troutman sanders

Data Privacy: The Current Legal Landscape

By:
Mark Mao
Ronald Raether, Jr.
Yanni Lin
Sheila Pham
Jonathan Yee
Sadia Mirza
Julia Hoffmann
Molly DiRago
Melanie Witte
Julie Hoffmeister

Annual Compendium – February 2018

DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE

(Annual Compendium, Ver. 1.1, February 22, 2018)

By Mark Mao, Ronald Raether, Jr., Yanni Lin, Sheila Pham, Jonathan Yee, Sadia Mirza, Julia Hoffmann, Molly DiRago, Melanie Witte, and Julie Hoffmeister

A. Data Breach Litigation: Beyond *Spokeo*

1. Consumer Breach Litigation: Moving Past *Neiman Marcus*
2. Business-to-Business Breach Litigation: Moving Past *Target*

B. Data Misuse Litigation: Where Technicalities Matter

1. Cases on Web and Online Tracking and Aggregation
   - ✓ For Preinstalled Computer Programs
   - ✓ For Website Data and Advertisement Exchanges
   - ✓ For Online Media

2. Cases on Mobile Tracking and Aggregation
   - ✓ For Mobile Ecosystems
   - ✓ For Mobile Videos
   - ✓ For the Driver's Privacy Protection Act (DPPA)

3. Cases on IoT Tracking and Aggregation, and Emerging Technologies
   - ✓ For Geolocation Tracking Technologies
   - ✓ For Audio Tracking Technologies
   - ✓ For Facial Tracking Technologies

C. Product Liability Litigation

D. Lessons Learned

IV. Developments in Regulatory Enforcement

A. The Federal Trade Commission

B. HIPAA Enforcement

C. Other Administrative Enforcement Efforts

V. Notable International Developments

A. *Schrems* 2.0 and the Future of EU-U.S. Data Flows

B. The Revised Draft ePrivacy Regulation

C. China's "Network Security Law" – One Year Later

I. INTRODUCTION – WHY DATA-BASED PRODUCTS ARE OUR FUTURE

In the last few years, the right to privacy has been hotly debated in the United States. Although not nearly as draconian as the views in Europe, some "consumer advocates" have taken issue with data collection as intrusive and offensive.

However, what critics do not understand or appreciate is that the next technological paradigm is completely dependent on both the quality and quantity of data. As connected things (IoT) explode in popularity, they make things such as augmented reality (AR) and autonomous vehicles possible. Indeed, data scientists have often explained that machine learning and artificial intelligence are heavily dependent on the quality of the data,[1] and not just the quantity of data. Where real-time data is available across a wide variety of different product verticals affecting the human experience, they enable AR and automation.

Despite the lack of clear regulation and guidance, companies will likely not be deterred in continuing to collect, use, and share geolocation data. As interconnectivity grows, so do the opportunities, and the companies that fail to leverage those opportunities may find themselves falling behind their competitors. In venturing into location-based advertising in augmented reality, companies should stay informed of recent enforcement actions, cases, and laws to determine how their role within the ecosystem may be impacted.

II. NEW LEGISLATION, REGULATIONS, AND INDUSTRY GUIDANCE

A. CHANGES AND UPDATES TO STATE BREACH STATUTES

Delaware: On August 17, 2017, Delaware revised its data breach notification law, which will take effect on April 14, 2018.[2] Key changes include:

- Broadening the definition of "personal information";
- Adding a risk of harm exception to notification;
- Requiring companies to offer free credit monitoring for a year if the breach involves an individual's social security number;
- Notice to Delaware's attorney general if the affected number of Delaware residents to be notified exceeds 500 residents; and
- Notification must occur no later than 60 days after determination of a breach.[3]

[1] Sessions, *et al.*, *The Effects of Data Quality On Machine Learning Algorithms* (MIT 2006), available at: http://mitiq.mit.edu/ICIQ/Documents/IQ%20Conference%202006/papers/The%20Effects%20of%20Data%20Quality%20on%20Machine%20Learning%20Algorithms.pdf; *see also* Lovatt, *The Need For Quality Data With Artificial Intelligence* (Blue Sheep, Mar. 29, 2017), available at: http://www.bluesheep.com/blog/the-need-for-quality-data-with-artificial-intelligence-0.

[2] https://legis.delaware.gov/BillDetail/26009

[3] *Id.*

Illinois: On May 6, 2016, Illinois revised its data breach notification law, which took effect on January 1, 2017. Key changes include[4]:

- Broadening the definition of "personal information," which now includes, among other things, medical information, health insurance information, biometric data, and an individual's "user name or email address in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach."[5]

Maryland: On May 4, 2017, Maryland revised its data breach notification law, which took effect on January 1, 2018.[6] Key changes include:

- Broadening the definition of "personal information" (which now includes, among other things, biometric data and health insurance identifiers);
- Notification must occur no later than 45 days after discovery or notification of a breach; and
- Allowing for alternative notice when a breach involves access only to an individual's email account, provided that certain requirements are met.[7]

New Mexico: On April 6, 2017, New Mexico enacted its first data breach notification law, which became effective on June 16, 2017.[8] Key points include:

- "Personal information" includes an individual's first name or first initial and last name in combination with a social security number, driver's license number, government-issued identification number, account number, credit card number, or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account, or biometric data;
- Risk of harm exception to notification if after appropriate investigation, it is determined that the breach does not give rise to significant risk of identity theft or fraud;
- Notification must occur no later than 45 days following discovery of the breach; and

[4] http://www.ilga.gov/legislation/publicacts/99/PDF/099-0503.pdf
[5] http://www.ilga.gov/legislation/BillStatus.asp?DocTypeID=HB&DocNum=1260&GAID=13&SessionID=88&LegID=85740
[6] http://mgaleg.maryland.gov/webmga/frmMain.aspx?id=hb0974&stab=01&pid=billpage&tab=subject3&ys=2017RS
[7] *Id*.
[8] https://www.nmlegis.gov/Legislation/Legislation?chamber=H&legType=B&legNo=15&year=17&AspxAutoDetectCookieSupport=1

- Notice to New Mexico's attorney general and major consumer reporting agencies if more than 1,000 New Mexico residents are notified.[9]

Tennessee: On April 4, 2017, Tennessee's governor signed into law an amendment to the state's data breach notification statute, effective the same day.[10] Key points include:

- Clarifying "that the consumer protection violation of failing to disclose a security breach of personal consumer information applies to a breach of unencrypted data or encrypted data when the encryption key has also been acquired by an unauthorized person";
- Revising the definitions of "breach of system security" and "personal information"; and
- Clarifying that "the present law authorization to extend the 45-day time limit for providing notice following a data breach by an additional 45 days applies when the legitimate needs of law enforcement require such an extension."[11]

Texas: On June 12, 2017, Texas amended its data breach notification law (affecting only state agencies and election data), which became effective on September 1, 2017.[12] Key changes include:

- Notification is required not just for breaches but also suspected breaches and unauthorized exposure of sensitive personal information; and
- Notification must occur no later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, to the department, including the chief information security officer and the state cybersecurity coordinator and/or the secretary of state (depending on the type of data involved).[13]

Virginia: On March 13, 2017, Virginia amended its data breach notification law, which became effective on July 1, 2017.[14] The amendment added notification requirements for "any employer or payroll service provider who experiences a breach of an employee's tax identification number and income tax withheld for that employee must notify the Attorney General's Office without unreasonable delay and provide the name and federal employer identification number (FEIN) of the employer suffering the breach."[15]

---

[9] *Id*.
[10] http://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0547&GA=110
[11] *Id*.
[12] http://www.legis.state.tx.us/billlookup/Actions.aspx?LegSess=85R&Bill=HB8
[13] http://www.legis.state.tx.us/billlookup/Text.aspx?LegSess=85R&Bill=HB8
[14] http://lis.virginia.gov/cgi-bin/legp604.exe?171+ful+CHAP0427 and https://www.oag.state.va.us/CCSWEB2/files/Data_Breach_Notification_Req.pdf
[15] *Id*.

B. NEW STATE LEGISLATION ON E-COMMERCE AND BIOMETRICS

1. Nevada's Amendments Regulating E-Commerce

As with many other states, Nevada responded to the FCC's repeal of FCC 16-148 with the tightening of its own laws on e-commerce.[16] Like California's Shine the Light Law, Nevada Senate Bill 538 requires that an internet operator make available a notice containing certain information relating to the privacy of covered information about consumers that is collected by the operator through its internet website or "online service."

SB 538 covers the connected networks of IoT in addition to the world wide web, as Section 6(d) requires that covered entities disclose "whether a third party may collect covered information about an individual consumer's online activities over time and across different internet websites or online services when the consumer uses the internet website or online service of the operator." In addition, SB 538 is unique in that Section 6(b) requires that covered entities provide "a description of the process, if any such process exists, for an individual consumer who uses or visits the internet website or online service to review and request changes to any of his or her covered information that is collected through the internet website or online service" – borrowing protections from the federal Fair Credit Reporting Act.

On the other hand, SB 538 allows an operator to remedy any failure relating to making such a notice available within 30 days after being informed of the failure. The bill authorizes the attorney general to seek an injunction or civil penalty against an operator who engages in any failure to remedy such a failure within 30 days after being informed.[17]

2. Washington's New Law for Biometrics

In May 2017, Washington became the third state[18] to pass state law broadly regulating the collection and use of "biometric information."[19] "Biometric identifiers" include "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique

[16] Chajson, *Nevada Senate Approves Internet Privacy Bill* (Jurist, May 30, 2017), available at: http://www.jurist.org/paperchase/2017/05/nevada-senate-approves-internet-privacy-bill.php.
[17] A copy of Nev. SB 538 may be found at: https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB538.pdf.
[18] *See* Illinois' Biometric Information Privacy Act (BIPA), 740 ILCS 14/1, and Texas' Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code Section 503.001.
[19] 2017 Wa. ALS 299; *see also* Kay, *et al.*, *The Next Steps For Biometrics Legislation Across The U.S.* (Law 360, May 25, 2017), available at: https://www.law360.com/articles/928056/the-next-steps-for-biometrics-legislation-across-the-us.

biological patterns or characteristics that is used to identify a specific individual."[20] The bill prohibits persons and entities from "enroll[ing] a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[21] Like its Texas counterpart, however, the new Washington law does not provide for a private right of action.[22]

Other states such as New Hampshire, Alaska, Connecticut, and Montana are also considering bills regulating the use of biometrics.[23] As the new Washington law demonstrates, however, a critical question will be whether the bill that is passed permits a private cause of action, much like Illinois' BIPA.[24]

C. LAWS AND REGULATIONS SURROUNDING THE GROWTH OF AUTONOMOUS VEHICLES

1. The DOT's "Automated Driving Systems: A Vision for Safety 2.0"

In September 2017, the Department of Transportation (DOT) issued voluntary guidance entitled "Automated Driving Systems (ADS): A Vision for Safety 2.0,"[25] which is intended to update and replace the "Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety," previously issued by the DOT in September 2016 under the Obama Administration.[26]

The September 2017 DOT guidance suggests "12 priority safety design elements" for ADSs, which are intended to help manufacturers "be creative and innovative when developing the best method for its system to appropriately mitigate the safety risks associated with their approach."[27] The guidance applies to vehicles under the National Highway Traffic Safety Administration's (NHTSA) jurisdiction, including heavy-duty commercial vehicles.[28] However, it applies only to vehicles with Automation Levels Three through Five, as defined by the Society of Automobile Engineers (SAE): Level Three (Conditional Automation) requires a driver, but is not required to monitor

[20] "Biometric identifiers" include "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." 2017 Wa. ALS 299, Section 3(1).
[21] 2017 Wa. ALS 299, Section 2(1).
[22] 2017 Wa. ALS 299, Section 4(2).
[23] Grande, *Wash. Expands Biometric Privacy Quilt With More Limited Law* (Law360, Jul. 21, 2017), available at: https://www.law360.com/cybersecurity-privacy/articles/934030/wash-expands-biometric-privacy-quilt-with-more-limited-law?nl_pk=d100b429-aa27-499d-ad44-acee4f8fe74b&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.
[24] *See Why Comcast And Verizon Are Suddenly Clamoring to Be Regulated*, *supra*.
[25] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf, p. i.
[26] https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.
[27] *Id.*, p. 1.
[28] *Id.*, p. 2.

the environment, although the driver must be ready to take control of the vehicle at all times with notice; Level Four (High Automation) allows vehicles to be capable of performing all driving function under certain conditions, while the driver may have the option to control the vehicle; Level Five (Full Automation) allows vehicles to be capable of performing all driving functions under all conditions.[29]

The 12 design elements for focus by manufacturers are:

a) System Safety: "Entities are encouraged to follow a robust design and validation process" adopting and following industry standards and recommendations by established and accredited organizations. Developing safety standards should include testing, validating, and verifying of systems and their individual components;[30]

b) Operational Design Domain (ODD): "Entities are encouraged to define and document the Operational Design Domain." Per the DOT, ADSs "should be able to operate safely within the ODD for which it is designed. In situations where the ADS is outside of its defined ODD or where conditions dynamically change to fall outside of the ADSs' ODD, the vehicle should transition to a minimal risk condition";[31]

c) Object and Event Detection, Classification, and Response (OEDR): OEDR should be able to detect and recognize a variety of objects and events, both for normal and hazardous conditions;[32]

d) Fallback (Minimal Risk Condition): Vehicles should have minimal risk conditions for fallback should any ADS not be able to be operated safely;[33]

e) Validation Methods: The standards of SAE and the International Organization for Standards (ISO) are recommended, but not exclusively;[34]

f) Human Machine Interface: At minimum, the human machine interface provides information as to whether the systems are functioning properly, currently engaged in ADS mode, experiencing a malfunction, and/or are requesting that the control transition from the ADS to the operator;[35]

[29] *Id.*, p. 4.
[30] *Id.*, p. 5.
[31] *Id.*, p. 6.
[32] *Id.*, p. 7.
[33] *Id.*, p. 8.
[34] *Id.*, p. 9.
[35] *Id.*, p. 10.

g) Vehicle Cybersecurity: Entities are encouraged to conduct systematic and thorough planning and testing for cybersecurity, by using practices such as those promulgated by the National Institute of Standards and Technology (NIST);[36]

h) Crashworthiness;

i) Post-Crash ADS Behavior;

j) Data Recording: "Learning from crash data is a central component to the safety potential of ADSs."[37]

k) Consumer Education and Training; and

l) Compliance with Federal, State, and Local Laws.

2. H.R. 3388, the "SELF DRIVE Act"

On September 2017, the House of Representatives also passed H.R. 3388, titled the "Safety Ensuring Lives Future Deployment and Research In Vehicle Evolution Act," or the "SELF DRIVE Act."

By its current terms, the SELF DRIVE Act bill would:

- Preempt new and existing state standards for the "design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems" unless the standard is "identical" to what is promulgated under the SELF DRIVE Act. However, laws and regulations on vehicle registration, licensing, or sales would remain left to the state. Similarly, so would regulations on "safety and emissions inspections, congestion management of vehicles on the street within a State or political subdivision of a State, or traffic unless the law or regulations is an unreasonable restriction on the design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems."[38]

- Require the Secretary of Transportation and the National Highway Traffic Safety Administration to issue long-term goals, plans, and guidelines, with express priorities and goals.[39]

[36] *Id.*, p. 11.
[37] *Id.*, p. 14.
[38] http://docs.house.gov/meetings/IF/IF00/20170727/106347/BILLS-115-HR3388-L000566-Amdt-9.pdf, Sec. 3.
[39] *Id.*, Sec. 4.

- Provide that a manufacturer may not offer for sale or introduce into commerce any highly automated vehicle, vehicle that forms partial driving automation, or automated driving system unless such manufacturer has developed a written cybersecurity plan that includes: (a) a written security plan that includes preventive measures, testing and monitoring, and updates; (b) limiting access to automated systems; and (c) employee training.[40]

- Require that a manufacturer may not offer for sale or introduce into commerce any highly automated vehicle, vehicle that forms partial driving automation, or automated driving system unless such manufacturer has developed a written privacy plan that describes: (1) how information of owners and occupants are collected, used, shared, and stored; (2) choices available for owner and occupant privacy; (3) manufacturer practices with respect to data minimization, de-identification, and data retention; and (4) the privacy obligations of the those who receive data from the manufacturer. Interestingly, the bill takes the position that "information about vehicle owners or occupants [that] is altered or combined so that the information can no longer reasonably be linked" to the vehicle, component, software, owner, or occupants need not be included in the privacy policy. Violations of this provision shall be enforced by the Federal Trade Commission under Title 5 of the FTC Act.[41]

- Raise the potential number of self-driving cars that a manufacturer can put on the road, including up to 100,000, by way of applying for exemptions, such as if the manufacturer can demonstrate that their vehicles provide "an overall safety level at least equal to the overall safety level of nonexempt vehicles."[42]

- Set up an industry advisory council and subcommittees that would report both to Congress and make certain information public.[43]

It is unclear if the SELF DRIVE Act will pass at all, or pass with any of these provisions unchanged. However, it is important to note that as self-driving technology continues to improve, momentum for federal standards to be put in place will continue to grow, as demonstrated by how the bill had overwhelmingly passed in the House.[44]

D. THE FIGHT OVER DATA PRIVACY REGULATIONS IN BROADBAND

1. Should the FCC Retreat from ISPs?

[40] *Id.*, Sec. 5.
[41] *Id.*, Sec. 12.
[42] *Id.*, Sec. 6.
[43] *Id.*, Sec. 9.
[44] *Should the Feds Be Responsible for Developing Safety Regulations for Self-Driving Cars?* (Countable 2017), https://www.countable.us/bills/hr3388-115-safely-ensuring-lives-future-deployment-and-research-in-vehicle-evolution-act.

Last August, the Ninth Circuit held in *FTC v. AT&T Mobility* that the FTC and FCC could not share jurisdiction over "common carriers," because whether or not an entity was a common carrier was based on the general status of the entity and not on its activity at any given time.[45] Until *AT&T Mobility*, the telecommunications industry had considered itself to be regulated by the FCC only when it was engaged in "traditional common carrier" activities. But when it engaged in what were traditionally considered "non-common carrier activities" – for example, when it acted as a mere internet service provider (ISP) – the telecommunications industry argued that it was not subject to the jurisdiction of the FCC. If the FCC had no jurisdiction over ISP-related activities, the FTC argued that they would have jurisdiction. *AT&T Mobility* flatly rejected the dichotomy.

Self-proclaimed "privacy advocates" welcomed *AT&T Mobility*, as it followed FCC ex-Commissioner Tom Wheeler's contentious 2015 announcement that ISPs would be considered "common carriers."[46] Where the FTC had no jurisdiction over ISPs, and ISPs were also considered common carriers, the FCC would have comprehensive jurisdiction over all data carriers. The FCC moved swiftly in accordance with the apparent political winds, issuing FCC 16-148 to regulate the data privacy practices of all common carriers, from cellular phone providers to ISPs. The FCC guidance had required ISPs to not only maintain comprehensive cybersecurity programs but also to provide detailed disclosures and obtain consumer opt-ins for data tracking.[47]

With the surprising ascension of the Trump Administration, however, Commissioner Wheeler stepped down and Republican Commissioner Ajit Pai was appointed Chairman of the FCC. Pai quickly revoked the classification of ISPs as common carriers[48] and revoked FCC 16-148.[49] Additionally, Pai sought to "secure online privacy by putting the FTC…back in charge of broadband providers' privacy practices,"[50] while announcing future plans to "restore Internet Freedom by repealing Obama-era Internet regulations."[51]

---

[45] *FTC v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016), 1003.
[46] Ruiz, *FCC Approves Net Neutrality Rules, Classifying Broadband Internet Service As a Utility* (New York Times, Feb. 26, 2015), available at: https://www.nytimes.com/2015/02/27/technology/net-neutrality-fcc-vote-internet-utility.html.
[47] FEDERAL COMM'CNS COMM'N, FCC 16-148, Report and Order; see also, Jenna Ebersole, *FCC Sets New Privacy Framework For Broadband Providers*, LAW360 (Oct. 27, 2016), available at: https://www.law360.com/articles/856450/fcc-sets-new-privacy-framework-for-broadband-providers.
[48] Kastrenakes, *FCC Announces Plan to Reverse Title II Net Neutrality* (The Verge, Apr. 26, 2017), available at: https://www.theverge.com/2017/4/26/15437840/fcc-plans-end-title-ii-net-neutrality.
[49] Ebersole, *3 Things to Watch After FCC's Privacy Rules Get The Ax* (Law360, Mar. 31, 2017), available at: https://www.law360.com/articles/908508/3-things-to-watch-after-fcc-s-privacy-rules-get-the-ax.
[50] Ebersole, *FTC, FCC Chiefs Seek to Set "Record Straight" On Privacy* (Law360, Apr. 5, 2017), available at: https://www.law360.com/articles/910144/ftc-fcc-chiefs-seek-to-set-record-straight-on-privacy.
[51] *Restoring Internet Freedom For All Americans* (FCC, April 26, 2017), available at: https://www.fcc.gov/document/restoring-internet-freedom-all-americans

On December 14, 2017, the FCC and FTC jointly issued a "Restoring Internet Freedom, FCC-FTC Memorandum of Understanding," formally memorializing the FCC and FTC's "joint efforts" to regulate ISPs, with the FTC "monitor[ing] the broadband market," and the FTC "investigat[ing] and tak[ing] enforcement action as appropriate…"[52] But *AT&T Mobility* is still Ninth Circuit precedence. Thus, whether a "joint effort" will be sufficient to fill the jurisdictional gap created by the case is still an open question – not to mention that whether the two agencies can even truly work together has yet to be proven.[53]

As of the date of this publication, the FCC has announced that it is now standing alongside the FTC in the FTC's appeal of *AT&T Mobility*. The FCC filed an amicus brief, agreeing with the FTC that the Ninth Circuit Court should have ruled that whether a provider was a common carrier was activity-dependent, not status-dependent. Otherwise, the FCC argues, ISPs could potentially be operating without regulatory supervision.[54]

2. FTC Regulation in Lieu of the FCC?

Setting aside the jurisdictional questions, it is unclear whether the FTC will actively police the data practices of ISPs. As a practical matter, the FTC has been far less active in policing data privacy practices under the Trump Administration than under the Obama Administration. For example, as devices have become more connected, the FTC issued several publications on cross-device tracking in the beginning of 2017 before the presidential election results. Noting that the Digital Advertising Alliance was also beginning to enforce its industry self-enforcing cross-device tracking requirements, the FTC opined in its "Cross-Device Tracking" staff report:

- With regard to de-identification and anonymization, the FTC "has repeatedly stated that data that is reasonably linkable to a consumer or a consumer's device is personally identifiable." Therefore, "consumer-facing companies that provide raw or hashed email addresses or usernames to cross-device tracking companies should refrain from referring to this data as anonymous or aggregate,

[52] Available at: https://www.ftc.gov/policy/cooperation-agreements/restoring-internet-freedom-fcc-ftc-memorandum-understanding.
[53] Carson, *As Movement to Repeal Net Neutrality Grows, 9th Circuit Decision Looms* (IAPP Jan. 10, 2018), available at: https://iapp.org/news/a/as-movement-to-repeal-net-neutrality-grows-9th-circuit-decision-looms/.
[54] Eggerton, *FCC to Court FTC Common Carrier Exemption Is Activity Based* (Broadcastingcable.com Jun. 2, 2017), available at: http://www.broadcastingcable.com/news/washington/fcc-court-ftc-common-carrier-exemption-activity-based/166269.

and should be careful about making blanket statements to consumers stating that they do not share 'personal information' with third parties."[55]

- With regard to opt-outs, the FTC indicated that it still takes the position that a consumer's exercise of an opt-out in one forum requires that the company affirmatively honor the opt-out in all other contexts and forums. The FTC recommended that consumer-facing companies and cross-device tracking companies should cooperate and coordinate "to ensure that all actors in the ecosystem are making truthful claims about the choices afforded to consumers."[56]

Given such broad policy statements, one would have expected that the FTC would have continued aggressively drawing lines for cross-device tracking practices throughout 2017, as hardware, applications, and stakeholders are becoming even more interconnected and codependent. Instead, as further discussed below, the FTC has been relatively quiet. That silence is suggestive of the likeliness that the FTC will continue to stay quiet in 2018 against broadband carriers and ISPs, as the broadband carriers and ISPs continue to innovate and push deeper into various data-based products.

Even if the FTC takes a more aggressive stance in the coming months, however, the FTC's regulatory powers are much more limited than those of the FCC. Where the FCC is tasked with the responsibility of regulating common carriers under the Telecommunications Act, the FTC is only given the power to prohibit "unfair and deceptive acts" under the Title 5 of the FTC Act. As Democratic FTC Commissioner Terrell McSweeny pointed out, "ISPs could change their terms of service at will, and so long as they were not deceptive, the FTC could do nothing about them beyond requiring ISPs to adhere to them, whatever they are."[57]

3. Will States and Cities Regulate Broadband Privacy?

With the retreat of the FCC and its efforts to police the data privacy practices of ISPs, states and cities have decided to take regulatory efforts into their own hands. In April, 11 state legislatures – including Minnesota, Nevada, Illinois, Massachusetts, Wisconsin, Montana, and Washington – introduced privacy bills intended to fill the gap

[55] *Cross-Device Tracking: An FTC Staff Report* (Jan. 2017), available at: https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf., at p. 12-13.
[56] *Id*. at 14.
[57] Eggerton, *McSweeny to FCC: FTC's Consumer Protection Authority Insufficient to Discipline ISPs* (Broadcasting & Cable, Jul. 20, 2017), available at: http://www.broadcastingcable.com/news/washington/mcsweeny-fcc-ftcs-consumer-protection-authority-insufficient-discipline-isps/167316.

left by the FCC. Critics pointed out that such bills were hastily drafted, often without sufficient understanding of the affected industries.[58]

Cities have since attempted to issue their own regulations as well. In Seattle, Mayor Ed Murray issued new rules requiring opt-in consent from users before cable internet providers collected user web-browsing history and other internet usage data.[59]

In the meanwhile, there are bipartisan efforts on Capitol Hill to reintroduce data privacy bills that would help fill the gap created by the FCC's withdrawal.[60] Nothing has been successful to date. Nonetheless, ISPs are now threatened with patchwork-regulation due to the flurry of state and local activity. Ironically, some have proposed their own "internet bill of rights,"[61] while others have requested that federal regulators step back in to prevent potentially conflicting state laws and local codes.[62]

E. NIST PREPARES FOR IOT AND AUTONOMOUS TECHNOLOGIES

1. NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*

The fifth draft version of NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations* ("Draft Version 5") was recently released for public comment.[63] The primary stated purpose of the publication is to assist in the design of privacy and security controls. Although previous versions have already been used as a basis for security and privacy architecture for years, legal and technical professionals should review the changes to better understand NIST's larger effort to update all its major publications for the advent of IoT.

---

[58] Kaye, *Industry Plays Whack-a-Mole to Fight Slew of State Privacy Bills* (Advertising Age, Apr. 17, 2017), available at: http://adage.com/article/privacy-and-regulation/industry-plays-whack-a-mole-fight-state-privacy-bills/308664/.

[59] *Seattle Restored ISP Privacy Rules In The First Local Blow to Trump's Rollback* (Fast Company, May 5, 2017), available at: https://news.fastcompany.com/seattle-restored-isp-privacy-rules-in-the-first-local-blow-to-trumps-rollback-4036776.

[60] Neidig, *House Republican Looks to Democrat Allies On Internet Privacy Bill* (The Hill, Jun. 6, 2017), available at: http://thehill.com/policy/technology/336592-house-republican-looks-for-dem-allies-on-internet-privacy-bill.

[61] Koenig, *AT&T Ad Pushes "Internet Bill of Rights"* (Law360, Jan. 24, 2018), available at: https://www.law360.com/articles/1005261/at-t-ad-pushes-internet-bill-of-rights-.

[62] Fung, *Why Comcast And Verizon Are Suddenly Clamoring to Be Regulated* (Jun. 28, 2017), available at: https://www.washingtonpost.com/news/the-switch/wp/2017/06/28/why-comcast-and-verizon-are-suddenly-clamoring-to-be-regulated/?hpid=hp_hp-cards_hp-card-technology%3Ahomepage%2Fcard&utm_term=.55aa48b2fe87, detailing how four telecom companies are arguing against AT&T and in favor of FTC regulation in the case of *FTC v. AT&T Mobility*.

[63] *Security And Privacy Controls For Information Systems And Organizations*, Draft Publ. 800-53 Ver. 5 (NIST 2017), available at: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf.

In contrast to the previous version of Publication 800-53, Draft Version 5 states that it:

- Incorporates security and privacy controls that are focused on outcome-based designs (i.e., the outcome would justify the design);
- Integrates privacy controls directly with security controls;
- Separates the selection of controls from the design of the controls, with the former being moved to an anticipated update to NIST Special Publication 800-37, *Risk Management Framework*; and
- Incorporates new state-of-the-art controls and designs to improve both cybersecurity and privacy governance.[64]

Draft Version 5 contains invaluable wisdom on IoT ecosystems for legal professionals and technologists alike. Legal professionals should use Draft Version 5 to set up their baseline policies and checklists. Technologists should look to Draft Version 5 for baseline standards in data collection and cybersecurity.

Closer Coordination between Privacy and Security

Chapter 2 includes many "fundamentals," which serve as themes embodying the NIST's vision for IoT: (a) closer coordination between privacy and security controls, (b) setting control baselines, and (c) greater emphasis on assurances and trustworthiness.

Section 2.4, "Security and Privacy Control Relationship," describes a common misunderstanding amongst those who are new to data privacy – privacy controls are not necessarily security controls. Privacy controls relate to what type of data an organization collects, how it uses it, and how it maintains that information. Security controls secure that information, but they do not necessarily prevent an organization from collecting or using data unless a privacy practice creates security concerns.

[64] Draft Publ. 800-53, Ver. 5, p. v-vi.

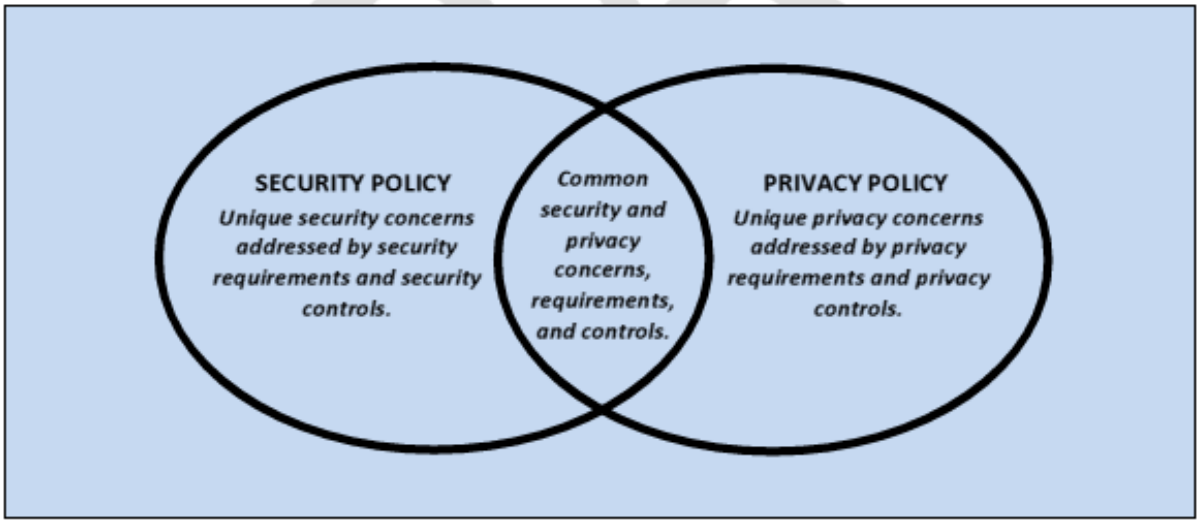

FIGURE 1: SECURITY AND PRIVACY RELATIONSHIP

[65]

Understanding the distinction is particularly important in the age of IoT, as the gatekeepers of data collection are not necessarily tasked with security, and vice versa. As IoT ecosystems and product verticals explode in connectivity, it becomes even more important for different gatekeepers to coordinate with each other to facilitate user privacy while ensuring data security.

Setting Control Baselines

Section 2.5 on Control Baselines defines a control baseline as "a collection of controls…specifically assembled or brought together to address the protection needs of a group, organization, or community of interest." It also "provides a generalized set of controls that represents an initial starting point for the subsequent tailoring activities that can be applied to the baseline to produce a more targeted or customized security and privacy solution for the entity it is intended to serve."[66]

Although it is not stated in Section 2.5, control baselines are increasingly important because IoT environments typically include multiple stakeholders, from the ecosystem owner to developers, processors, aggregators, and third-party advertisers. While organizations continue to compete for a foothold in IoT, NIST's hope is that control baselines will at least provide common ground amongst different stakeholders to discuss sharing some common privacy and security standards.

Greater Emphasis on Assurances and Trustworthiness

[65] Draft Publ. 800-53, Ver. 5, p. 12.
[66] Draft Publ. 800-53, Ver. 5, p. 13.

Whereas traditional security models focus on preventing vectors and intrusion, Publication 800-53 (or Draft Version 5) focuses heavily on trustworthiness and assurance. NIST defines "trustworthiness" as "worthy of being trusted to fulfill whatever critical requirements may be needed," and assurance as "the measure of confidence that the system functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system."[67] As will be more fully demonstrated herein, although the draft publication states that it is now more outcome focused, many of the new recommendations are still focused more on establishing procedural assurances and trustworthiness, with the desired outcome being the hopeful result.

Access Controls

Draft Version 5 contains several pieces of "supplemental guidance" that focus on refining controls for increasingly connected environments. "The Controls" begin with Section 3.1 on Access Controls:

- Section 3.1, AC-4 on Information Flow Management includes supplemental guidance on best practices for both facilitation and securing data flows, including monitoring object attributes and embedded objects, improving filters and data identification, and the logical and physical partitioning of data flows.

- Section 3.1, AC-8 on System Use Notification contains display and disclosure requirements not only to inform users of the organization's data collection practices (e.g., monitoring and recording), but also to monitor logins and system use.

- Section 3.1, AC-16 on Security and Privacy Attributes includes supplemental guidance on better establishing and maintaining proper security and privacy attributes, separating them amongst various active entities (i.e., individuals) and passive entities (i.e., objects). Those who have kept up with NIST's serialized releases and updates on IoT know that properly characterizing various individual and object attributes is important to NIST's design evolving framework for IoT.[68] Notably, because IoT allows for many potential user interfaces (UIs), AC-16(5) requires identification and control of displays for output devices. In addition, because user customization is often a selling point for IoT devices, AC-16(10) requires that organizations identify and control user configurations.

- Section 3.1, AC-18 on Wireless Access includes supplemental recommendations on assessment and reassessments to "limit the unauthorized use of wireless

[67] Draft Publ. 800-53, Ver. 5, p. 14.
[68] *See, e.g., Network of 'Things'*, Special Publ. 800-183 (NIST July 2016), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf.

communications outside of organization-controlled boundaries," and prevent attacks via wireless vulnerabilities.

- Section 3.1, AC-19 on Access Control and AC-20 on Use of External Systems are critical sections on those that support "bring your own device (BYOD)." AC-20(3) enumerates virtualization as a potential technique to limit security risks. AC-20(4) recommends that unclassified mobile devices be restricted from accessing modems, wireless interfaces, and classified data. AC-20(5) recommends container encryption for mobile environments.

- Section 3.1, AC-23 on Data Mining Protection provides new and supplemental recommendations to protect against data mining, by limiting the type and number of server inquiries and notifying the organization when unusual requests occur.

Audit, Testing, and Monitoring

- Section 3.3 on Audit and Accountability considers auditing for cloud and software-as-a-service (SaaS) models, in addition to using technology to conduct audits.

- Section 3.4 on Assessment, Authorization, and Monitoring has been updated to include some IT-best practices for user authorization and monitoring. Although NIST Special Publication 800-37 was meant to be open for adoption by both government and private organizations, CA-3 on System Interconnections left in requirements based on nationally classified information databases, while supplementing suggestions on authorization controls. Direct external connections to classified security systems are prohibited; direct external connections to unclassified security systems are prohibited without the use of authorized boundary protection devices; direct connections to public networks are prohibited; external connections are permitted by exception only (i.e., white-listed); and secondary and tertiary connections to interconnected systems should be controlled, verified, and validated.

- Section 3.4, CA-7 on Continuous Monitoring recommends monitoring including independent assessments, trend analysis, and risk monitoring (of risk measures).

Configuration Management and Contingency Planning

- Section 3.5, CM-2 on Baseline Configurations provides quintessential requirements for baseline configurations, which form a backbone of NIST's vision for IoT. CM-2(3) provides that an organization should retain "previous versions of baseline configurations to support rollback...[including] for example, hardware, software, firmware, configuration files, and configuration records."

- Section 3.5, CM-3 on Configuration Change Control recommends procedural justification and documentation of changes to baseline configurations, including cryptography management in CM-2(6). CM-4 to CM-6 provide additional recommendations regarding configuration changes.

- Section 3.5, CM-7 on Least Functionality recommends that unused systems, components, functions, and services be disabled, and if possible, that those used be whitelisted.

- Section 3.5, CM-8 on System Component Inventory provides supplemental recommendations on how to take inventory of system components. Notably, it recommends a non-duplicative and centralized inventory, geo-location tracking of components to detect compromise, and data mapping of personally identifiable information.

- Section 3.6 on Contingency Planning requires contingency plan design, training, testing, and establishing documented procedures for the same.

Identification and Authorization

Section 3.7 on Identification and Authorization has been updated to include some best practices. Interestingly, IA-2 on Identification and Authentication (Organizational Users) recommends multifactor authentication for access to both privileged and unprivileged accounts. In addition, IA-3 on Device Identification and Authentication recommends cryptographically-based bidirectional authentication before a connection can be made.

Individual Participation, Incident Response, and Privacy Authorization

Notably, the section regarding individual participation of subjects giving their data (Section 3.8) precedes the incident response section (Section 3.9). Such order places more focus on notice over consent. More importantly, Draft Version 5 discusses consumer choice in ways that are more closely aligned with international trends. Section 3.8, IP-3 on Redress discusses data subject redress mechanisms for data "accuracy," which is only required as a matter of American law in a limited number of industries. Section 3.8, IP-4, recites certain privacy-by-design principles while encouraging that privacy statements be written in ways that will be easy for the average consumer to understand. Lastly, Section 3.8, IP-6 on Individual Access recommends that individuals be permitted to access their personally identifiable information.

Section 3.12 on Privacy Authorization then tackles privacy recommendations from the perspective of collecting organizations as opposed to the perspective of the consumer. Again, paralleling international trends, Section 3.12, PA-3 on Purpose

Specification discusses limitations by initial "specifications" dictated privacy statements, which are more consistent with the tone set by European laws. Similarly, PA-4 on Informational Sharing with External Parties discusses proportionality and consistency with privacy statements to data subjects.

Planning and Program Management

- Section 3.14, PL-4 on Rules of Behavior recommends that organizations prescribe expected behavior from users with access.

- Section 3.14, PL-8 on Security and Privacy Architectures recommends supplier diversity, which is a departure from those who recommend tightly controlled security ecosystems through a limited set of closely-tied developers.

- Section 3.14, PL-10 on Baseline Selection again recommends an appropriate control baseline for the system, and adds that organizations might want to seek input from industry and related communities.

- Section 3.15 on Program Management contains a robust checklist for information officers setting up privacy compliance and security programs. By going through the 32 recommendations, then referencing the other sections for more specific explanations, information officers will be able to properly document each step of their privacy program setup.

System and Services Acquisition

Much like NIST's other recent updates with a focus on IoT, Draft Version 5 brings a much heavier emphasis on the vetting of suppliers and vendors as part of the product lifecycle.

- Section 3.18, SA-3 on System Development Life Cycle recommends the documentation of privacy and security goals and responsibilities throughout the system life cycle.

- Section 3.18, SA-4 on Acquisition Process recommends that organizations include in their acquisition contracts express specifications on how privacy and security goals could be defined, approved, monitored, tested, and achieved.

- Section 3.18, SA-9 on External System Services recommends that organizations include in their external services agreements express specifications on how to identify functions, ports, protocols, services, cryptography, processing, storage, and geographic location – in addition to specifying things such as how the provider would act in ways consistent with the interests of consumers.

- Section 3.18, SA-10 on Developer Configuration Management recommends that organizations require the developer of systems, system components, and system services to document and manage integrity changes, implement only approved changes, and track security flaws and resolutions. SA-10 goes onto additional detail, including recommending that design, change, and distribution of software, firmware, and hardware all be based on trust. Notably, SA-10 requires assessment of not just the object code, but the source code as well.

- Section 3.18, SA-12 on Supply Change Management recommends that organizations implement and document safeguards for their supply chains. SA-12 requires that supply chains be identified, tracked, researched, tested, validated, reassessed, and rehabilitated upon any findings of deficiencies.

- Section 3.18, SA-15 on Development Process, Standards, and Tools, recommends that organizations require their developers to follow a documented process focusing on "attack surface reduction," which "includes, for example, employing concept of layered surface defenses; applying the principles of least privilege and least functionality; depreciating unsafe functions; applying secure software development practices…and eliminating application program interfaces (APIs) that are vulnerable to attack."

- Section 3.18, SA-18 on Tamper Resistance and Detection recommends that organizations employ anti-tampering techniques for the system, system components, and system services.

- Section 3.18, SA-22 on Unsupported System Components recommends that components no longer available from the developer, vendor, or manufacturer be replaced.

System and Communication Protection

Section 3.19 has been substantially updated to accommodate the increased use of mobile and connected technologies. Recommendations include many updated best practices, including:

- Partitioning of applications (SC-2);

- Security function isolation, including hardware separation, minimizing non-security functions within security function boundaries, and layered structures (SC-3);

- Establishing controls and resource quotas to prevent or minimize damage caused by denial of service attacks (SC-5);

- Boundary controls, such as limiting access points, setting denial of access as default, monitoring internal threats that may compromise boundary safeguards, preventing discovery of components and devices, fail secure against boundary resource failures, design for dynamic isolation of select components, and disabling sender feedback on protocol validation failure (SC-7);

- Establishing and managing mobile code policies and procedures to "prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems" (SC-18);

- Verifying and monitoring session authenticity (SC-22);

- Employing system components with minimal functionality and information storage (SC-25);

- Employing honeypots (SC-26);

- Concealing and misdirection, including through the employ of virtualization (SC-30);

- System partitioning (SC-32);

- Employing honey clients, which actively seek malicious code and intruders (SC-35); and

- Employing detonation chambers, where potentially malicious items and vectors can be tested, but where the environment can then be destroyed (SC-42).

System and Services Acquisition

Section 3.20 on System and Services Acquisition includes an impressive list of robust updated best practices as well.

- Section 3.20, SI-4 on System Monitoring includes supplemental recommendations on system-wide intrusion detection, automated tools for real-time analysis, monitoring of inbound and outbound traffic, automated and manual inspection of anomalies, rogue wireless devices, situational awareness through a variety of information sources, and personally identifiable information monitoring to prevent unintended data coupling.

- Section 3.20, SI-7 on Software, Firmware, and Information Security provides recommendations on integrity checks and controls, such as using cryptographic protection and signatures, verifying and protecting boot processes and software, and verifying the trustworthiness of developers and vendors.

- Section 3.20, SI-12 on Information Management and Retention includes recommendations on minimizing personally identifiable information elements throughout the information lifecycle.

- Section 3.20, SI-14 on Non-Persistence recommends limiting the length of windows of opportunity for attackers, such as by refreshing system components, reimaging, and virtualization.

- Section 3.20, SI-20 on De-Identification includes interesting incorporation of new anonymization and de-identification techniques, such as differential privacy, in addition to more traditional methods such as masking, encryption, and hashing.

Conclusion

Although there will likely be some changes, we do not expect Draft Version 5 to be drastically revised. Therefore, legal professionals and technologists should take time to become familiar with the supplemental recommendations, as they will likely be the new measuring sticks for Publication 800-53.

Specifically, for compliance professionals, we recommend they first assess existing policies and procedures against Sections 3.9, 3.12, and 3.14 through 3.15, followed by additional sections as appropriate. Safeguards for privacy and security need to be properly vetted for consumer purposes as well as for the well-being of the organization as a whole.

For technical professionals, we recommend they assess their increasingly connected environments against Sections 3.5, 3.8, and 3.18 through 3.20, followed by additional sections as appropriate. Updated security and privacy techniques should be considered for incorporation into existing programs.

2. **NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations***

Draft Version 5 of Publication 800-53 promised a revised Publication 800-37 that would serve as the primary complementing guidelines for the selection of security and privacy controls. Almost immediately after Draft Version 5 of Publication 800-53 was released, NIST released a "Version 2 discussion draft" of its Publication 800-37.

By its terms, the "The RMF (Risk Management Framework) includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring. It also includes enterprise-level activities to help better prepare organizations execute the RMF at the system level."[69] Like Draft Version 5 of Publication 800-53, the draft revision to Publication 800-37 provides a number of considerations the organization should undertake and document – from preparation to categorization, to selection, to implementation, to assessment, to authorization, and then to monitoring – to demonstrate due diligence in the selection of organizational security and privacy controls.

The draft also provides a number of practical suggestions on how to best select a streamlined risk management framework:

- "Maximize the use of *common controls* at the organization level to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of *shared* or *cloud-based* systems, services, and applications to reduce the number of authorizations, enterprise-wide.
- Employ organization-wide *tailored* control baselines to increase the focus and consistency of security and privacy plans, and the speed of security and privacy plan development.
- Establish and publicize organization-wide *control parameters* to increase the speed of security and privacy plan development and the consistency of security and privacy plan content.
- Maximize the use of *automated tools* to manage security categorization; security and privacy control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for *low impact* systems if those systems cannot adversely affect higher impact systems through system connections.
- Maximize the *reuse* of RMF artifacts (e.g., security and privacy control assessment results) for standardized hardware/software deployments, including configuration settings.

[69] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Discussion Draft Publ. 800-37 Ver. 2 (NIST 2017), page ii, available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft.

- Reduce the *complexity* of the IT infrastructure by eliminating unnecessary systems, system components, and services — employ *least functionality* principle.

- Transition quickly to *ongoing authorization* and use *continuous monitoring* approaches to reduce the cost and increase the efficiency of security and privacy programs.

- Employ common sense security and privacy controls, *rightsizing* RMF activities for mission and business success."[70]

These suggestions are likely to be in the final version of Publication 800-37, as comparable themes are suggested by Publication 800-53, Draft Version 5.

NIST expects to finalize revisions by March 2018.[71]

F. THE FDA'S POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

On September 6, 2017, the FDA issued its "nonbinding recommendations" guidance for addressing premarket cybersecurity vulnerabilities in connected medical devices under the title "Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices."[72] This should not be confused with the FDA's guidance "Postmarket Management of Cybersecurity in Medical Devices," issued on December 28, 2016, which applies to postmarket cybersecurity vulnerabilities in connected medical devices (and which was covered in our last edition of this serialized publication).[73]

The FDA's guidance applies to interoperable devices, where interoperable devices are defined in Section 201(h)of the Federal Food, Drug, and Cosmetic Act (FD&C Act) as devices that have the ability to exchange and use information through an electronic interface with another medical/non-medical product, system, or device.[74] While the guidance states that it is a "nonbinding recommendation," it represents the

[70] Discussion Draft Publ. 800-37, Ver. 2, page 18.
[71] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft.
[72] FOOD AND DRUG ADMIN., DESIGN CONSIDERATIONS AND PREMARKET SUBMISSION RECOMMENDATIONS FOR INTEROPERABLE MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Sept. 6, 2017), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf.
[73] FOOD AND DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Dec. 28, 2016), http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.
[74] *Id.* at p.4.

FDA's recommendations to its own staff regarding the medical device community's responsibilities.

The FDA's guidance also states that it is designed to provide "manufacturers with design considerations when developing interoperable medical devices," and also to provide "recommendations regarding information to include in premarket submissions and device labeling."[75] This applies to premarket submissions for interoperable devices including premarket notifications, de novo requests, premarket approvals, product development protocols, and biological license applications.[76]

Specifically, for premarket designs, the FDA recommends that the manufacturer:[77]

- Consider the purpose of the electronic interface. This is an important requirement for the FDA, which requires the manufacturer to consider the other types of devices that the device is meant to connect to, the type of data exchanged, standards and requirements for transmission, timeliness, and reliability of information;[78]

- Identify all anticipated users;

- Conduct a comprehensive risk analysis to identify ways to mitigate risks. Here, the FDA recommends that "manufacturers include in their risk management approach a particular focus on the potential hazards, safety concerns, and security risks introduced when including an electronic interface";[79]

- Establish, maintain, and implement appropriate verification and validation to ensure that devices would work correctly, not only during premarket but while in use and with the release of software updates; and

- Use consensus standards related to medical device interoperability – although the FDA states that it is not recommending any particular interoperability standard.[80]

And for premarket submissions, the FDA recommends:

[75] *Id.* at p. 3.
[76] *Id.* at p. 4.
[77] *Id.* at p. 5-6.
[78] *Id.* at p. 6-7.
[79] *Id.* at p. 9.
[80] *Id.* at p. 12.

- That the applicant provide detailed device description, including describing the requirements for timeliness and integrity of information; describing the communications format, rate, and transmission method; discussing what the user should not do, contraindications, precautions, and warnings; discussing the functional and performance requirements; and listing all application programming interfaces if the device is software that can be used by other software, medical device or system;[81]

- Submission of risk analysis that addresses how unacceptable risks would be reduced to acceptable levels; fault tolerant behavior, boundary conditions, and fail-safe behavior; vulnerabilities that may be involved with the availability of an electronic interface; and risks likely arising from normal use as well as reasonably foreseeable misuse;[82]

- Documentation demonstrating appropriate performance testing, including verification and validation that the device and its electronic interface will perform as intended and specified, and that the device will still perform safely under abnormal conditions that are reasonably foreseeable to occur;[83]

- Labeling as recommended by the FDA, much of which are user recommendations resulting from the processes advanced by the FDA guidance.[84]

It is important to note that cyber-vulnerabilities often arise from the use of hardware and software in ways that were originally unintended. Thus, it appears that the FDA has chosen to focus on forcing manufacturers to specify during premarket stages exacting details regarding the purpose of the connected device and its supporting user interface, all other stakeholders in the ecosystem, and notices that will be provided to purchasing users. Like most security standards today, the standard for manufacturers is a procedural one:

> "[The] FDA recognizes that medical device interoperability is a shared risk among stakeholders…Manufacturers should have a defined process to systematically conduct risk evaluation and determine whether a risk is acceptable or unacceptable. It is not possible to describe all hazards and risks associated with medical device interoperability in this guidance. FDA recommends manufacturers define and document their process for objectively

[81] *Id.* at p. 13-14.
[82] *Id.* at p. 14-15.
[83] *Id.* at p. 15-16.
[84] *Id.* at p. 17-18.

assessing the foreseeable use and reasonably foreseeable misuse of their medical device throughout the device lifecycle."[85]

G. CFPB'S CONSUMER PROTECTION PRINCIPLES ON CONSUMER-AUTHORIZED FINANCIAL DATA SHARING

Although the CFPB has been walking on thin ice since the arrival of the Trump Administration, it still issued its "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" on October 18, 2017.[86] Included among the principles embraced are:

- Consumer access – Which should be safe and "not require consumers to share their account credentials with third parties."
- Data scope and usability – "Third parties with authorized access (should) only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary."
- Control and informed consent – Which includes the ability to revoke permissions and delete PI "in a timely and effective manner."
- Access transparency – So that "consumers are informed of, or can readily ascertain, which third parties…are accessing or using information regarding the consumers' accounts or other consumer use of financial services."
- Accuracy – Data that is accurate and current, while providing consumers with "reasonable means to dispute and resolve data inaccuracies…"
- Ability to dispute and resolve unauthorized access.
- Efficient and effective accountability mechanisms.

"Fintechs" and companies that use financial data should pay close attention to how the CFPB enforces its Consumer Protection Principles in the next few years.

H. THE FTC REVISES COPPA GUIDANCE FOR E-COMMERCE AND IOT

In June 2017, the FTC issued a revised Children's Online Privacy Protection Rule (COPPA) "Six-Step Compliance Plan for Your Business," which was primarily revised to cover new business models, new products, and new methods of obtaining

[85] *Id.* at p. 10.
[86] Available at: https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

parental consent.[87] The FTC's guidance clarified many important issues for emerging technology, some of which further tightened requirements:

- "Website or online services" for COPPA includes "connected toys or other Internet of Things devices," which may not necessarily connect over a public internet, and instead even via "offline" connections among "smart things";[88]
- An audio file may be personal information for the purposes of COPPA;[89]
- Even if a third-party is the party responsible for collecting information through your technology, you may still be responsible for complying with COPPA;[90] and
- Smart toys must be able to ensure the confidentiality, security, and integrity of personal information, although such toys may suffer from low-processing capabilities.[91]

On the other hand, some clarifications have made compliance friendlier for developers:

- A privacy policy does not necessarily have to disclose the actual identity of the third-parties receiving information collected, and instead may "list the type of businesses you disclose information to (for example, ad networks) and how they use the information";[92] and
- The FTC appears relatively open to different ways of obtaining consent, including by the receipt of a series of knowledge-based challenge questions that would likely only be known by the parent, and the use of facial recognition technology to validate a photo.[93]

III. EVOLVING CASE LAW

Last year, in the much-anticipated case of *Spokeo, Inc. v. Robins*, the U.S. Supreme Court was presented with the issue of whether a plaintiff that suffered no injury-in-fact may nonetheless have Article III standing for a mere procedural violation

[87] Cohen, *et al.*, *FTC Updates COPPA Compliance Plan For Business* (FTC Jun. 21, 2017), available at: https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business.
[88] *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan For Your Business* (FTC Rev. June 2017), Step 1, available at: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.
[89] *Id.*
[90] *Id.*
[91] *Id.*, Step 6.
[92] *Id.*, Step 2.
[93] *Id.*, Step 4.

under the Fair Credit Reporting Act (FCRA). The Court emphasized that "Article III standing requires a concrete injury even in the context of a statutory violation." [94] But the Court avoided clarifying what is meant by "an injury that is both 'concrete and particularized'," leaving open the possibility that even an "intangible harm" may nonetheless still be "concrete."

On remand, the Ninth Circuit provided no more clarity than the Supreme Court. The Circuit Court provided a two-prong test for ascertaining whether "intangible harm" allegedly prohibited by statute is sufficiently "concrete" for Article III purposes: (a) whether the harm is the type of intangible harm for which the legislature created legislation to protect consumers' concrete interest; and (b) whether the alleged violations actually harm or create a "material risk of harm" to the concrete interest.[95] While the court found that the allegations at issue related to accuracy risks covered by the FCRA, the court noted that some inaccuracies may be too trivial for purposes of the FCRA.[96]

As further demonstrated below, the Circuits remain divided and uncommitted to any firm lines with regard to data breach and privacy litigation. Litigants are likely to reach disparate results after filing *Spokeo*-based motions to dismiss, regardless of which Circuit they may be in.

A. DATA BREACH LITIGATION: BEYOND *SPOKEO*

1. Consumer Breach Litigation: Moving Past *Neiman Marcus*

Despite the mixed results over the past few years, motions to dismiss will likely remain as the first line of defense for defendants in data privacy litigation. For a short period of time, it was unclear whether the momentum had swung in favor of plaintiffs. The Seventh Circuit handed down a pair of appellate decisions in 2015 and 2016, holding that the "concrete and particularized" requirements of Article III were met by allegations of increased threat of fraud and identity theft after data had been stolen, and of the time and money spent trying to resolve such issues. In both instances, the Seventh Circuit held that reasonable inferences must be made in plaintiffs' favor at the pleading stage, particularly on the issue of the sufficiency of fear of future harm to establish Article III standing.[97]

[94] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1545-1550 (2016) (citations omitted).
[95] *Robins v. Spokeo, Inc.*, 2017 U.S. App. LEXIS 15211, *10 (9th Cir. Aug. 15, 2017).
[96] *Id.*, fn. 4.
[97] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 691-694 (7th Cir. 2015) (finding risk of future harm sufficient to establish Article III standing, based on allegations of harm *already* suffered); *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963, 966-967 (7th Cir. 2016) (accord, citing to same reasoning in *Remijas*).

However, other courts in the Seventh Circuit have since disagreed, sustaining motions to dismiss on the alternative ground of lack of sufficient allegations pled.[98] Notably, at least one Illinois District Court found the type of damages alleged in *Nieman Marcus* too *de minimis* to survive a motion to dismiss for failure to a state cause of action pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.[99]

Similarly, in other Circuits where data breach litigation has been just as contentiously litigated as in the Seventh Circuit, courts continued to find ways to dismiss claims in 2017, even where Article III standing was found:

- Third Circuit – The Third Circuit has applied the economic loss rule, making motions to dismiss difficult for plaintiffs to defeat.[100]

- Fourth Circuit – In *Galaria v. Nationwide Mutual Ins. Co.*, the court held that there needs to be credible causation between the alleged fraudulent activities against the consumers and the type of data allegedly breached.[101]

- Eighth Circuit – As with the Seventh Circuit, the Eighth Circuit has required that damage allegations be credible.[102]

- Ninth Circuit – Breach and damage allegations need to be credible and not speculative. In *Foster v. Essex*, for example, the Northern District Court held that because the personal information of plaintiffs were not stored on defendant's server (which was allegedly breached), the court granted defendant's motion for

[98] *In re VTech Data Breach Litig.*, 2017 U.S. Dist. LEXIS 103298 (N.D. Ill. Jul. 5, 2017) (dismissing without prejudice case alleging hackers exploited vulnerabilities in connected toys); *In re Barnes & Noble Pin Pad Litig.*, 2017 U.S. Dist. LEXIS (N.D. Ill. Jun. 13, 2017) (dismissing case based on PIN pad tampering with prejudice); *see also Dolmage v. Combined Ins. Co. of America*, Case No. 14-C-3809 (E.D. Ill., Nov. 8, 2017) (granting motion for summary judgment, finding that the "privacy rider" forming the basis of the alleged breach of privacy obligations was not part of the employer-employee relationship).

[99] *In re Barnes & Noble Pin Pad Litig.*, at *8.

[100] *Longenecker-Wells v. Benecard Servs.*, 2016 U.S. App. LEXIS 15696 (3rd Cir. Aug. 25, 2016) (granting motion to dismiss on basis of economic loss rule, in case relating to fraudulent tax returns filed); *Enslin v. Coca-Cola Co.*, 2017 U.S. Dist. LEXIS 49920 (Mar. 31, 2017) (granting motion for summary judgment on basis of economic loss rule, in employee breach case); but see *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 2017 U.S.App. LEXIS 1019 (3rd Cir. Jan. 20, 2017) (finding standing in case involving stolen laptops involving PII).

[101] *Galaria v. Nationwide Mut. Ins. Co.*, Case No. 13-cv-118, Dk. 89 (S.D. Oh. Aug. 16, 2017) (dismissing all causes of action except for one on bailment, which was subsequently dismissed in *Galaria v. Nationwide Mut. Ins. Co.*, 2017 U.S. Dist. 205304 (S.D. Oh. Dec. 13, 2017)); *but see Savidge v. Pharm-Save*, 2017 U.S. Dist. LEXIS 197635 (W.D. Ky. Dec. 1, 2017) (denying 12(b)(6) motion in part, including on basis the W-2 information allegedly breached and fraudulent tax activity could have causal nexus).

[102] *Alleruzzo v. SuperValue, Inc.*, 2017 U.S. App. LEXIS 16664 (8th Cir. Aug. 30, 2017) (in case involving retail store breach of customer PII, finding future likelihood of harm damages insufficient); *Kuhns v. Scottrade Inc.*, 2017 U.S. App. LEXIS 15817 (8th Cir. Aug. 21, 2017) (finding allegations of harm arising from hack of broker dealer systems too vague and insufficiently pled, failing to allege how any customer had suffered identity theft or damage).

summary judgment on the basis that the claims were implausible.[103] In *Antman v. Uber Technologies*, the Northern District Court granted a motion to dismiss on the basis that the data allegedly sold on the dark web was not the same data set as that which was allegedly breached.[104] And in *Cahen v. General Motors LLC*, the Northern District Court dismissed the complaint based on the vulnerability of connected cars after finding the allegations regarding the threat of future damages to be too speculative.[105] The Ninth Circuit affirmed the District Court's ruling upon appeal.[106][107]

- Eleventh Circuit – Where a plaintiff failed to allege that a fraudulent credit card charge was not reimbursed, the District Court dismissed the claims.[108]

- D.C. Circuit – Like the other five Circuits above, the D.C. Circuit has also required plaintiffs to plead credible damage to survive Rule 12(b)(6) challenges.[109]

In the Fourth and Fifth Circuits, where data breach litigation has been less frequent, courts have been more stringent on plaintiffs. These Circuits have outright dismissed as insufficient claims based on allegations of "future harm."[110]

On the other hand, courts in the Second Circuit are increasingly in conflict. Although motions to dismiss continued to be sustained in 2017,[111] some courts began to depart in early 2018. In *Fero v. Health Plan*, for example, the court reversed part of its prior decision on a motion for reconsideration, finding that certain plaintiffs that had

[103] *Foster v. Essex Prop., Inc.*, 2017 U.S. Dist. LEXIS 8373 (N.D. Cal. Jan. 20, 2017) (granting motion to dismiss because defendants furnished declarations stating that plaintiffs' information was not on the allegedly breached system, and plaintiff failed to rebut the declarations).
[104] *Antman v. Uber Technologies*, Case No. 15-cv-01175, Dkt. 175 (N.D. Cal. Nov. 25, 2017).
[105] *Cahen v. General Motors LLC*, 147 F. Supp. 3d 955, 972 (N.D. Cal. Nov. 25, 2015).
[106] *Cahen v. General Motors LLC*, 2017 U.S. App. LEXIS 26261 (9th Cir. Dec. 21, 2017).
[107] *But see In re Banner Health Data Breach Litig.*, Case No. 16-cv-02696, Dkt. 106 (D. Az. Dec. 20, 2017); *see In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 U.S. Dist. LEXIS 140212 (N.D. Cal. Aug. 30, 2017); *see Walters v. Kimpton Hotel & Rest. Grp.*, 2017 U.S. Dist. LEXIS 57014 (N.D. Cal. Apr. 13, 2017); *see also In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2017 U.S. Dist. LEXIS 18322 (D. Or. Feb. 9, 2017).
[108] *See Torres v. Wendy's Co.*, 2016 U.S. Dist. LEXIS 96947, *8-9 (M.D. Fla. Jul. 15, 2016).
[109] *Welborn v. IRS*, 2016 U.S. Dist. LEXIS 151673 (D.C. Cir. Nov. 2, 2016) (case alleging loss of tax payers' records, finding lack of standing and failure to state a claim, holding that general anxiety and fear of future harm were insufficient); *see also In re: Office of Personnel Management Data Security Breach Litig.* 2017 U.S. Dist. LEXIS 151449, *72 (D.C. Sept. 19, 2017) (while ultimately granting dismissal based on sovereign immunity, court required plaintiffs to plead credible damages).
[110] *Beck v. McDonald*, 2017 U.S. App. LEXIS 2095 (4th Cir. Feb. 6, 2017) (finding speculation on future harm damages too tenuous, affirming lower court's dismissal); *Bradix v. Advance Stores Co.*, 2016 U.S. Dist. LEXIS 87368 (E.D. La. Jul. 5, 2017) (in case alleging loss of employee PII, finding allegations of "as yet identified" attempts to secure vehicle financing insufficient, especially without any negative impact on credit score).
[111] *Whalen v. Michaels Stores, Inc.*, 2017 U.S. App. LEXIS 7717 (2nd Cir. May 2, 2017) (case alleging stolen credit and debit card information, affirming lower court's dismissal on basis of lack of actual fraudulent charges, as opposed to attempted fraud and fear of future harm).

merely alleged "increased risk of harm" (as opposed to actual misuse) had sufficient standing, due to plaintiffs' allegations that their private information was being sold on the dark web.[112] And in *Byrne v. Avery Center For Obstetrics & Gynecology*, the Supreme Court of Connecticut reversed a trial court's dismissal, finding that there might be a private cause of action for breach of confidentiality by a medical center.[113]

In addition, plaintiffs have also begun exploring new theories of liability for data breaches. For example, earlier in 2017, plaintiffs successfully defeated motions to dismiss in two separate cases by arguing that because the FCRA requires consumer reporting agencies to assure that "consumer reports" are delivered only to the intended recipients, also implicit in such a requirement is a security obligation.[114] But the court in one of these cases later dismissed the FCRA cause of action for failure to show the defendant was a "furnisher,"[115] and other district courts have not permitted FCRA causes of action for data breaches.[116]

Meanwhile, the first data breach litigation to receive class certification passed quietly in the first half of 2017. In *Smith v. Triad of Alabama*, the Alabama court certified plaintiffs' proposed Fed. Rules of Civ. Proc. Rule 23(b)(3) classes, in a case involving a breach of fewer than a 1,000 patient records.[117] Despite being the first of its kind, the order received hardly any press coverage.

It is still much more common for plaintiffs to fail to reach class certification. If plaintiffs survive a motion to dismiss, the lack of a unifying federal statute on data incidents typically creates overwhelming individual questions. For example, in *Dolmage v. Combined Ins. Co. of America*, the court found it difficult to find commonality and typicality when trying to reconcile over 20 state laws to determine whether the allegedly

[112] *Fero v. Health Plan*, 2018 U.S. Dist. LEXIS 8999 (W.D.N.Y. Jan. 19, 2018).
[113] *Byrne v. Avery Ctr. For Obstetrics & Gynecology*, 327 Conn. 540 (Jan. 16, 208).
[114] *See, e.g., In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 2017 U.S.App. LEXIS 1019 (3rd Cir. Jan. 20, 2017) (finding standing in case alleging FCRA violations for stolen laptops involving PII); *Galaria v. Nationwide Mut. Ins. Co.*, 2016 U.S. App. LEXIS 16840 (6th Cir. Sept. 12, 2016) (remanding to district court to decide whether plaintiffs sufficiently stated a cause of action under the FCRA, where plaintiffs alleged that they submitted insurance and financial applications to Nationwide thereby creating a duty by Nationwide to secure PII pursuant to FCRA).
[115] *Galaria v. Nationwide Mut. Ins. Co.*, Case No. 13-cv-118, Dk. 89 (S.D. Oh. Aug. 16, 2017).
[116] *In re Experian Data Breach Litig.*, 2016 U.S. Dist. LEXIS 184500 (C.D. Cal. Dec. 29, 2016), at *5-6 ("Plaintiffs cannot allege that there was a 'furnishing' of consumer reports under the FCRA"); *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, at *43-44 (Cons. MDL, N.D. Ala. Sept. 12, 2016) (where plaintiffs argued that their health information were also "consumer reports," the court refused to find either defendant a "consumer reporting agency"); *Dolmage v. Combined Ins. Co. of America*, 2015 U.S. Dist. LEXIS 6824 (N.D. Ill. Jan. 21, 2015) (finding no furnishing of consumer report).
[117] *Smith v. Triad of Ala., LLC*, 2017 U.S. Dist. LEXIS 38574 (M.D. Ala. Mar. 17, 2017) (breach involving records the hospital held for surrounding clinics).

breached privacy policy was part of the insurance contract as a matter of law, and when trying to determine how the damages would be calculated on that basis.[118]

One important defense receiving increasing attention in privacy litigation has been class arbitration waivers. In *Bernardino v. Barnes & Noble Booksellers, Inc.*, 2018 U.S. Dist. LEXIS 15812 (S.D.N.Y. Jan. 31, 2018), the online bookseller successfully compelled plaintiffs to arbitrate their grievances alleging user privacy violations.[119] Where there is no direct contractual privity between the plaintiffs and the defendant vendor, however, at least one circuit court has held that arbitration cannot be compelled.[120] Nonetheless, the trend is towards arbitrability, especially where Congress expressly overrode the efforts of the CFPB to prohibit class arbitrations against banks.[121]

In assessing the trends of 2017, it appears that motions to dismiss are most warranted when a Rule 12(b)(1) challenge can be made alongside a strong 12(b)(6) challenge against the individual causes of action. Otherwise, defendants are expected to be increasingly reliant on other class action tools, such as class-arbitration waivers, motions for summary judgment, and defeating class certification.

2. Business-to-Business Breach Litigation: Moving Past *Target*

After the District Court of Minnesota refused to dismiss the negligence cause of action brought by financial institutions against Target arising from its data breach, many plaintiffs had high hopes for retail business-to-business data breach litigation, particularly since data breach litigation had struggled for decades before its recent resurgence.[122]

With regard to business-to-business litigation, however, litigation since *Target* has led to mixed results. Although some large retail breaches have allowed for significant recoveries by way of settlements with financial institutions, financial institutions have also lost a number of significant cases.

First, in *SELCO Comm. Credit Union v. Noodle & Co.*, the District Court of Colorado dismissed the complaint brought by credit unions as barred by the economic loss rule. Although there was no privity of contract between the credit union and the

[118] *Dolmage v. Combined Ins. Co. of America*, 2017 U.S. Dist. LEXIS 67555 (N.D. Ill. May 3, 2017) (allegations that Dillard's insurer left Dillard employee's SSN and other information on publicly available website, alleging invasion of privacy in addition to FCRA violation).
[119] *Bernardino v. Barnes & Noble Booksellers, Inc.*, 2018 U.S. Dist. LEXIS 15812 (S.D.N.Y. Jan. 31, 2018).
[120] *Henson v. United States Dist. of N. Cal. (In re Henson)*, 869 F.3d 1052 (9th Cir. Sept. 5, 2017).
[121] McCoy, *Senate Overturns New Rule Allowing Class-Action Suits Against Banks* (USA Today Oct. 25, 2017).
[122] *In re Target Corp. Customer Data Sec. Breach Litig.*, 2014 U.S. Dist. LEXIS 167802 (D. Minn. Dec. 2, 2014).

defendant, the court noted that the parties were free to negotiate "within the (PCI DSS) chain," thus evoking the economic loss rule for any claim that lay outside.[123]

Second, in *Community Bank of Trenton v. Schnuck Markets*, the Southern District Court of Illinois granted a motion to dismiss by the defendant supermarket chain, including on the claims for negligence by the credit card issuing banks. The court found that while some other courts had found a duty of care existed between the plaintiff banks and the defendants, those decisions were made assessing the state laws at issue in those cases, but not for the State of Missouri, which was at issue in *Schnuck Markets*. "In the absence of such legislation, this court declines to sua sponte create a duty where the Missouri government has declined to do so."[124]

Third, in *USAA Fed. Savings Bank v. PLS Fin. Serv.*, an intrusion affected the defendant, which processed checks deposited by USAA members. The Northern District Court of Illinois refused to find any general duty of care with regard to the securing of PII by the defendant, acknowledging that it was deviating from precedence involving large retail breaches.[125]

Nonetheless, it is important to recognize that as with consumer litigation, plaintiffs in business-to-business breach litigation have continued to obtain mixed results, some of which have also been in their favor in 2017 and in early 2018.[126]

B. DATA MISUSE LITIGATION: WHERE TECHNICALITIES MATTER

Compared to data breach cases, there is arguably greater disparity amongst data misuse cases. The cases in this section are divided into different types of "common practices":

1. Cases on Web and Online Tracking and Aggregation

- ✓ For Preinstalled Computer Programs – Although data collection through different components and software applications has been the subject of much controversy, *Krise v. SEI/Aaron's* offered some important lessons. The case alleged that SEI/Aaron's, a rent-to-own business, impermissibly used a preinstalled computer program on its rental computers to collect renters' information. The court ultimately held that defendant was entitled to summary judgment, citing to a number of defenses against the wiretap and invasion of

[123] *SELCO Cmty Credit Union v. Noodles & Co.*, 2017 U.S. Dist. LEXIS 113562, *16 (D. Colo. Jul. 21, 2017).
[124] *Cmty. Bank of Trenton v. Schnuck Mkts.*, 2017 U.S. Dist. LEXIS 66014 (S.D. Ill. May 1, 2017).
[125] *USAA Fed. Sav. Bank v. PLS Fin. Servs.*, 2017 U.S. Dist. LEXIS 82277, fn. 4 (N.D. Ill. May 30, 2017).
[126] *See, e.g., Veridian Credit Union v. Eddie Bauer*, 2017 U.S. Dist. LEXIS 186201 (W.D. Wash. Nov. 9, 2017) (denying motion to dismiss, albeit finding no special legal relationship between financial institutions and defendant); *see also CVS Pharm, Inc. v. Press Am., Inc.*, 2018 U.S. Dist. LEXIS 2282 (S.D.N.Y. Jan. 4, 2018) (denying motion to dismiss in business to business case between health care provider and its vendor).

privacy claims, including the terms and conditions that the renters signed and the technical details of the alleged spyware.[127] Notably, in the related case of *Byrd v. Aaron's*, where plaintiffs tried to certify a class involving both renters and their household members, the court held that there were too many individualized questions regarding actual use.[128]

- ✓ For Website Data and Advertisement Exchanges – In *Mount v. Pulsepoint*, plaintiffs alleged that Pulsepoint had improperly circumvented their web browser privacy preferences by placing tracking cookies on their computers. On appeal, the Second Circuit affirmed the dismissal granted by the lower court.[129] The court noted the lower court's denial of Pulsepoint's standing challenge, finding that the alleged loss of privacy was sufficient. However, the court held that there were no viable claims for invasion of privacy or violation of consumer protection laws because plaintiffs were only able to allege that Pulsepoint associated the activities it tracked to devices and browsers. Plaintiffs did not allege that there was individually identifiable information traceable to individuals.

- ✓ For Website Data and Advertisement Exchanges – In *Smith v. Facebook*, plaintiffs were Facebook users that alleged Facebook and various healthcare websites were impermissibly tracking their activities through "like" and "share" buttons, cookies, and browser fingerprinting. Plaintiffs alleged that such practices contravened defendants' privacy policies and HIPAA. On May 9, 2017, the court granted Facebook and the website defendants' motion to dismiss with prejudice.[130] The court reasoned that Facebook users had already agreed to Facebook's collection practices through third-party websites as part of Facebook's terms and conditions. The court also noted that it did not appear that Facebook was collecting HIPAA-covered sensitive information. As to the website defendants, the court noted that just because Facebook was located in California, and its buttons were imbedded on the websites, jurisdiction was not automatically conferred on the court.

- ✓ For Website Data and Advertisement Exchanges – Facebook tracks users with a wide-reaching advertisement network, which includes its own fleet of affiliate and partner sites that use the Facebook "like" and "share" buttons. While these buttons may seem simple, they are actually embedded in the affiliate and partner sites – or even on advertisement banner space – so when a user visits the affiliate webpage, the user's server actually communicates with the website server and with Facebook's server. In *In re: Facebook Internet Tracking Litigation*, plaintiffs alleged that Facebook impermissibly continued to track users after they logged off of the Facebook website. On June 30, 2017, the District

[127] *Krise v. SEI/Aaron's Inc.*, 2017 U.S. Dist. LEXIS 133818 (N.D. Ga. Aug. 22, 2017).
[128] *Byrd v. Aaron's, Inc.*, Case No. 11-101 (W.D. Penn. Sept. 26, 2017).
[129] *Mount v. PulsePoint, Inc.*, 2017 U.S.App.LEXIS 5262 (2nd Cir. Mar. 27, 2017).
[130] *Smith v. Facebook*, No. 16-01282, Dkt. No. 64 (N.D. Cal. May 9, 2017).

Court granted Facebook's motion to dismiss, permitting plaintiffs an amendment on only the two breach of contract causes of action.[131] Importantly, the court held that Facebook's use of its buttons and advertisement relationships did not violate the Wiretap Act or the Stored Communications Act because Facebook was a party to the communications. In addition, the court reiterated precedence and pointed out that there could be no viable claim for invasion of privacy when plaintiffs themselves were actively visiting the web pages, and thereby had no expectation of privacy. Although the court also dismissed the fraud cause of action for lack of actual damage, for the contract causes of action, the court cited to minority precedence and held that only "nominal damages" were required. Nonetheless, in November 2017, the contractual causes of action were dismissed because the court found that the privacy promises allegedly made did not exist at the time period at issue.[132]

- ✓ For Website Data and Advertisement Exchanges – In *Cole v. Gene by Gene*, plaintiffs alleged that the genetic testing company impermissibly shared testing information with third-party community website administrators of "projects," in violation of the Alaska Genetic Privacy Act. After previously denying motions to dismiss, the court denied plaintiffs' motion for class certification in July 2017, finding that there were individualized questions on user consent, including user agreements and privacy settings subsequently made.[133]

- ✓ For Website Data and Advertisement Exchanges – In *hiQ Labs v. LinkedIn*, aggregator hiQ Labs aggressively sought clarity on the issue of "scraping." hiQ Labs harvested and scraped user profiles and data of those who opted to share their profiles publicly. At issue was whether it was a violation of the Computer Fraud and Abuse Act (CFAA) for hiQ Labs to access and scrape information from LinkedIn's servers after LinkedIn had sent it a cease and desist letter allegedly revoking any permission it may have had to harvest the information. The court sided with hiQ Labs, noting that First Amendment rights may be implicated where the information harvested involved publicly available information.[134]

- ✓ For Online Media – One of the most dangerous statutes for website owners remains Michigan's Preservation of Personal Privacy Act (PPPA), sometimes known as the Video Rental Privacy Act. Not only does the PPPA provide for actual damages and attorneys' fees for misuse of covered media without user consent,[135] it has also proven to be one of the most difficult causes of action to

[131] *In re Facebook Internet Tracking Litig.*, 2017 U.S. Dist. LEXIS 102464 (N.D. Cal. Jun. 30, 2017).
[132] *In re Facebook Internet Tracking Litig.*, 2017 U.S. Dist. LEXIS 190819 (N.D. Cal. Nov. 17, 2017).
[133] *Cole v. Gene By Gene, Ltd.*, No. 14-0004, Dkt. No. 182 (D. Ala. Jul. 25, 2017).
[134] *hiQ Labs, Inc. v. Linkedin Corp.*, 2017 U.S. Dist. LEXIS 129088 (N.D. Cal. Aug. 14, 2017).
[135] MCLS Section 445.1715.

defeat by way of a motion to dismiss.[136] Notably, one of the largest data misuse settlements to date, which settled for over $8 million, alleged that Reader's Digest had violated the PPPA by selling its subscriber information to third parties without subscriber consent.[137]

- ✓ For Online Media – In November 2017, the Ninth Circuit took the position that it agreed with the Third Circuit's "ordinary person" standard for the purposes of determining whether information was "personally identifiable information" under the VPPA, as opposed to the First Circuit's "reasonably and foreseeably likely to reveal" standard in *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482 (1st Cir. 2016).[138] Thus, the Ninth Circuit took the position that disclosure of Roku device and video information alone were not violations of the VPPA, even if the disclosure could allow resourceful third parties to cross-reference with other information to identify the individual.[139]

2. Cases on Mobile Tracking and Aggregation

Although the mobile environment has been arguably more important than the desktop environment these past few years, there are but a handful of cases involving the alleged misuse of data through application program interfaces (APIs) and software development kits (SDKs), which are more effective for the mobile environment. How mobile application developers interact with operating system owners also tends to be different from their interactions with the desktop environment. A number of important decisions in 2016 highlight how these differences can lead to different legal problems:

- ✓ For Mobile Ecosystems – In *Opperman v. Path, Inc.*, plaintiffs alleged that while the owner of the operating system advertised the security and privacy of its devices, its partners and application developers improperly accessed end-users' personal information and private address books without consent. Plaintiffs thereby sought to hold both the owner and developers liable. While the non-owner defendants settled out, the owner was left alone to face two separate motions for class certification. In certifying the claims for intrusion upon seclusion against the main developer Path, the court similarly certified the claim for "aiding and abetting" against the ecosystem owner in 2016, although plaintiffs were left with merely "nominal" damages.[140] Plaintiffs' attempt to certify the false advertising claims against the owner was then denied in July 2017, as there was

[136] *Ruppel v. Consumers Union of United States*, No. 16-2444, 2017 U.S. Dist. LEXIS 90985 (S.D.N.Y., Jun. 12, 2017) (denying motion to dismiss based on Article III standing); *see also Perlin v. Time, Inc.*, No. 16-110635, 2017 U.S. Dist. LEXIS 21401 (E.D. Mich. Feb. 15, 2017) (denying motion to dismiss also on Article III standing).
[137] *Taylor v. Trusted Media Brands*, No. 16-1701, Dkt. No. 71 (S.D.N.Y. Jun. 8, 2017) (settling for over $8.2 million for over 1.1 million class members).
[138] *Eichenberger v. ESPN, Inc.* 2017 U.S. App. LEXIS 24168, *9 (Nov. 29, 2017).
[139] *Id* at *13-14.
[140] *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 92403 (N.D. Cal. July 15, 2016).

not enough evidence of persistent and pervasive advertising regarding user privacy, as opposed to sporadic statements.[141]

- ✓ For Mobile Videos – In April 2017, the Eleventh Circuit finally resolved the appeal of *Perry v. Cable News Network (CNN)*. Plaintiff, a cable subscriber, alleged that he had downloaded and used the CNN iOS application, which impermissibly tracked and disclosed his use to third parties, in contravention of the VPPA. The Eleventh Circuit affirmed the lower court's dismissal, and cited to *Ellis v. Cartoon Network*[142] for the proposition that plaintiff is not a "subscriber" (statutory "consumer") for the purposes of the VPPA because there was no "ongoing commitment or relationship with CNN" other than the download of the application itself.[143]

- ✓ For the Driver's Privacy Protection Act (DPPA) – The use of drivers' licenses as a means of identification in mobile technologies has become increasingly popular. As a result, there has been a recent bout of new litigation filed regarding whether such use violates the DPPA. In *Whitaker v. Appriss*, a case involving the use of police records containing drivers' license information, the court held that use of a hard copy of a driver's license is not "personal information, from a motor vehicle record" for the purposes of the DPPA.[144] The court also pointed out that where an individual provides their driver's license, there can be no violation when the information is then used and reused thereafter.[145]

3. Cases on IoT Tracking and Aggregation, and Emerging Technologies

Cases involving connected things are still very much in the early stages of litigation. With IoT, there is also greater opportunity for data collection and companies are exploring new ways to use identifiers and emerging technologies:

- ✓ For Geolocation Tracking Technologies – In *Beckman v. Niantic*, the court dismissed plaintiffs' claims notwithstanding their allegations that Pokémon Go's terms were illusory because they could be changed at any time. The court found it dispositive that plaintiffs did not suffer any actual harm from the collection of geolocation information.[146]

- ✓ For Geolocation Tracking Technologies – In *Moreno v. S.F. Bay Area Rapid Transit Dist.*, a Ninth Circuit district court dismissed without prejudice plaintiffs' claims for illegal interception and invasion of privacy, where the mobile

[141] *Opperman v. Kong, Inc.*, No. 13-453, 2017 U.S. Dist. LEXIS 116333 (N.D. Cal. Jul. 25, 2017).
[142] *Ellis v. Cartoon Network*, 803 F.3d 1251 (11th Cir. 2015).
[143] *Perry v. CNN, Inc.*, 854 F.3d 1336 (11th Cir. Apr. 27, 2017).
[144] *Whitaker v. Appriss*, Case No. 13-826 (N.D. In. Jul. 18, 2017), p. 8.
[145] *Id.*, p. 11.
[146] *Beckman v. Niantic, Inc.*, Case No. 2016CA008330 (Circuit Ct. of Palm Beach Cnty. Fla. May 1, 2017).

application tracked the geolocation of the user without allegedly sufficiently informing users of the tracking during onboarding.[147] Notably, the Court indicated that even drawing all reasonable inferences in plaintiff's favor, the anonymous tracking of location information is not "highly offensive or egregious."[148]

- ✓ For Audio Tracking Technologies – In *Satchell v. Sonic Notify,* plaintiff alleges that defendants improperly tracked them using audio technologies in conjunction with their sports applications, which resulted in defendants unlawfully intercepting and recording plaintiffs' conversations. The court granted the motion to dismiss of the Golden State Warriors' mobile application developer, YinzCam, with prejudice, noting that even the amended complaint fails to explain how the developer, as opposed to the other defendants, unlawfully intercepted and recorded messages.[149]

- ✓ For Audio Tracking Technologies – *In re Vizio, Inc., Consumer Privacy Litigation* involves a consolidated complaint alleging impermissible aggregation by Vizio through its smart television offerings. The Central District Court of California twice denied motions to dismiss, permitting broad and vague allegations on the various wiretap and unlawful interception claims.[150]

- ✓ For Facial Tracking Technologies – A number of companies have challenged whether "facial geometry" derived from photographs are covered by the Illinois Biometric Information Protection Act (BIPA), a statute that expressly exempts photographs. The courts have thus far uniformly disagreed, finding that even geometric information derived from photographs may be covered by BIPA, at least for the purposes of a challenge pursuant to a motion to dismiss.[151]

- ✓ For Facial Tracking Technologies – Until early 2018, whether BIPA required actual damages appeared to be an open question. Although the Second Circuit held that BIPA did require actual damages in *Santana v. Take-Two Interactive Software*,[152] many commentators initially believed that the Second Circuit decision is not authoritative for Illinois. In December 2017, an Illinois appellate court corroborated the Second Circuit and held that BIPA indeed requires actual

[147] *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 U.S. Dist. LEXIS 206009 (N.D. Cal. Dec. 14, 2017).
[148] *Id.*, at *19-20.
[149] *Satchell v. Sonic Notify, Inc.*, Case No. 16-04961, Dkt. 89 (N.D. Cal. Nov. 20, 2017); *but see Rackemann v. Linsr, Inc.*, No. 17-00624, 2017 U.S. Dist. LEXIS 162567 (S.D. In., Sept. 29, 2017 (finding differently in case involving Indiana Colts with different developers).
[150] *See In Re: Vizio, Consumer Privacy Litigation*, No. 16-02693, Dkt. No. 199 (C.D. Cal. Jul. 25, 2017); *see also In Re: Vizio, Consumer Privacy Litigation*, 2017 U.S. Dist. LEXIS 60780 (C.D. Cal. Mar. 2, 2017).
[151] *Monroy v. Shutterfly, Inc.*, 2017 U.S. Dist. LEXIS 149604 (N.D. Ill. Sept. 15, 2017); *Rivera v. Google, Inc.*, 2017 U.S. Dist. LEXIS 27276 (N.D. Ill. Feb. 27, 2017); *In re Facebook Biometric Info. Privacy Litig.*, 2016 U.S. Dist. LEXIS 60046 (N.D. Cal. May 5, 2016).
[152] *Santana v. Take-Two Interactive Software, Inc.*, 2017 U.S. App. LEXIS 23446 (2nd Cir. Nov. 21, 2017).

damages for any person to claim they were "aggrieved" under the statute.[153] The *Rosenbach* decision is expected to help numerous defendant companies obtain dismissals in the recent flurry of suits where they were alleged to have improperly used biometrics at the workplace.

C. PRODUCT LIABILITY LITIGATION

Privacy and security vulnerabilities in consumer goods and products have been the source of much debate these past few years, but plaintiffs have had a tough time finding good examples to make headway and create convincing precedence. Nonetheless, as the future of technology is now focused on connected home devices and autonomous vehicles, four 2017 decisions are particularly noteworthy.

First, in *FTC v. D-Link Systems*, the court showed skepticism regarding whether the FTC had standing under Article 5 of the Federal Trade Commission Act for "unfair practices" against the manufacturer for alleged cyber vulnerabilities in its connected home cameras. The court noted that under Article 5, the FTC must allege actual substantial harm to consumers, and the FTC failed to so do. Thus, the unfairness claims were dismissed with leave to amend. On the other hand, the court hinted that the FTC might be able to better plead their fraud claims on amendment, and potentially use that to amend its other claims as well.[154]

Second, in *Jungens v. Build.com*, the Eastern District Court of Missouri held that defendant's' transmission of credit card information to undisclosed third parties did not constitute a wiretap violation because the defendant was a party.[155] Perhaps more importantly, the court also noted that the fact that JavaScript may allow third-party advertisers to intercept certain payment data and other information was not sufficient for the purposes of plaintiff's unjust enrichment claim because the plaintiff failed to allege that "any specific portion of the money she paid was intended or required to be spent on data protection."[156]

Third, in *Flynn v. FCA US LLC (Fiat)*, plaintiffs alleged that the automobile manufacturer should be liable for cyber vulnerabilities in its connected cars. Although Fiat argued that no vehicles of plaintiffs had actually been hacked, the court denied the manufacturer's motion to dismiss for lack of Article lll standing, finding that the plaintiffs sufficiently alleged that they overpaid for their vehicles, which may be a viable theory. On the other hand, the court also held that the economic loss rule applied to bar most of the plaintiffs' claims, leaving essentially unjust enrichment claims.[157]

---

[153] *Rosenbach v. Six Flags Entm't Corp*, 2017 Ill. App. LEXIS 812 (Dec. 21, 2017).
[154] *FTC v. D-Link Sys.*, 2017 U.S. Dist. LEXIS 152319 (N.D. Cal. Sept. 19, 2017).
[155] *Jurgens v. Build.com, Inc.*, 2017 U.S. Dist. LEXIS 186999, *13 (E.D. of Mo. Nov. 13, 2017).
[156] *Id.* at *17-18.
[157] *Flynn v. FCA US LLC dba Chrysler Group LLC*, Case No. 15-0855 (S.D. Ill. Aug. 21, 2017).

Fourth, in contrast to *Flynn*, the Ninth Circuit affirmed the lower district court's refusal in *Cahen v. Toyota Motor Corp* to allow a case alleging cyber vulnerability against Toyota to proceed beyond the pleadings stage. In particular, as to plaintiffs' unjust enrichment theory, the court noted, "plaintiffs have only made conclusory allegations that their cars are worth less and have not alleged sufficient facts to establish Article III standing."[158] The stark contrast between *Cahen* and *Flynn* demonstrates the continued division amongst circuits and lower courts in privacy litigation, even between two circuits traditionally regarded as relatively "plaintiff friendly."

D. LESSONS LEARNED

As the cases of 2017 demonstrate, it is increasingly important for data privacy professionals to have a deep appreciation for the workings and intricacies of technology. Although privacy law in the United States has traditionally been sectoral, courts are beginning to discuss privacy expectations as if fundamental rights are implicated. Surveying the legal landscape, organizations engaged in e-commerce and mobile advertising should be aware of a number of important recent trends:

First, courts are increasingly assessing the entirety of user ecosystems as part of a claim and not just individual sites and applications. Some plaintiffs have convinced courts to assess consumers' expectations across the *entire user ecosystem*, which can include defendants' advertising partners and network affiliates. This is particularly problematic for platform owners, as it is impossible for them to police their third-party developers to ensure total compliance with platform rules and policies. For example, when developers provide only limited disclosures regarding the workings of their technology, they may be trying to legitimately protect their own proprietary information.

Second, organizations should require that their advertisers disclose all "piggybacking" third parties. When an organization allows third-party "affiliates" to use its website or mobile application to advertise, the third parties may then allow others to "piggyback" and also advertise in the same space. Although these other parties are not in contractual privity with the owner, they may nonetheless be able to track and target the owner's users. For example, organizations integrating third-party SDKs into their websites and mobile applications should carefully consider what data is being shared through the SDKs. As they are directly integrated into the websites and applications, SDKs can be even more invasive than third-party advertisers using banner space. As with third-party cookies, proper disclosure and consent remain the best defense against privacy violation claims for the use of SDKs.

Third, strong defenses require more foresight and anticipation. The current legal landscape for privacy misuse cases proves the importance of careful technical planning in addition to legal planning in an evolving area of law. At a minimum, organizations

[158] *Cahen v. General Motors LLC*, 2017 U.S. App. LEXIS 26261, *4 (9th Cir. Dec. 21, 2017).

need to take into consideration how disclosures and consent work throughout the user ecosystem and not just where the user interfaces with their product. Organizations need to do a better job of strong data classification and mapping (internally and externally as to their partners) as well as assessing the business practices of their business partners and vendors, instead of simply relying on what they are told. For example, in an environment where motions to dismiss are less likely to be granted, creating a record of the consent process throughout the ecosystem may help organizations defeat class certification. A well-crafted user interface that tactfully obtains consent throughout the process should help organizations create a better record of individualized experiences and of how different sets of data were actually collected and used. And, in other cases, an agreement might include class arbitration waivers and other terms that allow the application of the economic loss rule, which altogether bar most, if not all, of the claims brought by eager plaintiffs.

IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

Perhaps due in part to the international environment on privacy law, regulators are taking aggressive stances on privacy practices, many of which have been responsible for the technological growth in the United States these past two decades. From expanding the definition of "personal information," to prohibiting certain types of third-party behavioral advertising, regulators are increasingly cracking down on business practices that have been around since the birth of the world wide web.

A. The Federal Trade Commission

The FTC remains the most active cop on the privacy block. This is especially true with the FCC recently announcing its withdrawal from privacy enforcement in broadband, ceding the authority to the FTC.

In 2017, the FTC took action on a number of noteworthy matters:

- *In re Vizio*: In February 2017, Vizio agreed to pay $2.2 million to the FTC for allegedly collecting the viewing histories of 11 million smart televisions without the end-users' consent.[159] As part of the consent decree, Vizio was required to delete data previously collected, prominently disclose and obtain affirmative express consent, implement a comprehensive data privacy program, and participate in biennial assessments. In a concurring opinion that read almost like a dissenting opinion, new Trump-appointee and Acting FTC Chairman Maureen Ohlhausen indicated that "under our statute (the FTC Act), we cannot find a

[159] FTC Press Release, *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories On 11 Million Smart Televisions Without Users' Consent* (FTC Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

practice unfair based primarily on public policy. Instead, we must determine whether the practice causes substantial injury."[160]

- *In re Sentinel Labs; In re SpyChatter; In re Vir2us*: In February 2017, the FTC settled with three U.S. companies that allegedly deceived consumers about their participation in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) program.[161]

- *In re Turn*: In April 2017, the FTC settled its allegations against Turn, Inc., which enables online sellers to target digital advertisements to consumers. The consent decree bars Turn from "misrepresenting the extent of its online tracking or the ability of users to limit or control the company's use of their data." Turn is also required to provide a more effective opt-out for consumers.[162]

- *In re Blue Global*: In July 2017, the FTC entered into a $104 million settlement with Blue Global, a loan lead generator, over allegations that the company induced customers to fill out online applications for loans and then sold the PI to "virtually anyone."[163] The FTC charged that, in reality, defendants sold very few loan applications to lenders, and instead sold the applications to the first buyer willing to pay for them.[164]

- *In re TaxSlayer*: In August 2017, the FTC settled its allegations against the online tax preparation service for exposing the personal financial information of approximately 9,000 account users.[165]

[160] Allison Grande, *FTC's Smart-TV Privacy Settlement Unlikely to See an Encore*, LAW360 (Feb. 7, 2017), https://www.law360.com/articles/889449.
[161] FTC Press Release, *Three Companies Settle FTC Charges That They Deceived Consumers about Participation in International Privacy Program* (Feb. 22, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/three-companies-settle-ftc-charges-they-deceived-consumers-about
[162] FTC Press Release, *FTC Approves Final Consent Order with Online Company Charged with Deceptively Tracking Consumers Online and Through Mobile Devices* (Apr. 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-consent-order-online-company-charged.
[163] FTC Press Release, *FTC Halts Operation That Unlawfully Shared and Sold Consumers' Sensitive Data* (Jul. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/ftc-halts-operation-unlawfully-shared-sold-consumers-sensitive.
[164] Gorta, *Payday Loan Lead Generator Pays $104M to End FTC Suit* (Law360, Jul. 5, 2017), https://www.law360.com/articles/941303/payday-loan-lead-generator-pays-104m-to-end-ftc-suit.
[165] FTC Press Release, *Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That It Violated Financial Privacy and Security Rules* (Aug. 29, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges.

- *In re Decusoft; In re Tru Communication; In re Md7*: In September 2017, the FTC settled with three U.S. companies that allegedly deceived consumers about their participation in the EU-U.S. Privacy Shield Framework.[166]

- *In re VTech*: In January 2018, the FTC entered into a $650,000 deal with toymaker VTech for allegedly collecting personal information from hundreds of thousands of children without providing direct notice and obtaining their parents' consent, and for allegedly failing to take reasonable steps to secure the data.[167]

- *In re Prime Sites*: In February 2018, the FTC entered into a $235,000 settlement with an online talent search company, for allegedly collecting and disseminating children's personal information without the proper parental consent. The FTC noted that the respondent falsely represented in its website terms that it was not knowingly collecting the information of children under the age of 13, and that the site falsely claimed that certain casting directors were interested in participants.[168]

Notably, it is unclear which of the FTC's statements and policies promulgated by the Obama Administration will survive under the Trump Administration. The latter is likely to require the FTC take action only where there is demonstrable harm, as opposed to "risk of harm."[169] Indeed, Acting Chairman Maureen Ohlhausen has commented that the FTC should focus on cases where there is "substantial consumer injury," including cases where there are allegations of "informational injury."[170]

Perhaps to avoid the criticism that the new administration is not doing enough to secure the privacy and cybersecurity of consumers, the FTC recently took a number of actions against large and successful corporations.[171]

---

[166] FTC Press Release, *Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation In EU-US Privacy Shield Framework* (Sept. 8, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed.

[167] FTC Press Release, *Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act* (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

[168] FTC Press Release, *Online Talent Search Company Settles FTC Allegations IT Collected Children's Information Without Consent And Misled Consumers* (Feb. 5, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/online-talent-search-company-settles-allegations-it-collected.

[169] Wendy Davis, *Ohlhausen Outlines Privacy Approach, Focus On "Concrete" Harms,* MediaPostPolicyBlog (Feb. 2, 2017) (reporting on Ohlhausen's comments before the American Bar Association), http://www.mediapost.com/publications/article/294365/ohlhausen-outlines-privacy-approach-focus-on-con.html.

[170] Koenig, *FTC Chief Says Real Consumer Harms Must Guide Cases* (Law360, Sept. 19, 2017), https://www.law360.com/articles/965388/ftc-chief-says-real-consumer-harms-must-guide-cases.

[171] *See, e.g.*, Crosby, *Lenovo Pays $3.5M to End FTC's Adware Dispute* (Law360, Sept. 5, 2017) (on third party software), https://www.law360.com/articles/960518/lenovo-pays-3-5m-to-end-ftc-s-adware-dispute; *see also*, FTC Press Release, *Uber Settles FTC Allegations That It Made Deceptive Privacy And Data Security Claims* (Aug. 15, 2017) (on alleged employee practices), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

B. HIPAA Enforcement

In 2017, the Office of Civil Rights (OCR) and Department of Health and Human Services (HHS) continued to aggressively pursue covered entities. Noteworthy enforcement actions included:

- MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) – Fined $2.2 million for the loss of a USB data storage device in 2011, which was allegedly followed by additional failures to implement corrective measures as promised.[172]

- Children's Medical Center of Dallas – Fined $3.2 million for allegedly failing to secure electronic health records until after an unencrypted laptop with information about approximately 2,500 patients was stolen from its building. The deficiencies were contrary to the OCR's prior recommendations to implement controls and encrypt data.[173]

- St. Joseph Medical Center of Illinois – Fined $475,000 for allegedly failing to timely notify more than 800 of its patients of a data breach.[174]

- Memorial Healthcare Systems – Fined $5.5 million[175] for allegedly failing to properly segregate and safeguard information amongst affiliates through an organized health care arrangement. The improper access by affiliates eventually led to federal charges relating to the selling of that information and filing of tax returns for some of the 106,000 or so patient records at issue.[176]

- Metro Community Provider Network – A federally-qualified health center agreed to pay $400,000 for failing to implement a security management process to safeguard ePHI.[177]

- The Center for Children's Digestive Health – A small, for-profit pediatric clinic

---

[172] Press Release, *HIPAA Settlement Demonstrates Importance of Implementing Safeguards For ePHI* (Jan. 18, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/MAPFRE.
[173] John Kennedy, *Texas Hospital Fined $3.2M For Losing Unprotected Devices*, LAW360 (Feb. 1, 2017), https://www.law360.com/articles/887365/texas-hospital-fined-3-2m-for-losing-unprotected-devices.
[174] Diana Novak Jones, *HHS, Ill. Hospital Network Settle Data Breach Action*, LAW360 (Jan. 10, 2017), https://www.law360.com/articles/879391/hhs-ill-hospital-network-settle-data-breach-action.
[175] At $5.5 million, this matched the other largest HIPAA settlement in history involving the Illinois Advocate Health Care Network in 2016. *See*: https://www.law360.com/articles/825148/ill-hospital-chain-inks-record-5-5m-hipaa-deal.
[176] Kass, *$5.5M HIPAA Deal Matches Biggest Privacy Payout*, Law360 (Feb. 16, 2017), https://www.law360.com/articles/893172.
[177] Press Release, *Overlooking Risks Leads to Breach, $400,000* (Apr. 12, 2017), https://www.hhs.gov/about/news/2017/04/12/overlooking-risks-leads-to-breach-settlement.html.

was fined $31,000 for not having a business associate agreement.[178]

- CardioNet – A wireless health services provider paid $2.5 million for allegedly failing to secure ePHI for its mobile device services. The deal is the first time the OCR reached a settlement with a wireless services provider.[179]

- St. Luke's Roosevelt Hospital Center – Paid $387,200 for allegedly impermissibly disclosing a complainant's sensitive PHI to the complainant's employer.[180]

- 21st Century Oncology – Agreed to an additional $2.3 million in bankruptcy, from insurance proceeds, to the HHS for a 2015 data breach involving the patient information of 2.2 million people.[181]

- Fresenius Medical Care – Agreed to pay $3.5 million for five data breaches at five of its locations in 2012.[182]

- Filefax – Despite closing doors, Filefax agreed to pay $100,000 to the HHS for impermissibly disclosing the personal health information of 2,150 individuals by leaving the information in an unlocked truck in the parking lot.[183]

C. Other Administrative Enforcement Efforts

In addition to the FTC and the OCR/HHS, a number of other regulators are increasing their efforts in the data privacy arena. For example, in addition to issuing guidance on securing connected medical devices, the FDA recently took action on St. Jude pacemakers to ensure patients were checking in with their doctors for firmware updates, thereby making them less vulnerable to hacking.[184]

Similarly, the Financial Industry Regulatory Authority (FINRA), as a semi-governmental and self-regulatory organization, has become very aggressive with regard

[178] Press Release, *No Business Associate Agreement? $31k Mistake* (Apr. 20, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html.
[179] Kass, *Wireless Health Co. Strikes $2.5M HIPAA Deal*, Law360 (Apr. 24, 2017), https://www.law360.com/articles/916476/wireless-health-co-strikes-2-5m-hipaa-deal.
[180] Press Release, *Careless Handling of HIV Information Jeopardizes Patient's Privacy, Costs Entity $387k* (May 23, 20017), https://www.hhs.gov/about/news/2017/05/23/careless-handling-hiv-information-costs-entity.html.
[181] Press Release, *Failure to Protect Health Records of Millions of Persons Cost Entity Millions of Dollars* (Dec. 28, 2017), https://www.hhs.gov/about/news/2017/12/28/failure-to-protect-the-health-records-of-millions-of-persons-costs-entity-millions-of-dollars.html.
[182] Press Release, *Five Breaches Add Up to Millions In Settlement Costs For Entity That Failed to Heed HIPAA's Risk Analysis And Risk Management Rules* (Feb. 1, 2018), https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.
[183] Press Release, *Consequences For HIPAA Violations Don't Stop When a Business Closes* (Feb. 13, 2018).
[184] Field, *FDA Announces Security Update for St. Jude Pacemakers* (Law360, Aug. 30, 2017), https://www.law360.com/articles/959128/fda-announces-security-update-for-st-jude-pacemakers.

to its enforcement efforts. In 2017, FINRA issued three orders to its broker-dealer members with significant fines near or exceeding $1 million,[185] with more apparently to come.

State regulators are no less active than the federal regulators. Like the FTC, state AGs have been particularly aggressive with regard to online privacy practices:

- In January 2017, the New York Attorney General entered into a settlement agreement for $115,000 with Acer for a debugging-mode vulnerability on its company website, which left customer PI vulnerable.[186]

- In February 2017, the New Jersey Division of Consumer Affairs entered into a $1.1 million settlement with Horizon Blue Cross/Blue Shield of New Jersey for its failure to secure the information of more than 690,000 insureds due to lost laptops, which were password protected but not encrypted as required by HIPAA.[187]

- In February and March 2017, the New York Attorney General entered into settlement agreements with five separate mobile developers, requiring that they pay small penalties in addition to providing better disclosure of their terms and privacy practices.[188]

- In April 2017, the Massachusetts Attorney General entered into a settlement agreement with Copley Advertising, which provided real-time advertising intelligence by using geo-fencing. The AG had alleged that the geo-fencing practice, which in this instance was around reproductive clinics, violated consumer protection laws. The respondent had contested the allegations.[189]

---

[185] Crosby, *FINRA Fines State Street, Acorns $2M Over Record Keeping* (Law360, Jul. 12, 2017), https://www.law360.com/articles/943723/finra-fines-state-street-acorns-2m-over-record-keeping; Mannion, *FINRA Fines HSBC, Others $2.4M In Customer Records Row* (Law360, Jul. 5, 2017), https://www.law360.com/articles/941232/finra-fines-hsbc-others-2-4m-in-customer-records-row.

[186] Melissa Daniels, *Acer Settles with NY AG For $115k After Data Breach*, LAW360 (Jan. 26, 2017), https://www.law360.com/articles/885253/acer-settles-with-ny-ag-for-115k-after-data-breach.

[187] O'Sullivan, *Horizon, NJ Reach $1.1M Settlement over Privacy Lapse*, Law360 (Feb. 17, 2017), https://www.law360.com/articles/893419/horizon-nj-reach-1-1m-settlement-over-privacy-lapse-.

[188] Press Release, *A.G. Schneiderman Announces Settlements with Mobile App Developers for Failure to Disclose Data Collection Practices* (Feb. 9, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-mobile-app-developers-failure-disclose-data; Grande, *Heart Apps Revise Ad, Privacy Practices in Deal with NY AG* (Law360 Mar. 24, 2017), https://www.law360.com/articles/905950/heart-apps-revise-ad-privacy-practices-in-deal-with-ny-ag.

[189] Press Release, *A.G. Reaches Settlement with Advertising Company Prohibiting "Geofencing" Around Massachusetts Healthcare Facilities* (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

- In April 2017, the New York Attorney General settled with TRUSTe for $100,000. TRUSTe had provided an FTC COPPA certification program, but the AG alleged that TRUSTe failed to properly conduct privacy assessments.[190]

- In May 2017, the New York Attorney General and Safetech Products entered into a settlement whereby the connecting doors and padlocks manufacturer agreed to better use encryption and secure its wireless communications. The AG had alleged that the company did not use encryption in its transmissions and its password protocols were poor.[191]

- In May 2017, Target paid $18.5 million to 47 states and the District of Columbia to settle the states' attorneys general probe over the 2013 breach.[192]

- In June 2017, the New York Attorney General and CoPilot Provider Support Services agreed to $130,000 in penalties. The AG alleged that the company had waited more than a year to notify over 220,000 patients of a potential data event.[193]

- In August 2017, Nationwide Mutual Insurance agreed to pay $5.5 million to 32 state attorneys general for the 2012 data breach that potentially affected 1.27 million people.[194]

- In October 2017, tech vendor SAManagement agreed to pay $264,000 to Vermont to settle claims that it failed to secure 660 social security numbers associated with the state's health-care exchange, Vermont Health Connect. SAManagement had acted as a subcontractor for support services.[195]

---

[190] Carson, *New York AG Settles with TRUSTe Over COPPA Safe Harbor Program* (IAPP Apr. 6, 2017), https://iapp.org/news/a/new-york-ag-settles-with-truste-over-coppa-safe-harbor-program/.
[191] Press Release, *A.G. Schneiderman Announces Settlement with Tech Company Over Sale of Insecure Bluetooth Doors and Padlocks* (May 22, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-tech-company-over-sale-insecure-bluetooth-door.
[192] Trader, *Target Pays $18.5M to Settle States' Probe Over 2013 Breach* (May 23, 2017), https://www.law360.com/articles/927369/target-pays-18-5m-to-settle-states-probe-over-2013-breach.
[193] Arndt, *CoPilot Reaches Settlement for Delaying Data Breach Notification* (Modern Healthcare, June 15, 2017), available at: http://www.modernhealthcare.com/article/20170615/NEWS/170619934.
[194] Salvatore, *Nationwide Pays $5.5M to AGs Over Data Breach* (Law360, Aug. 9, 2017), https://www.law360.com/articles/952737/nationwide-pays-5-5m-to-ags-over-data-breach.
[195] Stoller, *Vt. Reaches Health-Care Exchange Vendor Data Security Settlement* (Bloomberg BNA Sept. 29, 2017), https://www.bna.com/vt-reaches-healthcare-n73014470344/.

- In November 2017, the New York Attorney General and Hilton agreed to a $700,000 settlement for data security incidents exposing over 350,000 credit card numbers in two separate breaches in 2015.[196]

- In November 2017, Cottage Health agreed to pay $2 million for allegedly failing to secure the private information of more than 50,000 patients from 2011 through 2013, in two separate data breaches.[197]

- In November 2017, the Massachusetts Attorney General reached a settlement agreement that included payment of $100,000, with a Medicaid processing company that processed bills for schools all over New England for a lost laptop containing information regarding more than 2,600 Massachusetts children.[198]

- In January 2018, the New York Attorney General and a healthcare provider entered into a $1.15 million deal to end an investigation alleging it risked revealing the HIV status of 2,460 New Yorkers by mailing them information in transparent window envelopes.[199]

Looking at the state attorneys general landscape, it is important to note that the State of New York has been much more active with public enforcement actions than other states. This has not always been the case. Organizations doing business in active states need to take heed.

V. NOTABLE INTERNATIONAL DEVELOPMENTS

Although many of the transcontinental data transfer issues can be dealt with by data and network segregation, international organizations are not always able to do so easily. In such an environment, it is still important for organizations to keep apprised of international developments that will likely affect them.

A. *Schrems* 2.0 and the Future of EU-U.S. Data Flows

Thousands of applicants have now come to rely on the EU-U.S. Privacy Shield Program, as a means of demonstrating "adequate safeguards" to protect the personal

[196] Press Release, *A.G. Schneiderman Announces $700,000 Joint Settlement With Hilton After Data Breach Exposed Hundreds of Thousands of Credit Card Numbers* (Oct. 31, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed.
[197] Vogt, *Cottage Health Pays Calif. $2M to Settle Data Breach Suit* (Law360, Nov. 27, 2017), https://www.law360.com/articles/988045/cottage-health-pays-calif-2m-to-settle-data-breach-suit.
[198] Powell, *Mass. AG, Medicaid Billing Co. Reach Deal Over Data Breach* (Law360 Dec. 1, 2017), https://www.law360.com/articles/989475/mass-ag-medicaid-billing-co-reach-deal-over-data-breach.
[199] Press Release, *A.G. Schneiderman Announces Settlement Over Privacy Breach of New Yorker Members' HIV Status* (Jan. 23, 2018), https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-aetna-over-privacy-breach-new-york-members-hiv.

information of European data subjects. Although the program successfully passed its first-year review by the European regulators,[200] numerous suggestions were made,[201] which leaves the details of the program in somewhat of a limbo. It is unclear what the Department of Commerce and FTC will do in response, especially with cyber espionage being a hot topic with the Trump Administration.

Indeed, European authorities have been pushing for the program to be "temporary." EU Data Protection Supervisor Giovanni Buttarelli stated "[i]n my view it's an interim instrument for the short term. Something more robust needs to be conceived…We should work in two tracks."[202]

There are other signs as well. In scrutinizing the EU-Canada airline passenger data-sharing pact, for example, in Fall 2017, the Court of Justice for the European Union (CJEU) scrutinized Canada's pact step by step, focusing on the EU principles of necessity, proportionality, and retention. The scrutiny was more strict and narrow, and departed from language such as "adequacy."[203]

Then in December 2017, the Article 29 Working Party updated its guidance on corporate data transfer rules, specifically for Binding Corporate Rules.[204] The European Commission also announced that it would be conducting a review of all foreign data transfer deals,[205] signaling that it was facing increasing pressure to bring all foreign countries in line with the stricter GDPR rules.

However, even if the Privacy Shield needs to be overhauled, organizations currently do not have better alternatives. The advocacy group of Max Schrems has challenged the adequacy of EU Standard Model Clauses as a transfer mechanism, and the precedence allowing for them. The Irish High Court referred the matter to the CJEU for review, indicating concurrently that "there are well founded grounds for believing that

---

[200] Press Release, *EU-U.S. Privacy Shield: First Review Shows It Works But Implementation Can Be Improved* (European Commission Oct. 18, 2017), http://europa.eu/rapid/press-release_IP-17-3966_en.htm; see also Grande, *EU Privacy Shield Gets Good Marks, For Now* (Law 360, Oct. 19, 2017), https://www.law360.com/articles/975630/eu-privacy-shield-gets-good-marks-for-now.

[201] *Id.*; Angle, *EU Privacy Regulator Group's First Annual Privacy Shield Report – Ensuring a Future for the EU-U.S. Data Transfer Regime* (Bloomberg BNA, Jan. 22, 2018), https://biglawbusiness.com/eu-privacy-regulator-groups-first-annual-privacy-shield-report-ensuring-a-future-for-the-eu-u-s-data-transfer-regime/.

[202] Stupp, *EU Privacy Watchdog: Privacy Shield Should Be Temporary* (Euractiv.com, Aug. 2, 2017), https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/.

[203] Lynch, *EU Court Ruling May Signal Problems For Data Privacy Shield* (Bloomberg BNA, Aug. 21, 2017), https://www.bna.com/eu-court-ruling-n73014463158/.

[204] Lynch, *EU Privacy Chiefs Release Corporate Data Transfer Rules Update* (Bloomberg BNA, Dec. 6, 2017), https://www.bna.com/eu-privacy-chiefs-n73014472873/.

[205] *Commission Conducting Review of All Foreign Data Transfer Deals* (Euractiv.com, Nov. 8, 2017), https://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/.

the SCC decisions are invalid…"[206] Although the case was not allowed to proceed as a class action,[207] Schrems has indicated that he intends to continue pushing the case.[208]

B. The Revised Draft ePrivacy Regulation

While the Global Data Privacy Regulation (GDPR) has received substantial press, drafts of the complementary ePrivacy Regulation has received far less attention. It would be a grave mistake for any organization with substantial e-commerce activities to not pay attention to these developments.

A proposed draft of EU's ePrivacy Regulation (the "ePrivacy Reg") was released in January 2017, demonstrating how the EU will take on emerging connective technologies with a perspective dramatically different from the U.S.[209] The initial draft was updated in September 2017.[210]

Intended to supplement the GDPR and repeal Directive 2002/58/EC generally, the ePrivacy Reg will have significant consequences for device manufacturers and software developers in IoT, autonomous cars, and augmented reality. In particular, the ePrivacy Reg:

- *Provides general limits on the use and storage of "electronic data"*: Article 5 states that "[e]lectronic communications data shall be confidential." Articles 6 and 7 keep tight control of the processing of "electronic communications metadata" and "electronic communications content," limiting their storage and specifying erasure and anonymization obligations absent the data subject's express opt-in and consent. Even where there is consent, the processing typically still needs to be "necessary" for the purposes of fulfilling the data subject's request. Notably, there are tighter restrictions on the processing of "content" as opposed to "metadata."

- *Limits end-user data collection through "terminal equipment":* Article 8 prohibits data collection through terminal equipment absent a permissible use and mandates disclosures when connectivity is for more than just connectivity.

---

[206] Kelleher, *Standard Contractual Clauses to Be Reviewed By CJEU* (IAPP Oct. 3, 2017), https://iapp.org/news/a/standard-contractual-clauses-to-be-reviewed-by-cjeu/.
[207] Grande, *EU High Court Axes Class Claims In Facebook Privacy Row* (Law360, Jan. 25, 2018), https://www.law360.com/articles/1005556/eu-high-court-axes-class-claims-in-facebook-privacy-row.
[208] *Id.*
[209] Proposal For a Regulation of the European Parliament And of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, 2017/0003(COD), https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-10-F1-EN-MAIN-PART-1.PDF
[210] https://iapp.org/media/pdf/resource_center/Council-EU-proposed-ePrivReg-Sept2017.pdf.

Pursuant to the definitions found in Annex B, "terminal equipment" appears to cover all types of connected things.

- *Specifies software privacy settings:* Article 10 requires that "software placed on the market permitting electronic communications" include "the option to prevent any other parties than the end-user from storing information on the terminal equipment of an end-user or processing information already stored on that equipment." It also requires that [u]pon installation or first usage, the software…shall inform the end-user about the privacy setting options and, to continue with the installation or usage, require the end-user to consent to a privacy setting.[211]

Notably, the provisions provide that the specified settings on terminal equipment shall apply to "terminal equipment placed on the market," and therefore would apply extra-territorially. On the other hand, Article 10 limits the requirement to the import and retail phase, without specific obligations to keep supporting the device and its software once it has been sold.[212]

Many commerce-minded critics point out that the ePrivacy Reg is not IoT-development friendly because it requires affirmative consent after disclosure in an environment where "operators don't always know how the data will be used until after the fact." Furthermore, critics note that the "centralized" consent model envisioned for IoT is jnot currently possible, with there being an unmanageable plethora of do-not-track signals, without anyone to unite them all.[213] Indeed, some have noted that the new proposed regulations may not allow smart phones to be "smart" altogether.[214]

C. China's "Network Security Law" – One Year Later

On November 7, 2016, China enacted its Cybersecurity Law, which became effective on June 1, 2017. Within it, a "Network Information Security" section sets forth requirements for the protection of the personal information of Chinese data subjects, in a framework that was supposed to be similar to the GDPR:

- Under Article 40, network operators must "establish and complete user information protection systems."

---

[211] *Id.*
[212] Jeroen Terstegge, *The EU's Privacy By Default 2.0*, Privacy Tracker (Jan. 6, 2017), https://iapp.org/news/a/the-eus-privacy-by-default-2-0/.
[213] Sachin Kothari, *The ePrivacy Regulation: It's Not Just About Cookies Anymore*, Privacy Tracker (Feb. 2, 2017), https://iapp.org/news/a/its-not-just-about-cookies-anymore/.
[214] Harting, *The Flaws of ePrivacy: Will Phones Still Be Allowed to Be Smart* (IAPP, Oct. 23, 2017), https://iapp.org/news/a/the-flaws-of-eprivacy-will-phones-still-be-allowed-to-be-smart/.

- Under Article 41, network operators "collecting and using personal information shall abide by principles of legality, propriety and necessity, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consent of the person whose data is gathered."

- Under Article 42, network operators "must not disclose, distort or damage personal information they collect, with the agreement of the person whose information is collected, personal information may not be provided to others." Under Article 43, individuals have the right to request correction.

- Under Article 43, network operators must honor deletion of information where an individual discovers violations of the provisions of law in the collection or use of their personal information.[215]

Nearly one year after the passage of China's Cybersecurity Law, American predictions that the law was to be used primarily for political purposes and protectionism have thus far proven to be mostly true. Reports indicate that since the law took effect, over 40% of the enforcement actions were to remove "politically harmful contents," and less than three percent were for protecting the "rights and interests" of the "internet user."[216]

On the other hand, the central government has begun to make appearances as if it would take enforcement actions against some of China's largest companies as well[217] – although what will ultimately be done remains to be seen.

[215] Jason Meng and Wei Fan, *China Strengthens Its Data Protection Legislation*, Privacy Bar Section (Nov. 15, 2016), https://iapp.org/news/a/china-strengthens-its-data-protection-legislation/.
[216] Zhao, *An Update on China's Cybersecurity Law, 3 Months In* (Law360 Sept. 8, 2017), https://www.law360.com/articles/960697/an-update-on-china-s-cybersecurity-law-3-months-in.
[217] Ramli, *China Scolds Baidu, Ant for Alleged User Privacy Violations, Privacy & Security Law Report* (Bloomberg BNA, Jan. 22, 2018), no longer available online.