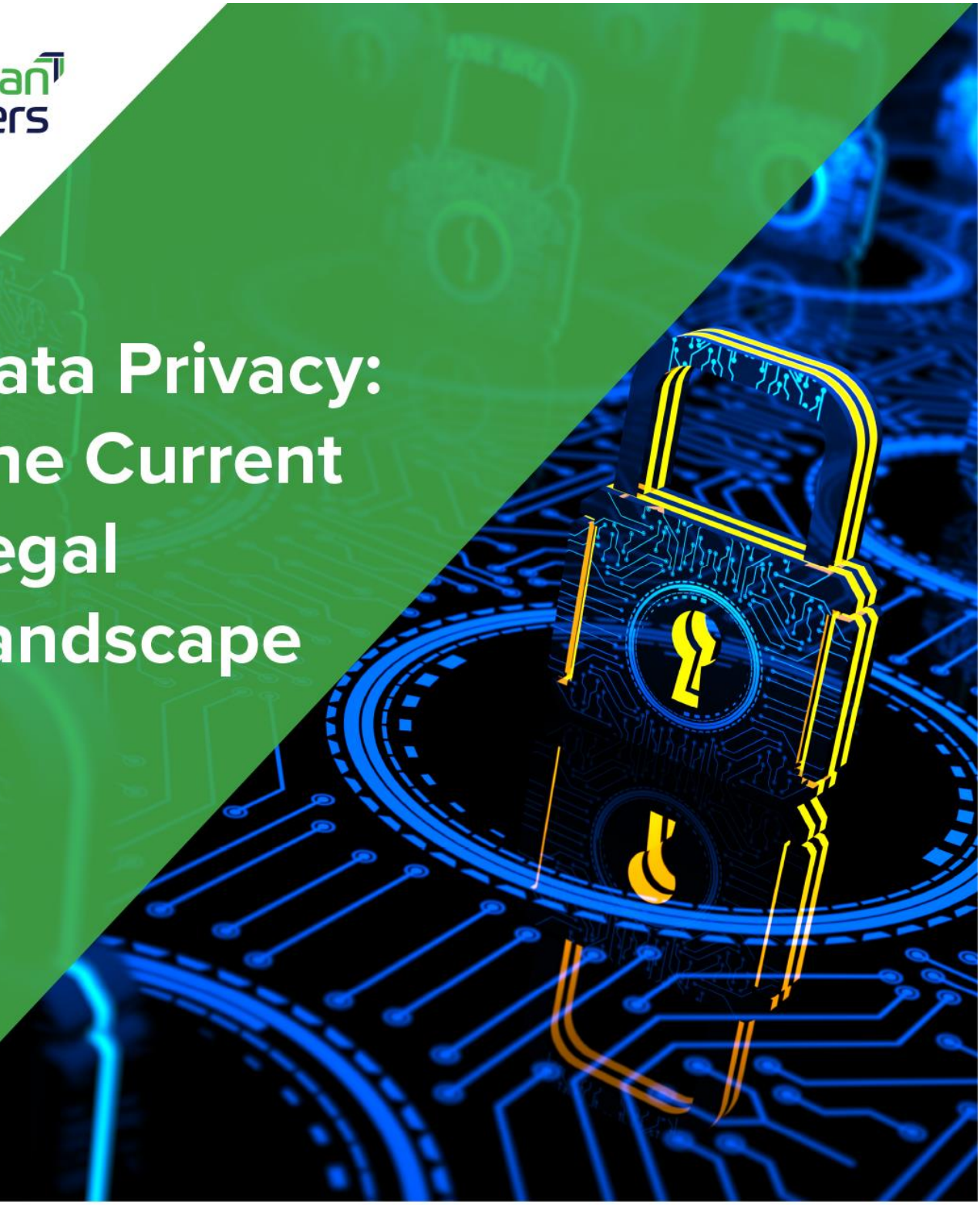
troutman sanders

Data Privacy: The Current Legal Landscape



By:
Mark C. Mao
Ronald I. Raether, Jr.
Sheila M. Pham
Megan Nicholls
Yanni Lin
Melanie Witte
Molly DiRago
Jonathan Yee
Julia Hoffmann

Mid-Year Update • October 2017

DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE

(Mid-Year Update, Ver. 1.1, October 11, 2017)

By Mark C. Mao, Ronald I. Raether, Jr., Sheila M. Pham, Megan Nicholls, Yanni Lin, Melanie Witte, Molly DiRago, Jonathan Yee, and Julia Hoffmann

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

2. Cases on Mobile Tracking and Aggregation
   - ✓ For Mobile Ecosystems
   - ✓ For Mobile Videos
   - ✓ For Use of Drivers' Licenses

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

C. Product Liability Litigation

D. Lessons Learned

IV. Developments in Regulatory Enforcement

A. The Federal Trade Commission

B. HIPAA Enforcement

C. Other 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, user privacy has been the rage in the United States. Although not nearly as draconian as the views in Europe, some consumers have taken issue with data collection as intrusive and offensive.

However, what many 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 make AR plausible and automation possible.

Similarly, AR is heavily dependent on data quality. The drive for real-time location data is a perfect example of the hunger of the AR industry for higher-quality data. To make AR plausible, the "virtual reality" mixed in as a visual overlay must be tailored to the user experience.

Companies such as Niantic, Snapchat, Instagram, and Facebook all implement some form of geo-tagging, which allows users to designate a geographical location in relation to a photo, filter, object – and even a Pokémon. On the social media side, social media platforms such as Snapchat allow users to place augmented reality objects and frames into their chats and create geofilters showing where the user is and what the user is doing.

While these features allow users to feel more connected to each other and their environment, they similarly allow companies and advertisers to gain further valuable insight into individuals and their tendencies. Location data, which once told companies an individual's particular location, is now enriched with the addition of knowing what users are doing, how the location is relevant to the user, and what the user is feeling at the location.

The overlay of augmented reality provides a new level of advertising options for companies, whereby companies can leverage the knowledge of user behavior coupled with user locations. Companies can create geo-fences, which are virtual boundaries within which certain responses are triggered, and populate advertising augmented reality filters or objects when users enter the geo-fenced area. For example, if a user created a geofilter in Snapchat of a wedding at a certain location, a nearby restaurant

[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.

could obtain this data and create a geo-fence around the vicinity and push advertisement filters to all users within the geo-fence, encouraging wedding guests to continue the party at the nearby restaurant.

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. 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 its voluntary guidance entitled "Automated Driving Systems (ADS): A Vision For Safety 2.0,"[2] 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.[3]

The September 2017 guidance suggests "12 priority safety design elements" for Automated Driving Systems (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:"[4] By its terms, the guidance states that it applies to vehicles under the NHTSA's jurisdiction, including heavy-duty commercial vehicles.[5] 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 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.[6]

The 12 design elements for focus by manufacturers are:

[2] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf, p. i.
[3] https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.
[4] *Id.*, p. 1.
[5] *Id.*, p. 2.
[6] *Id.*, p. 4.

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;[7]

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 in which conditions dynamically change to fall outside of the ADS’ ODD, the vehicle should transition to a minimal risk condition”;[8]

c) Object and Event Detection, Classification, and Response (OEDR): Object and Event Detection, Classification and Response (OEDR) should be able to detect and recognize a variety of objects and events, both for normal and hazardous conditions;[9]

d) Fallback (Minimal Risk Condition): Vehicles should have minimal risk conditions for fallback should any ADS not be able to be operated safely;[10]

e) Validation Methods: The standards of SAE and the International Organization for Standards (ISO) are recommended, but not exclusively;[11]

f) Human Machine Interface: At minimum, the human interface provides information as to whether the systems are functioning properly, currently engaged in ADS mode, are experiencing a malfunction, and/or are requesting that the control transition from the ADS to the operator;[12]

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);[13]

h) Crashworthiness;

i) Post-Crash ADS Behavior;

[7] *Id.*, p. 5.
[8] *Id.*, p. 6.
[9] *Id.*, p. 7.
[10] *Id.*, p. 8.
[11] *Id.*, p. 9.
[12] *Id.*, p. 10.
[13] *Id.*, p. 11.

j) Data Recording: “Learning from crash data is a central component to the safety potential of ADSs.”[14]

k) Consumer Education and Training; and

l) Federal, State, and Local Laws.

2. H.R. 3388, the “SELF DRIVE Act"

On September 2017, the House of Congress also passed H.R. 3388, entitled 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:

- Preempts 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 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.”[15]

- Requires the Secretary of Transportation and the National Highway Traffic Safety Administration to issue long-term goals, plans, and guidelines, with express priorities and goals.[16]

- Provides 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.[17]

- States that 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: (1) describes how information of owners and occupants are

[14] *Id.*, p. 14.
[15] http://docs.house.gov/meetings/IF/IF00/20170727/106347/BILLS-115-HR3388-L000566-Amdt-9.pdf, Sec. 3.
[16] *Id.*, Sec. 4.
[17] *Id.*, Sec. 5.

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.[18]

- Raises 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."[19]

- The setting up of industry advisory council and subcommittees that would report both to Congress and make certain information public.[20]

It is unclear if the SELF DRIVE Act will pass, or even pass with any of these provisions unchanged. However, it is important to note that as self-driving technology continues to improve, momentum for some federal standards to be put in place will continue to grow, as demonstrated by how the bill had overwhelmingly passed in the House.[21]

B. THE FIGHT OVER DATA PRIVACY REGULATIONS IN BROADBAND

1. Should the FCC Retreat from ISPs?

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 an entity was a common carrier was based on the general status of the entity and not its activity at any given time.[22] 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 they engaged in what were traditionally considered "non-common carrier activities" – such 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-activities, the FTC argued that they would have jurisdiction. *AT&T Mobility* flatly rejected the dichotomy.

---

[18] *Id.*, Sec. 12.
[19] *Id.*, Sec. 6.
[20] *Id.*, Sec. 9.
[21] *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.
[22] *FTC v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016), 1003.

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."[23] 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 guidance had required ISPs to not only maintain comprehensive cybersecurity programs but provide detailed disclosures and obtain consumer opt-ins for data tracking.[24]

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[25] and revoked FCC 16-148.[26] Additionally, Pai sought to "secure online privacy by putting the FTC…back in charge of broadband providers' privacy practices,"[27] while announcing future plans to "restore Internet Freedom by repealing Obama-era Internet regulations."[28]

But *AT&T Mobility* was still controlling precedence. Thus, Pai effectively revoked any ability for the federal government to regulate ISPs: the FTC apparently did not have any ability to regulate them because ISPs were frequently the same "traditional common carriers," and the FCC had just revoked its authority to regulate ISPs.

As of the date of this publication, the FCC has announced that it is now standing alongside the FTC in its appeal of *AT&T Mobility*. The FCC filed an amicus brief, agreeing with the FTC that the court should have ruled that whether a provider was a common carrier was activity-based dependent, not status-based dependent. The FCC argues that otherwise, ISPs could potentially be operating without regulatory supervision.[29]

---

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] *Restoring Internet Freedom For All Americans* (FCC, April 26, 2017), available at: https://www.fcc.gov/document/restoring-internet-freedom-all-americans

[29] 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.

2. Can the FTC Regulate in Lieu of the FCC?

It is unclear whether the FTC would 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 a number of 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, and should be careful about making blanket statements to consumers stating that they do not share 'personal information' with third parties."[30]

- 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."[31]

Given such broad policy statements, one would have expected the FTC to have continued to aggressively draw 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 how the FTC will likewise stay quiet in 2017 against broadband carriers and ISPs, as they 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

[30] *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.
[31] *Id*. at 14.

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."[32]

3. Will States and Cities Be Regulating Broadband Privacy?

With the retreat of the FCC and its efforts to police the data privacy practices of ISPs, however, 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 left by the FCC. Critics pointed out that such bills were hastily drafted, often without sufficient understanding of the affected industries.[33]

Cities have since attempted to issue their own codes 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.[34]

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.[35] 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 requested that federal regulators step back in to prevent potentially conflicting state laws and local codes.[36]

C. NIST PREPARES FOR IOT AND AUTONOMOUS TECHNOLOGIES

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

---

[32] 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.

[33] 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/.

[34] *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.

[35] 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.

[36] 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*.

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.[37] 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 the NIST's larger effort to update all of its major publications for the advent of the internet-of-things (IoT).

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

- Is outcome based;
- 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.[38]

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 a number of "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 on 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

[37] *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.
[38] Draft Publ. 800-53, Ver. 5, p. v-vi.

controls secure that information, but they do not necessarily prevent an organization from collecting or using data unless a privacy practice creates security concerns.

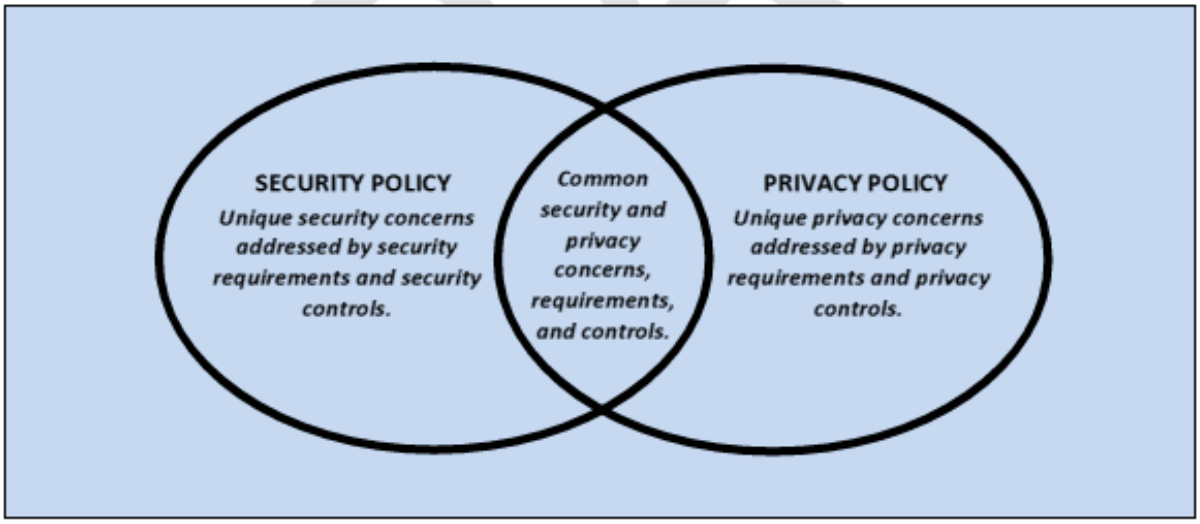


FIGURE 1: SECURITY AND PRIVACY RELATIONSHIP

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."[39]

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, the 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

[39] Draft Publ. 800-53, Ver. 5, p. 13.

Whereas traditional security models focus on preventing vectors and intrusion, Publication 800-53 focuses heavily on trustworthiness and assurance. The 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."[40] 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 a number of "supplemental guidance[s]" 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 the NIST's serialized releases and updates on IoT know that properly characterizing various individual and object attributes is important to the NIST's design evolving framework for IoT.[41] Notably, because IoT allows for a number of 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

[40] Draft Publ. 800-53, Ver. 5, p. 14.
[41] *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 takes into account 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 Publication 800-37 was meant to be open for adopting 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 the 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 bidirectional authentication that is cryptographically based before a connection can be made.

Individual Participation, Incident Response, and Privacy Authorization

Notably, the individual participation of subjects (Section 3.8) giving their data precedes the incident response section (Section 3.9). More importantly, Draft Version 5 discusses consumer choice in ways that are aligned closer to 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 those of the consumer. Again, paralleling international trends, Section 3.12, PA-3 on Purpose Specification discusses limitations by initial "specifications" dictated privacy statements, more in the tone of 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 also 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 setup.

System and Services Acquisition

Much like the 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 chain. 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 a number of 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 honeyclients, 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 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 Version 5 to be drastically revised. Therefore, legal professionals and technologists should take time to get 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**

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

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."[42] Like the current draft revision to 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.
- Reduce the *complexity* of the IT infrastructure by eliminating unnecessary systems, system components, and services — employ *least functionality* principle.

[42] *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

- 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."[43]

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.

The NIST expects to finalize revisions by March 2018.[44]

D. 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."[45] The document should not be confused with the FDA's "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).[46]

By its terms, the Guidance applies to interoperable devices, where "interoperable devices are devices as defined in Section 201(h)of the Federal Food, Drug, and Cosmetic Act (FD&C Act) that have the ability to exchange and use information through an electronic interface with another medical/non-medical product, system, or device.[47] While the Guidance states that it is a "nonbinding recommendation," it represents the FDA's recommendations to its own staff regarding the medical device community's responsibilities.

The Guidance 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

[43] Discussion Draft Publ. 800-37, Ver. 2, page 18.
[44] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft.
[45] 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.
[46] 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.
[47] *Id.* at p.4.

device labeling."[48] This applies to premarket submissions for interoperable devices including premarket notifications, de novo requests, premarket approvals, product development protocols, and biological license applications.[49]

Specifically, for premarket designs, the FDA recommends that the manufacturer:[50]

- 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;[51]

- 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";[52]

- 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.[53]

And for premarket submissions, the FDA recommends 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;[54]

[48] *Id.* at p. 3.
[49] *Id.* at p. 4.
[50] *Id.* at p. 5-6.
[51] *Id.* at p. 6-7.
[52] *Id.* at p. 9.
[53] *Id.* at p. 12.
[54] *Id.* at p. 13-14.

- 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;[55]

- 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;[56]

- Labeling as recommended by the FDA, much of which are user recommendations resulting from the processes advanced by the Guidance.[57]

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 assessing the foreseeable use and reasonably foreseeable misuse of their medical device throughout the device lifecycle."[58]

E. 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 states that it was primarily revised to cover new business models, new products, and new methods of obtaining parental consent.[59] The guidance clarified a number of important issues for emerging technology, some of which further tightened requirements:

[55] *Id.* at p. 14-15.
[56] *Id.* at p. 15-16.
[57] *Id.* at p. 17-18.
[58] *Id.* at p. 10.
[59] 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.

- "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 amongst "smart things";[60]

- An audio file may be personal information for the purposes of COPPA;[61]

- Even if a third-party is the party responsible for collecting information through your technology, you may still be responsible for complying with COPPA;[62] 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.[63]

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";[64] 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.[65]

F. 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.[66] 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

[60] *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.
[61] *Id.*
[62] *Id.*
[63] *Id.*, Step 6.
[64] *Id.*, Step 2.
[65] *Id.*, Step 4.
[66] 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.

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) provides 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 logic 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.[67]

2. Washington's New Law for Biometrics

In May 2017, Washington became the third state,[68] to pass state law broadly regulating the collection and use of "biometric information."[69] "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."[70] 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."[71] Like its Texas counterpart, however, the new Washington law does not provide for a private right of action.[72]

---

[67] A copy of Nev. SB 538 may be found at: https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB538.pdf.
[68] 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.
[69] 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.
[70] "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).
[71] 2017 Wa. ALS 299, Section 2(1).
[72] 2017 Wa. ALS 299, Section 4(2).

Other states such as New Hampshire, Alaska, Connecticut, and Montana are also considering bills regulating the use of biometrics.[73] As the new Washington law demonstrates, however, a critical question will be whether whatever is passed permits a private cause of action, much like Illinois' BIPA.[74]

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 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." [75] 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.[76] 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.[77]

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

[73] 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.
[74] See *Why Comcast And Verizon Are Suddenly Clamoring to Be Regulated*, *supra*.
[75] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1545-1550 (2016) (citations omitted).
[76] *Robins v. Spokeo, Inc.*, 2017 U.S. App. LEXIS 15211, *10 (9th Cir. Aug. 15, 2017).
[77] *Id.*, fn. 4.

period of time, it was unclear whether the momentum had swung in favor of plaintiffs. The Seventh Circuit had 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.[78]

However, other courts in the Seventh Circuit have since disagreed, sustaining motions to dismiss on the alternative ground of lack of sufficient allegations pled.[79] Notably, at least one Illinois District Court has found the type of damages alleged in *Nieman Marcus* too *de minimus* to survive a motion for failure to a state cause of action pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.[80]

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

- Third Circuit – The economic loss rule has been particularly difficult for plaintiffs to surpass, regardless of whether plaintiffs can establish standing.[81]

- Eighth Circuit – As with the Seventh Circuit, the Eighth Circuit requires that damage allegations be credible.[82]

- 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 was not stored on defendant's server (which was allegedly breached), the court granted defendant's motion for

[78] *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*).
[79] *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 *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).
[80] *In re Barnes & Noble Pin Pad Litig.*, at *8.
[81] *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).
[82] *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.[83] Similarly, in *Cahen v. Toyota Motor Corp.*, the Northern District Court dismissed the complaint after finding the allegations regarding the threat of future damages to be too speculative.[84] The District Court of Nevada denied future threat of harm as a theory of damages, limiting the class to those that suffered actual damages.[85]

- Eleventh Circuit – Where a plaintiff failed to allege that a fraudulent credit card charge was not reimbursed, the District Court dismissed the claims.[86]

- 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.[87]

In the Second, Fourth, and Fifth Circuits, where data beach litigation has been less frequent, courts have been more stringent on plaintiffs. These Circuits have outright dismissed claims based on allegations of "future harm" as insufficient.[88]

Notably, 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.[89] That theory has not been followed by other district courts, however.[90]

---

[83] *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).

[84] *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 972 (N.D. Cal. Nov. 25, 2015). See also *Antman v. Uber Techs., Inc.*, 2015 U.S. Dist. LEXIS 141945 (N.D. Cal. Oct. 19, 2015) (finding allegation of risk of identity theft credible due to lack of usable PII for identity theft).

[85] *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 2016 U.S. Dist. LEXIS 115598, *13 (D. Nev. Aug. 29, 2016) (granting motion to strike proposed class definition to only plaintiffs that suffered actual damages).

[86] *Torres v. Wendy's Co.*, 2016 U.S. Dist. LEXIS 96947, *8-9 (M.D. Fla. Jul. 15, 2016).

[87] *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).

[88] *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); *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).

[89] 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

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.[91] 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 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.[92]

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 the 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. [93]

With regard to consumer 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

---

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 PI pursuant to FCRA).

[90] *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).

[91] *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).

[92] *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).

[93] *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.[94]

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."[95]

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.[96]

B. Data Misuse Litigation: Where Technicalities Matter

Compared to data breach cases, there is arguably even 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 privacy claims, including the terms and conditions that the renters signed and the technical details of the alleged spyware.[97] 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.[98]

[94] *SELCO Cmty Credit Union v. Noodles & Co.*, 2017 U.S. Dist. LEXIS 113562, *16 (D. Colo. Jul. 21, 2017).
[95] *Cmty. Bank of Trenton v. Schnuck Mkts.*, 2017 U.S. Dist. LEXIS 66014 (S.D. Ill. May 1, 2017).
[96] *USAA Fed. Sav. Bank v. PLS Fin. Servs.*, 2017 U.S. Dist. LEXIS 82277, fn. 4 (N.D. Ill. May 30, 2017).
[97] *Krise v. SEI/Aaron's Inc.*, 2017 U.S. Dist. LEXIS 133818 (N.D. Ga. Aug. 22, 2017).
[98] *Byrd v. Aaron's, Inc.*, Case No. 11-101 (W.D. Penn. Sept. 26, 2017).

- ✓ 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.[99] 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.[100] 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 using a wide-reaching advertisement network, which includes its own fleet of affiliate and partner sites that use the Facebook "like" and "share" buttons. These buttons may seem simple, but, 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 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 Court granted Facebook's motion to dismiss, permitting plaintiffs an amendment on only the two breach of contract causes of action.[101] 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

[99] *Mount v. PulsePoint, Inc.*, 2017 U.S.App.LEXIS 5262 (2nd Cir. Mar. 27, 2017).
[100] *Smith v. Facebook*, No. 16-01282, Dkt. No. 64 (N.D. Cal. May 9, 2017).
[101] *In re Facebook Internet Tracking Litig.*, 2017 U.S.Dist.LEXIS 102464 (N.D. Cal. Jun. 30, 2017).

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.

- ✓ For Website Data and Advertisement Exchanges – In *Cole v. Gene by Gene*, plaintiffs allege 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.[102]

- ✓ 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.[103]

- ✓ 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,[104] it has also proven to be one of the most difficult causes of action to defeat by way of a motion to dismiss.[105] Notably, one of the largest data misuse settlements to date, which settled for over $8 million, alleged that Readers Digest had violated the PPPA by selling its subscriber information to third parties without subscriber consent.[106]

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 SDKs,

[102] *Cole v. Gene By Gene, Ltd.*, No. 14-0004, Dkt. No. 182 (D. Ala. Jul. 25, 2017).
[103] *hiQ Labs, Inc. v. Linkedin Corp.*, 2017 U.S. Dist. LEXIS 129088 (N.D. Cal. Aug. 14, 2017).
[104] MCLS Section 445.1715.
[105] *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).
[106] *Taylor v. Trusted Media Brands*, No. 16-1701, Dkt. No. 71 (SDNY Jun. 8, 2017) (settling for over $8.2 million for over 1.1 million class members).

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.[107] The attempt to certify the false advertising claims against the owner was then denied in July 2017, as there was not enough evidence of persistent and pervasive advertising regarding user privacy, as opposed to sporadic statements.[108]

- ✓ 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 Video Privacy Protection Act (VPPA). The Eleventh Circuit affirmed the lower court's dismissal, and cited to *Ellis v. Cartoon Network*[109] 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.[110]

- ✓ 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 Driver's Privacy Protection Act (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.[111] 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.[112]

[107] *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 92403 (N.D. Cal. July 15, 2016).
[108] *Opperman v. Kong, Inc.*, No. 13-453, 2017 U.S.Dist.LEXIS 116333 (N.D. Cal. Jul. 25, 2017).
[109] *Ellis v. Cartoon Network*, 803 F.3d 1251 (11th Cir. 2015).
[110] *Perry v. CNN, Inc.*, 854 F.3d 1336 (11th Cir. Apr. 27, 2017).
[111] *Whitaker v. Appriss*, Case No. 13-826 (N.D. In. Jul. 18, 2017), p. 8.
[112] *Id.*, p. 11.

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.[113]

- ✓ For Audio Tracking Technologies – In *Satchell v. Sonic Notify,* plaintiffs allege 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 the Golden State Warriors and its application developer, noting that the complaint failed to explain how those defendants, as opposed to the audio technology developer Sonic Notify, unlawfully intercepted and recorded messages.[114]

- ✓ 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.*[115]*

- ✓ 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.[116]

C. PRODUCT LIABILITY LITIGATION

[113] *Beckman v. Niantic, Inc.*, Case No. 2016CA008330 (Circuit Ct. of Palm Beach Ctny. Fla. May 1, 2017).
[114] *Satchell v. Sonic Notify, Inc.*, No. 16-04961, 2017 U.S. Dist. LEXIS 31456 (N.D. Cal. Feb. 13, 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).
[115] 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).
[116] *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).

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, two 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.[117]

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 III 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.[118]

D. LESSONS LEARNED

As the cases of 2017 demonstrate, it is increasingly important for data privacy professionals to have a deeper 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.

[117] *FTC v. D-Link Sys.*, 2017 U.S. Dist. LEXIS 152319 (N.D. Cal. Sept. 19, 2017).
[118] *Flynn v. FCA US LLC dba Chrysler Group LLC*, Case No. 15-0855 (S.D. Ill. Aug. 21, 2017).

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 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 just 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 allow the economic loss rule to bar most, if not all, of the claims brought by eager plaintiffs.

IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

Perhaps somewhat due 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 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.[119] 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 Chairman Maureen Ohlhausen indicated that "under our statute (the FTC Act), we cannot find a practice unfair based primarily on public policy. Instead, we must determine whether the practice causes substantial injury."[120]

- *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.[121]

- *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.[122]

- *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."[123] 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.[124]

---

[119] 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.
[120] Allison Grande, *FTC's Smart-TV Privacy Settlement Unlikely to See An Encore*, LAW360 (Feb. 7, 2017), https://www.law360.com/articles/889449.
[121] 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
[122] 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.
[123] 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.
[124] 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.

- *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.[125]

- *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 U.S.-EU Privacy Shield Program.[126]

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 that the FTC take action only where there is demonstrable harm, as opposed to "risk of harm."[127] 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."[128]

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.[129]

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.[130]

---

[125] 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.
[126] 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.
[127] 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.
[128] 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.
[129] 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.
[130] 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.

- Children's Medical Center of Dallas – Fined $3.2 million for allegedly failing to secure electronic health records until after an unencrypted laptop with 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.[131]

- St. Joseph Medical Center of Illinois – Fined $475,000 for allegedly failing to timely notify of a breach.[132]

- Memorial Healthcare Systems – Fined $5.5 million[133] 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.[134]

- 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.[135]

- The Center For Children's Digestive Health – A small, for-profit pediatric clinic was fined $31,000 for not having a business associate agreement.[136]

- 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.[137]

- St. Luke's Roosevelt Hospital Center – Paid $387,200 for allegedly impermissibly disclosing a complainant's sensitive PHI to the complainant's employer.[138]

---

[131] 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.
[132] 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.
[133] 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.
[134] Kass, *$5.5M HIPAA Deal Matches Biggest Privacy Payout*, Law360 (Feb. 16, 2017), https://www.law360.com/articles/893172.
[135] 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.
[136] Press Release, *No Business Associate Agreement? $31k Mistake* (Apr. 20, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html.
[137] 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.
[138] 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.

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.[139]

Similarly, the Financial Industry Regulatory Authority (FINRA), as a semi-governmental and self-regulatory organization, has become very aggressive with regard to its enforcement efforts. In 2017, FINRA issued three orders to its broker-dealer members with significant fines near or exceeding $1 million,[140] 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.[141]

- 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.[142]

- 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.[143]

---

[139] 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.
[140] 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.
[141] 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.
[142] 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-.
[143] 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.

- 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.[144]

- 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.[145]

- 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.[146]

- In May 2017, Target paid $18.5 million to 47 states and the District of Columbia to settle their probe over the 2013 breach.[147]

- 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.[148]

- In August 2017, Nationwide Mutual Insurance agreed to pay $5.5 million to 32 state Attorney Generals for the 2012 data breach that potentially affected 1.27 million people.[149]

Looking at the state Attorney General landscape, it is important to note that the State of New York has been much more active with public enforcement actions than

---

[144] 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.
[145] 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/.
[146] 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.
[147] 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.
[148] Arndt, *CoPilot Reaches Settlement For Delaying Data Breach Notification* (Modern Healthcare, June 15, 2017), available at: http://www.modernhealthcare.com/article/20170615/NEWS/170619934.
[149] 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.

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 information of European data subjects. However, as the program receives its first-year review, it is unclear whether it can survive unchanged.

After having merely received "a few" complaints about the program, European authorities are already arguing for the program being merely "temporary." In light of President Trump's ascension, 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."[150]

There are other signs as well. In scrutinizing the EU-Canada airline passenger data-sharing pact, 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."[151]

However, even if the Privacy Shield needs to be overhauled, it is not as if organizations 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 has referred the matter to the CJEU for review, indicating concurrently that "there are well founded grounds for believing that the SCC decisions are invalid…"[152]

B. The Revised Draft ePrivacy Regulation

[150] 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/.
[151] Lynch, *EU Court Ruling May Signal Problems For Data Privacy Shield* (Bloomberg BNA, Aug. 21, 2017), https://www.bna.com/eu-court-ruling-n73014463158/.
[152] 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/.

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.[153] The initial draft was updated in September 2017.[154]

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. 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.[155]

[153] 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

[154] https://iapp.org/media/pdf/resource_center/Council-EU-proposed-ePrivReg-Sept2017.pdf.

[155] *Id.*

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.[156]

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 just not currently possible, with there being an unmanageable plethora of do-not-track signals, without anyone to unite them all.[157]

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 on its face:

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

- 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.[158]

---

[156] 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/.
[157] 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/.
[158] 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/.

Nearly one year after its passage, American predictions that the law was to be used primarily for political purposes and protectionism have thus far proven true. Reports indicate that since the law took effect, over 40% of the enforcement actions were to remove "politically harmful contents," and less than 3% were for protecting the "rights and interests" of the "internet user."[159]

[159] 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.