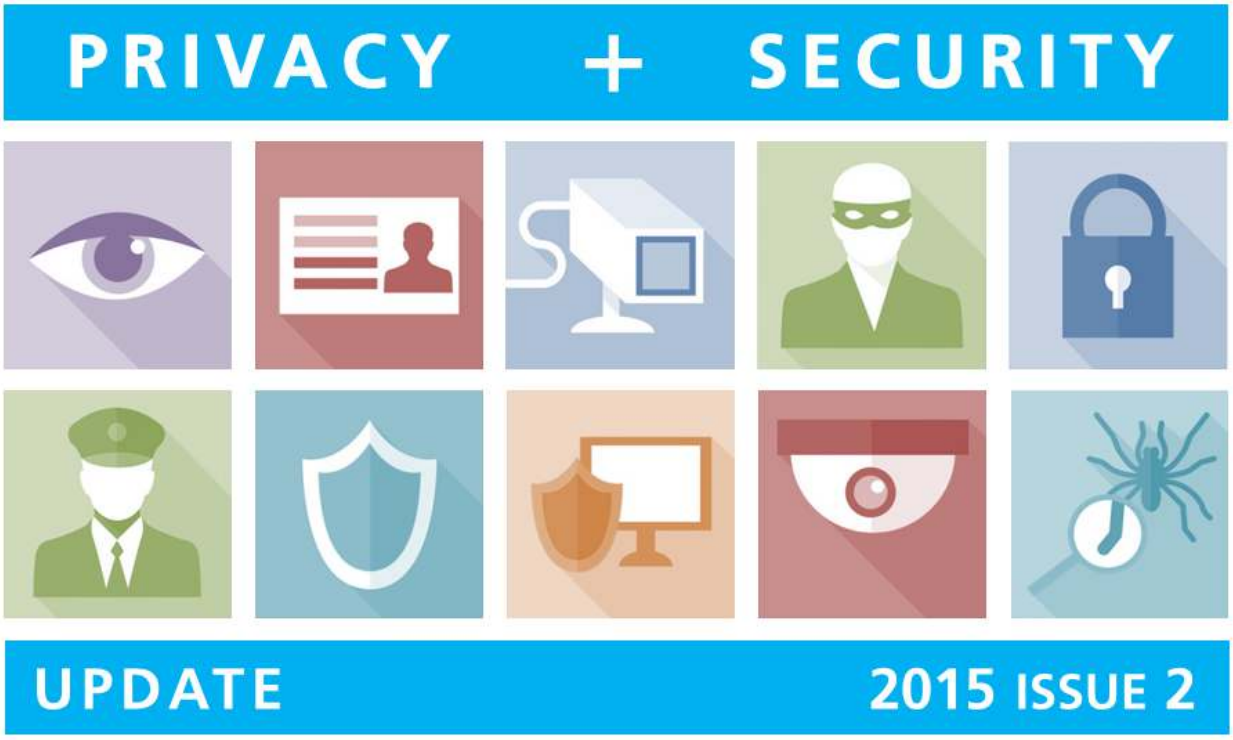


PRIVACY + SECURITY UPDATE

Facebook Privacy Sherpas, the Internet of Things, and Other Privacy + Security Updates

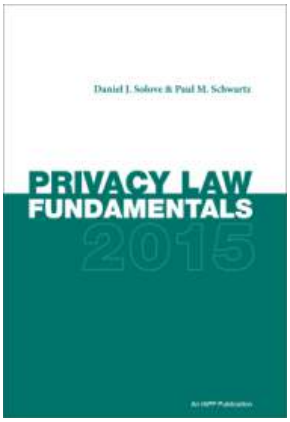
By Daniel J. Solove + Paul M. Schwartz

2015 Issue 2

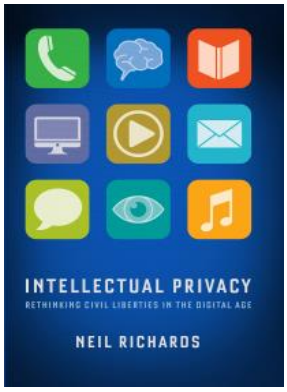
This post is part of a post series where we round up some of the interesting news and resources we're finding. For a PDF version of this post, and for archived issues of previous posts, click here.

GENERAL DEVELOPMENTS

Books



Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals (3rd ed. 2015) [Link]
" This book is my go-to reference for when I need quick, accurate information on privacy laws across sectors and jurisdictions. Solove and Schwartz masterfully make complex privacy law more accessible and understandable for anyone, from the most experienced practitioner to first year law student." – Nuala O'Connor, Center for Democracy & Technology



Neil Richards, Intellectual Privacy, Rethinking Civil Liberties in the Digital Age (2015) [Link]
My book jacket blurb: "*Intellectual Privacy* is a profound and compelling account of how privacy is essential to freedom to speak, write, read, think, create, and explore new ideas. Neil Richards demonstrates how surveillance by the government and companies threaten those core values at the foundation of any democratic society. With great thoughtfulness and engaging writing, *Intellectual Privacy* is lively and accessible, yet rigorous and powerful. This is one of the most important books about freedom of speech and ideas ever written."

Articles, Blog Posts, and Scholarship

Alessandro Acquisti, Laura Brandimarte, & George Loewenstein, Privacy and Human Behavior in the Age of Information, 347 Science 509 (Jan. 2015) [Link]
Overview of Professor Acquisti's social science research about privacy, demonstrating that many common understandings about people's attitudes and behavior of privacy are wrong.

Science, Special Issue: The End of Privacy (Jan. 2015) [Link]
A series of interesting articles about privacy.

General Privacy and Security 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.
-- 70+ 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.

Symposium On Usable Privacy and Security (July 22-24, 2015 in Ottawa, Canada) [Link]

-- Brings together "an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy."

PRIVACY AND THE MEDIA

Identifying Anonymous Speakers

Music Group Macao Commercial Offshore Ltd. v. Does I-IX, 2015 WL 75073 (N.D. Cal., Jan. 6, 2015) [Link]
Music Group and its CEO sued several defendants, all of whom were anonymous Twitter users. The plaintiffs claimed that these unnamed defendants had tweeted the company encouraged domestic violence and spread rumors that the CEO frequented prostitutes. The court held that the plaintiffs could subpoena the identifies of the speakers without violating the First Amendment.

Online Shaming

Jon Ronson, How One Stupid Tweet Ruined Justine Sacco's Life, N.Y. Times (Feb. 12, 2015) [Link]
-- Chronicles the online attacks and shaming of a person who made one bad tweet.
-- I love Andrew Myers' illustration with this story

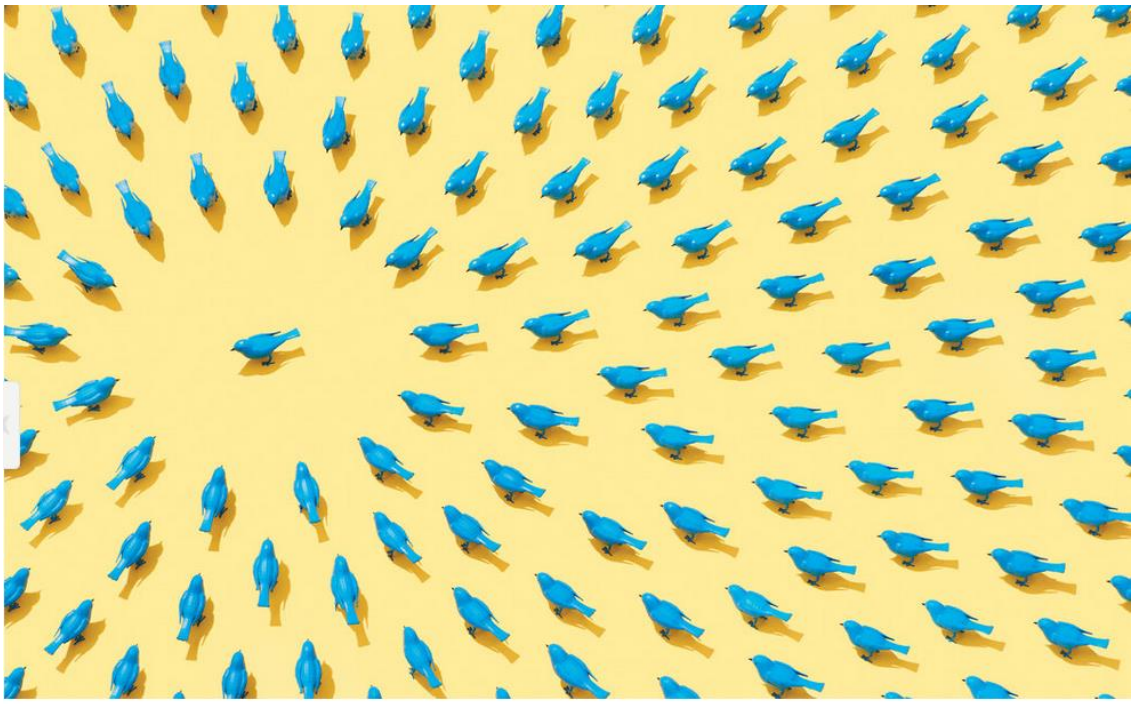


Photo illustration by Andrew B. Myers. Prop stylist: Sonia Rentsch.

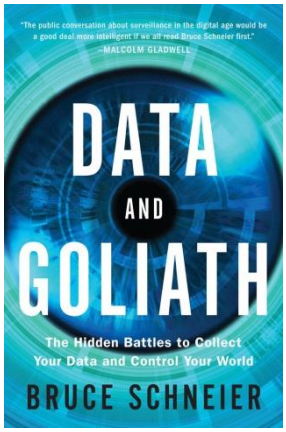
Social Media Use

Researchers Demonstrate that Facebook "Likes" Predict Personality, Mental Health, Political Views Better than Friends or Family [Link]
-- Quote from article: "Researchers from Cambridge and Stanford universities have created a computer program which can use Facebook 'likes' to predict personality traits like openness, conscientiousness, and neuroticism. With a given number of 'likes', the program can predict personality traits more accurately than friends (70 'likes'), family (150 'likes'), and even spouses (300 'likes'). What's more, the researchers found that computer's judgments had 'higher external validity when predicting life outcomes such as substance use, political attitudes, and physical health.'"

PRIVACY AND LAW ENFORCEMENT

Books

Bruce Schneier, *Data and Goliath* (March 2015) [Link]
-- Schneier examines NSA surveillance, the Snowden revelations, and more. Schneier is a wise and compelling thinker, reasoned and not shrill. Everything he says is worth listening to.
-- Blurb by Prof. Yocai Benkler "*Data and Goliath* is the indispensable guide to understanding the most important current threat to freedom in democratic market societies. Whether you worry about government surveillance in the post-Snowden era, or about Facebook and Google manipulating you based on their vast data collections, Schneier, the leading, truly independent expert writing about these threats today, offers a rich overview of the technologies and practices leading us toward surveillance society and the diverse solutions we must pursue to save us from that fate."



NATIONAL SECURITY AND FOREIGN INTELLIGENCE

NSA

Mark Hosenball and Warren Strobel, Reuters, *Obama Abandons Telephone Data Spying Reform Proposal* (2015) [Link]
-- The Obama Administration abandoned a proposal to give a third party control over the U.S. telephone call data that the NSA gathered.

-- Although the Obama Administration does not want a third party to control the data, the President still intends for a non-governmental actor to retain it.

Foreign Intelligence Surveillance Act

Government Releases Two FISC Opinions in EFF FOIA Lawsuit (Jan. 26, 2015) [Link]
On Jan. 26, 2015, in response to a FOIA lawsuit, the government released two opinions of the Foreign Intelligence Surveillance Court (FISC) dating from 2007. The ongoing lawsuit, filed by the Electronic Frontier Foundation (EFF), seeks to obtain key FISC opinions "reinterpreting federal surveillance" after Sept. 11, 2001. The opinions are available here and here.

HEALTH PRIVACY

HIPAA: Enforcement

1.5 Years in Prison for a HIPAA Violation [Link]
A man was sentenced to 1.5 years in prison for a HIPAA violation

State Law

New Jersey S562 [Link]
-- Health insurance carriers must encrypt patient data; they "shall not compile or maintain computerized records that include personal information, unless that information is secured by encryption or by any other method or technology rendering the information unreadable, undecipherable, or otherwise unusable by an unauthorized person."
-- Password-protected access is no longer sufficient; encryption must be used
-- Violations are considered a violation of New Jersey's Consumer Fraud Act
-- Potential for treble damages
-- Effective August 1, 2015
-- Contrast to HIPAA, where encryption is "addressable" rather than required
-- Applies just to health insurance carriers, not to providers
-- For helpful analysis, see Kiki Taylor at Norton Rose Fullbright Data Protection Report [Link]

Medical Identity Theft

Ponemon Institute, *2014 Fifth Annual Study on Medical Identity* (Feb. 2015) [Link]
-- 2 million+ patients victimized by identity theft in 2014
-- 22% increase from 2013
-- 65% of victims had to pay more than $13,000 in costs to deal with the identity theft

Lawsuits

Jennifer Emily, *Free from Ebola but Not Fear*, Dallas Morning News (Feb. 28, 2015) [Link]
-- From the article: " She says that Texas Health Resources violated her privacy while she was a patient at Presbyterian by ignoring her request that "no information" be released about her. She said a doctor recorded her on video in her hospital room and released it to the public without her permission."
-- "Before Pham's flight to Maryland on Oct. 16, she said, a doctor wearing a video camera under his protective hood came into her room and said he was filming her for educational purposes. Pham said she did not give permission for the video, which was released to the media."
-- See Daniel J. Solove's earlier blog post, *Ebola and Privacy: Snooping, Confidentiality, and HIPAA* [Link]

Conferences

healthprivacysummit

5th International Summit on the Future of Health Privacy (June 3-4, 2015 – Washington, DC) [Link]
-- Keynotes include Deanna Fei and Lucia Savage
-- Registration is free to attend or watch live-streaming video.

Articles, Blog Posts, and Scholarship

World Privacy Forum, Student Privacy 101: Health Privacy in Schools—What Law Applies? (2015) [Link]

Deborah Peel, The Greatest Data Breach You've Never Heard Of, TED Talk (2015) [Link]
Critiques existing rules and protections regarding privacy of health data

M. Leeann Habte, Jennifer M. Forde, & Claire N. Marblestone, The Regulatory Framework of Genetic Privacy, Bloomberg BNA (Jan. 26, 2015) [Link]
-- Explores the overlapping state and federal laws protecting consumers' genetic information.
-- "The federal Genetic Information Nondiscrimination Act (GINA) and state laws prohibit such discrimination. With regards to the protection of genetic information more generally, however, the Health Insurance Portability and Accountability Act (HIPAA) imposes no special restrictions on the use and disclosure of sensitive information, such as genetic information. All protected health information (PHI) is subject to essentially the same standards. In contrast, state laws impose a host of special restrictions on the collection, retention, use, disclosure and form of consent for genetic information. Therefore, organizations that collect and use genetic information in multiple states must be aware of these differing compliance obligations."

FINANCIAL DATA

Fair Credit Reporting Act (FCRA)

***Freckleton v. Target Corp.*, No. 14-0807, 2015 WL 165293 (D. Md. Jan. 12, 2015)** [Link]
Denying Target's motion to dismiss, a court allowed a rejected job applicant's Fair Credit Reporting Act claims to proceed. The plaintiff's FCRA claims are premised on the company's practice of running background checks on job applicants and then, without prior notice, using the information to take adverse employment actions. Target argued that its conduct fell within the FCRA's Section 1681a(y) exception, which waives the prior notice requirement when an employer is conducting an investigation of an employee. Finding the exception inapplicable, the court noted that the background check "was not performed in connection with an investigation into misconduct," but rather was initiated to determine if the individual had ever violated any law ever. Interpreting the investigation exception to permit such a broad inquiry, the court held, would allow the exception to destroy the rule and vitiate the protections that the act was intended to provide.

CONSUMER DATA

Electronic Communications Privacy Act (ECPA)

In re Carrier IQ, Inc., No. 12-MDL-2330, 2015 WL 274054 (N.D. Cal. Jan. 21, 2015) [Link]
Ruling on a motion to dismiss, a federal court rejected smart phone manufacturers' claims that the plaintiffs lacked standing and failed to state a claim under the Wiretap Act. The suit alleges that the manufacturers installed error-logging software on its phones that also collected a variety of information about the substance of users' phone usage, such as URLs visited and the contents of text messages. The court ruled that plaintiffs alleged injury in fact where their phones' performance had been degraded by the software's operation. The court further found

that the plaintiffs had sufficiently alleged a Wiretap Act claim because: (1) the logging of incoming and outgoing text message constitutes an "interception" (2) text message and search terms constitute the "contents" of communication, although usernames and passwords do not (3) software can constitute a "device."

Internal Privacy Compliance

Kashmir Hill, *The Guy Standing Between Facebook and Its Next Privacy Disaster,* Fusion (Feb. 2, 2015) [Link]
-- Survivor TV show winner Yul Kwon now serves as Facebook's privacy conscience – refers to his team as "privacy sherpas"
-- Reviews new products and changes for privacy issues via "Privatron," his tool for keeping track of more than 1000 Facebook projects
-- "FTC consent decrees are wonderful things, aren't they?" says Grimmelman. "They force companies to slow down and actually plan their privacy protections using a rational process."
-- "Kwon says the Federal Trade Commission's crackdown was a turning point for the company: 'The FTC consent order made it a priority for us.'"

"We refer to ourselves as the privacy sherpas."

Yul Kwon, head of Facebook's privacy program (PHOTO CREDIT: Christophe Wu/Facebook)

Computer Fraud and Abuse Act (CFAA)

***United States v. Steele*, --- Fed. Appx. ----, 2014 WL 7331679 (4th Cir. Dec. 24, 2014)**
-- Ruling on an appeal from a criminal conviction, the Fourth Circuit weighed in on the "dialogue among the circuit courts on the reach of 18 U.S.C. § 1030(a)(2). "The broad view holds that when employees access computer information with the intent to harm their employer, their authorization to access that information terminates, and they are therefore acting 'without authorization' under § 1030(a)(2). The narrower construction . . . holds that § 1030(a)(2) applies to employees who unlawfully access a protected computer, but not to the improper use of information lawfully accessed." "This split," the court noted "focuses on employees who are authorized to access their employer's computers but use the information they retrieve for an improper purpose."
-- Adhering to its narrow construction of the law, the court upheld a defendant's criminal conviction for accessing his former employer's servers. It distinguished the case hand from those limiting CFAA liability by noting that termination of employment logically terminates authorized access, rejecting, inter alia, the defendant's argument that, because his former employer failed to change its server password, his access was not unauthorized.

Internet of Things

FTC Report, Internet of Things: Privacy & Security in a Connected World (Jan. 27, 2015) [Link]
-- Recommendations include: (1) security by design – building security into devices as they are being designed; (2) training employees about security (music to my ears!); (3) good vendor management; (4) data minimization; (5) a flexible approach to notice and choice.
-- Takes the position that legislation on the Internet of Things would be premature
-- Recommends data security and beach notification legislation
-- FTC Commissioner Maureen Ohlhausen's partial dissent from FTC Internet of Things Report (Jan. 27, 2015) [Link]
-- FTC Commissioner Wright's dissent from FTC Internet of Things Report (Jan. 27, 2015) [Link]

TRUSTe Releases Data on Consumer Attitudes Towards Smart Devices (Jan. 2015) [Link]
TRUSTe has released new data showing growing consumer interest in "connected" devices.

-35% own a smart device other than a smart phone, smart TV's are the most popular
-79% say "T*hey're concerned that the devices will snap up their personal information"*
-69% want data stored on consumer's smart devices to belong to the device owner

Future of Privacy Forum, *The Connected Car and Privacy: Navigating New Data Issues* (2014) [Link]
This paper discusses the extent of the data gathered from automobiles, and how the information is employed. For instance, other than the widely known geolocation data in vehicles that help drivers navigate through GPS and onboard sensors, through these sensors, data can be collected on the physical and biological characteristics of a driver, including enabling facial and voice recognition and tracking vital signs. The prediction is that cars will be capable of adapting to different drivers in the future through the use of these sensors, which can detect a specific driving style, and cameras that can immediately identify a driver. Automakers are also researching whether vehicles can record a driver's health in real-time, such as incorporating sensors in the steering wheel to detect the driver's pulse and temperature. In gathering data on the driver's alertness, speed, and his manner of stopping and steering, automakers also aim to develop new safety mechanisms that would produce a sound to keep the driver attentive when he is exhausted, or potentially turn off the radio, prevent incoming mobile calls from coming through, or stopping the car if the driver experiences a heart attack.

Privacy Policies

Pew Internet Research, "Web IQ" Quiz (Nov. 25, 2014) [Link]
"52% of internet users believe — incorrectly — that this statement is true, and that privacy policies actually ensure the confidentiality of their personal information."

Resources

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

Reports and Studies

Online Trust Alliance, 2015 Data Breach and Readiness Guide (Feb. 13, 2015) [Link]
-- After reviewing more than 1,000 data breaches from 2014, the Online Trust Alliance (OTA) found that more than 90% of them could have been avoided.
-- The OTA separated the breaches into four categories:

(1) caused by external intrusions (40%)
(2) caused by mistaken or intentional employee action (29%)
(3) caused by lost or stolen devices or documents (18%)
(4) caused by social engineering or fraud (11% percent)

-- "[T]he first nine months of 2014 resulted in 904 million records being exposed, which is a 95% increase from the same period of time in 2013."
-- "[D]ata breaches in 2014 have touched nearly every household and business in North America, Europe and other regions of the world."

> **"While some may claim these breaches are the result of highly technical and sophisticated efforts, the data reported by the FBI and other organizations continually report more than 90 percent were avoidable had widely accepted best practices and security controls been applied." -- Online Trust Alliance**

Data Breaches

ISIS Sympathizers Hack U.S. Central Command Twitter, YouTube Accounts [Link]
On Jan. 12, 2015, unidentified hackers gained access to the Twitter and YouTube accounts for the U.S. Central Command, one of the Pentagon's nine "unified commands." CENTCOM's area of responsibility in Central Asia includes most of the Middle East and North Africa. The hackers had control of the account for about an hour, using them to release information allegedly obtained from Pentagon IT systems. It is not clear how the hackers obtained this information or gained access to the social media accounts. The Pentagon says that most of the information the hackers released was already publicly available and that no classified/operational systems were compromised.

Morgan Stanley Insider Breach - Info on 900 Clients Taken, Politico (Jan. 6, 2015) [Link]
Morgan Stanley announced on Jan. 5, 2015 that a disgruntled employee has absconded with data on up to 900 of its wealth management clients, although none of the stolen data included passwords or Social Security numbers.

Cost of Target Data Breach [Link]
Target data breach cost $162 million thus far.

Ransomware

Alina Simone, *How My Mom Got Hacked,* N.Y. Times (Jan. 2, 2015) [Link]
-- First-person account of dealing with CryptoWall ransomware.
-- "But Mr. Wisniewski had a more pragmatic take. 'From what we can tell, they almost always honor what they say because they want word to get around that they're trustworthy criminals who'll give you your files back.' Welcome to the new ransomware economy, where hackers have a reputation to consider."

Other News of Note

Security Risks for Fingerprint "Passwords" [Link]
"Biometrics researcher Jan Krisller demonstrated how he spoofed a politician's fingerprint using just a high definition photo at a conference held by the Chaos Computer Club in Germany this weekend. Krisller, who also goes by "Starbug," and the group previously showed off a way to spoof Apple's Touch ID system by creating a fake finger modeled off a fingerprint left on a glass surface."

The Most Popular Passwords of 2014 [Link]
The top 10:
1. 123456
2. password
3. 12345
4. 12345678
5. Qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football

EDUCATION PRIVACY

Cyberbullying

Natasha Singer, *Protecting Data Privacy at School and Play*, NYT (Dec. 2, 2014) [Link]
"Ms. Dennedy recommended that parents ask the chief technology officer at their children's school for a list of software programs used in the classroom as well as the specific kinds of information each collected from students. She also encouraged parents to ask what kind of security protocols were being used to secure students' personal information."

Illinois Law May Provide Access to Social Media Passwords in Cyberbullying Cases [Link]
-- Illinois Right to Privacy in the School Setting Act: "An elementary or secondary school must provide notification to the student and his or her parent or guardian that the elementary or secondary school may request or require a student to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website if the elementary or secondary school has reasonable cause to believe that the student's account on a social networking website contains evidence that the student has violated a school disciplinary rule or policy." [Link]
-- According to a letter from a school district sent to parents: "School authorities may require a student or his or her parent/guardian to provide a password or other related account information in order to gain access to his/her account or profile on a social networking website if school authorities have reasonable cause to believe that a student's account on a social networking website contains evidence that a student has violated a school disciplinary rule or procedure." [Link]

Conferences

THE HIGHER EDUCATION PRIVACY CONFERENCE

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.

INTERNATIONAL PRIVACY LAW

European Union

Finland's Information Society Code [Link]
-- Finland recently passed the Information Society Code, which codifies a number of existing data privacy and security laws, as well as new laws and standards.
-- Higher standards for of security for electronic communication distributors, including companies based outside of the EU but offer services within Finland.
-- Telecom providers and service providers (e.g., online retailer) jointly liable to consumers for problems that arise from consumer transactions.
-- For more background, see Eeva Haaramo, *Finland gets tough on privacy, with new law to give Apple, Facebook messages total security*, Norse Code, Jan. 5, 2015 [Link]

Asia

New Chinese Regulation Defines "Consumer Personal Information" [Link]
The Chinese State Administration for Industry and Commerce released its Measures for the Punishment of Conduct Infringing the Rights and Interests of Consumers, defining consumer personal information as "information collected by an enterprise operator during the sale of products or provision of services, that can, singly or in combination with other information, identify a consumer." Specific examples include name, gender, occupation, birth date, identification card number, residential address, contact information, income and financial status, health status, and consumer status."

25 Billion Cyberattacks in Japan in 2014 [Link]
-- Increase from 310 million in 2005
-- Lesson: Invest in cyberattacks – better growth than the stock market! :)

Australia

Office of the Australian Information Commissioner, *Guide to Securing Personal Information* (Jan. 2015) [Link]
Provided guidance about "reasonable steps entities are required to take under the Privacy Act of 1988) to protect personal data.

***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."

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

Click below to sign up for Professor Solove's newsletter. It is free and is only sent out occasionally, so it will not clog your inbox.