ABA Privacy and Information Security Developments

May 2017 Update
(April 17-May 25, 2017)
presented May 31, 2017
Jenner & Block LLP

Mary Ellen Callahan
Calvin Mohammadi
Brett Weinstein
Carla Weiss
Agenda

• Regulatory Update (Weinstein)
• Enforcement Actions (Callahan)
• Litigation Update (Mohammadi)
• Data Breach and Cybersecurity (Weiss)
Federal Regulatory

- **NPRM** on Broadband ISPs and Net Neutrality Rules ("Restoring Internet Freedom Notice of Proposed Rulemaking").
- Final NPRM is substantively very similar to the draft released by Chairman Pai on April 27.
- Changes:
  - Asks about the jurisdictional effects of finding broadband to be an interstate information service.
  - References the D.C. Circuit’s denial of the petition for rehearing *en banc* of its decision upholding the 2015 Title II Order, and the Ninth Circuit’s grant of the petition for rehearing *en banc* of its decision regarding the scope of the common carrier exemption in Section 5 of the FTC Act.
State Regulatory

– Illinois legislation (SB 1502 and HB 2774)
  • Based in part on California’s “Shine the Light” law but much more expansive.
  • Requires disclosures regarding information sharing practices.
  • Requires operators to make available information upon disclosing to a third party
  • Provides for a private right of action.

– H.B. 3449 would prohibit the use of geolocation information without customer consent.
– GDPR Update
  • Goes into effect May 25, 2018, just under a year from now.
  • The Garante (Italian data protection authority) released its first guide for the application of the GDPR.
  • Bavarian Data Protection Authority released a questionnaire to assist with GDPR implementation.
  • The Irish regulator has launched www.GDPRandYou.ie.
Cybersecurity Law (CSL) (China) effective June 1, 2017.

- It has now released several draft accompanying rules.
- The CSL and the rules create new obligations for “critical infrastructure,” however what qualifies is unclear.
- The obligations upon “critical infrastructure,” including data localization and security assessments, are also ill-defined.
- China may delay full implementation of the law, giving companies more time to prepare; potential 18-month phase-in period from June.
Federal Legislation

• Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act of 2017
Target reaches settlement with 47 state Attorneys General and DC on 2013 breach

- Led by CT and IL AGs
- Required security standards including encryption in transit and at rest
- Comprehensive security program w CISO
  - Many requirements already in place
- Comply with PCI DSS
NY State Enforcement

NY AG Settlement with Safetech Products

• Insecure wireless doors and padlocks
• Bluetooth-enabled products
• Allegation that the Safetech locks failed to secure passwords (security researchers, 8/16)
• NY AG settlement:
  – Encrypt all passwords/keys/credentials
  – Prompt users to change default password
  – Establish comprehensive security program
Enforcement

FTC, State and International Partners - Crackdown on Tech Support Scams

• *Operation Tech Trap* – trick consumers, charge to “repair” computer

• 16 enforcement actions May 12 announcement, 29 in total

• Criminal charges against 7

• Florida, Alabama, Province of Ontario
Final Settlement in Turn, Inc.
April 21 (originally announced December 2016)

• Misrepresented opting out of targeted advertising
FTC workshops

• April 17, 2017 – Health and Technology
• May 24, 2017 – Identity Theft
• June 28, 2017 – Connected Cars
Litigation – Class Actions

Moreno v. SF Bart, 4:17-cv-02911 (N.D. Cal)

- Claim: SF BART’s app, “BART Watch,” secretly collects personal data.
- The purpose of the app is to allow users to report criminal activity observed while riding BART. The complaint alleges that the app also collects unique mobile identification numbers and device locations without disclosing this to users, allowing BART to periodically monitor users’ locations even when they aren’t using the app and to track the identities of purportedly anonymous reporters.

Zak v. Bose Corp., 1:17-cv-02928 (N.D. Ill.)

- Claim: Bose secretly collects and shares information about its app users’ listening habits.
- The Bose Connect app allegedly discloses users’ private listening histories and preferences to third parties.

Auman v. Confide Inc., 1:17-cv-02848 (S.D.N.Y.)

- Claim: Confide, a private messaging app used by members of the Trump administration, fails to adhere to its privacy promises.
- Confide is a self-proclaimed “encrypted, ephemeral and screenshot protected messenger” service. The complaint alleges that it is easy to change a couple system settings to reduce the effectiveness of its privacy safeguards.
Litigation – Class Actions

Richards v. MD Live, Inc., 0:17-cv-60760 (S.D. Fla.)
• **Claim:** Telehealth provider MDLive’s app secretly captures screenshots of sensitive patient information, and stores and covertly transmits those screenshots without restricting access to medical providers with a legitimate need to see the data.

Martin v. Scottrade Inc., 8:17-cv-01042 (M.D. Fla)
• **Claim:** Scottrade failed to take appropriate steps to protect consumers’ sensitive data, which resulted in a breach that compromised over 4.6 million people’s personal info.
• The complaint alleges Scottrade beached a duty to its customers by failing to design and implement firewalls, by failing to properly and adequately encrypt data and by unnecessarily retaining personal information.
Litigation - Settlements

**Target**

- Target reached an $18.5 million settlement to resolve investigations into a 2013 data breach – the largest multistate data breach deal ever reached.
- The 2013 breach resulted in the payment card info of 41 million customers being compromised.
- Under the terms of the deal, Target must adopt advanced security measures, including a comprehensive info security program and hiring independent personnel to update and maintain data encryption programs.
- Target had previously reached a $39 million settlement with financial institutions, and is close to reaching a $10 million settlement with consumers to end multidistrict litigation.

**Kmart**

- Kmart reached a $5.2 million deal (including $1.7 million in attorneys fees) that ends a dispute with a class of banks. The deal will be finalized once an Illinois federal judge reviews the settlement distributions.
- The lawsuit was filed in 2015 by financial institutions that were forced to reimburse funds stolen from Kmart customers after a breach that resulted in the information from 8.1 million credit and debit cards being stolen by hackers who breach point of sales systems.
Litigation

**FTC v. AT&T Mobility LLC, 3:14-cv-04785 (9th Cir.)**

- Early May: Ninth Circuit granted the FTC’s request for rehearing en banc of the Court’s earlier decision to dismiss an FTC case against AT&T over allegedly “unfair and deceptive” practices.
- The original decision held AT&T was not subject to FTC jurisdiction due to being a common carrier.
- The activities at issue were non-common carrier activities, but the Court had held the exemption was “status based,” not “activity based.”
- This decision had removed a wide class of telecommunications and technology activities from the FTC’s jurisdictional reach.

**In re: Vizio Inc. Consumer Privacy Litigation, 8:16-02693 (C.D. Cal.)**

- **Vizio** litigation: various privacy challenges to televisions that, until a recent settlement with the FTC, were programmed to collect users’ video watching history for advertising purposes.
- The District Court allowed the case to move forward, finding Vizio was a “video tape service provider” under the VPPA.
- Mid-May: the Chamber of Commerce filed an amicus brief urging immediate appellate review. The brief highlights the potential the Plaintiffs’ arguments have to disturb well established internet advertising business models.
- Late May: Vizio argued its settlement with the FTC rendered the case moot.
Litigation

**Krakauer v. Dish Network LLC, 1:14-cv-00333 (M.D.N.C.)**

- January: a North Carolina jury awarded a class of Dish customers $20.5 million for illegal telemarketing calls made by a marketer working w/ Dish. The marketer made calls to Dish customers without checking if recipients were on the Do-Not-Call Registry.
- May: a North Carolina federal judge trebled those damages to $61 million because Dish was aware the marketer had a history of TCPA violations, and nonetheless performed virtually no oversight of the marketers operations.

**Beckman v. Niantic Inc., 50-2016-CA-008330**

- **Claim:** a Pokemon Go user sued the app maker alleging the game’s privacy policy and terms of use were deceptive and unenforceable because they reserved the right for the app maker to gather consumer data.
- A Florida judge dismissed the case because the plaintiff was not able to show he suffered an actual injury.
- The judge reasoned that the plaintiff’s case was based only on “fears of possible of speculative future injury”/that Niantic might in the future collect the plaintiff’s personal data.
Litigation

In re Opinions and Orders Addressing Bulk Collection of Data, 13-08, U.S. Foreign Intelligence Surveillance Court

• 2013: ACLU and Yale Media Freedom and Information Access Clinic asked the surveillance court to unseal its judicial opinions dealing with the legality of collecting data en masse. The decisions were made public in 2014, but with significant redactions.
• The ACLU and Yale Clinic asked for the redacted portions to be released, and in January 2017, the surveillance court in an en banc opinion denied that request on jurisdictional grounds.
• Late April: ACLU and Clinic urged a full bench to reconsider this denial, arguing that the public has a First Amendment right to access the secret legal discussions.


• Late May: 4th Circuit resurrected constitutional challenge to the NSA’s “upstream” collection of internet communications. This reversed and remanded an October 2015 ruling that Wikimedia lacked standing.
• The 4th Circuit found Wikimedia plausibly claimed its communications had been intercepted by the NSA b/c it engages in more than 1 trillion annual communications that go through every possible channel of the internet, so its communications must have been intercepted by the NSA at least once.
Microsoft Sues Over Xbox Game Currency Theft

- May 19: Microsoft filed a trio of suits in California federal court
- The suits allege that websites run by Chinese companies and residents have reaped millions of dollars by
  - selling access to stolen Microsoft accounts
  - fraudulently acquiring virtual gaming currencies, which allow Xbox users to buy upgrades and enhancements
- The suit doesn’t accuse the defendants of hacking accounts to obtain virtual currencies but of illegally obtaining the credentials of accounts, presumably from third-party hackers, and trafficking them through a site called iGSKY.
  - Microsoft has already managed to have iGSKY’s PayPal account shut down
Wannacry Ransomware Attack

• May 12: worldwide cyberattack encrypting data and demanding Bitcoin ransom payments
• Affected computers were those that had not been updated with a Microsoft security patch released in March
  - Primarily affected computers running Windows 7
• Attack infected more than 230,000 computers in over 150 countries, including: Britain’s National Health Service, Spain's Telefónica, FedEx, and Deutsche Bahn
• The fortuitous discovery of a “kill switch” allowed a malware researcher to shut down the software before it executed its payload, stopping the spread of the ransomware before the US was greatly affected.
Trump Cybersecurity EO

- Issued May 11, 2017, President Trump EO presents continuity with President Obama’s multiple EOs on cybersecurity rather than a departure on policy.
- Primarily focuses significantly on federal agencies and their own cybersecurity readiness through three major areas of focus.

1. Risk management and IT modernization in the executive branch
   - Requires adherence to the NIST Framework
   - Requires agency heads to each prepare a risk management report
   - Preferences shared IT services across the executive branch
(2) Protection of critical infrastructure

- Requires various agency heads to identify how they can support the cybersecurity efforts of critical infrastructure entities
- Focused on “section 9 entities”—those “at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”
- Directs various agency heads to address three types of potential threats: (1) botnets (automated and distributed attacks); (2) power outages associated with a significant cyber incident; and (3) cybersecurity risks facing the defense industrial base and its supply chain.

(3) Consumer Cybersecurity

- Requires a report to focus “on the Nation’s strategic options for deterring adversaries and better protecting the American people from cyber threats”
- Requires a report an engagement strategy for cybersecurity international cooperation
- Promotes cybersecurity workforce development
Thank you!

Mary Ellen, Calvin, Brett and Carla

Jenner & Block LLP
mecallahan@jenner.com
cmohammadi@jenner.com
bweinstein@jenner.com
cweiss@jenner.com