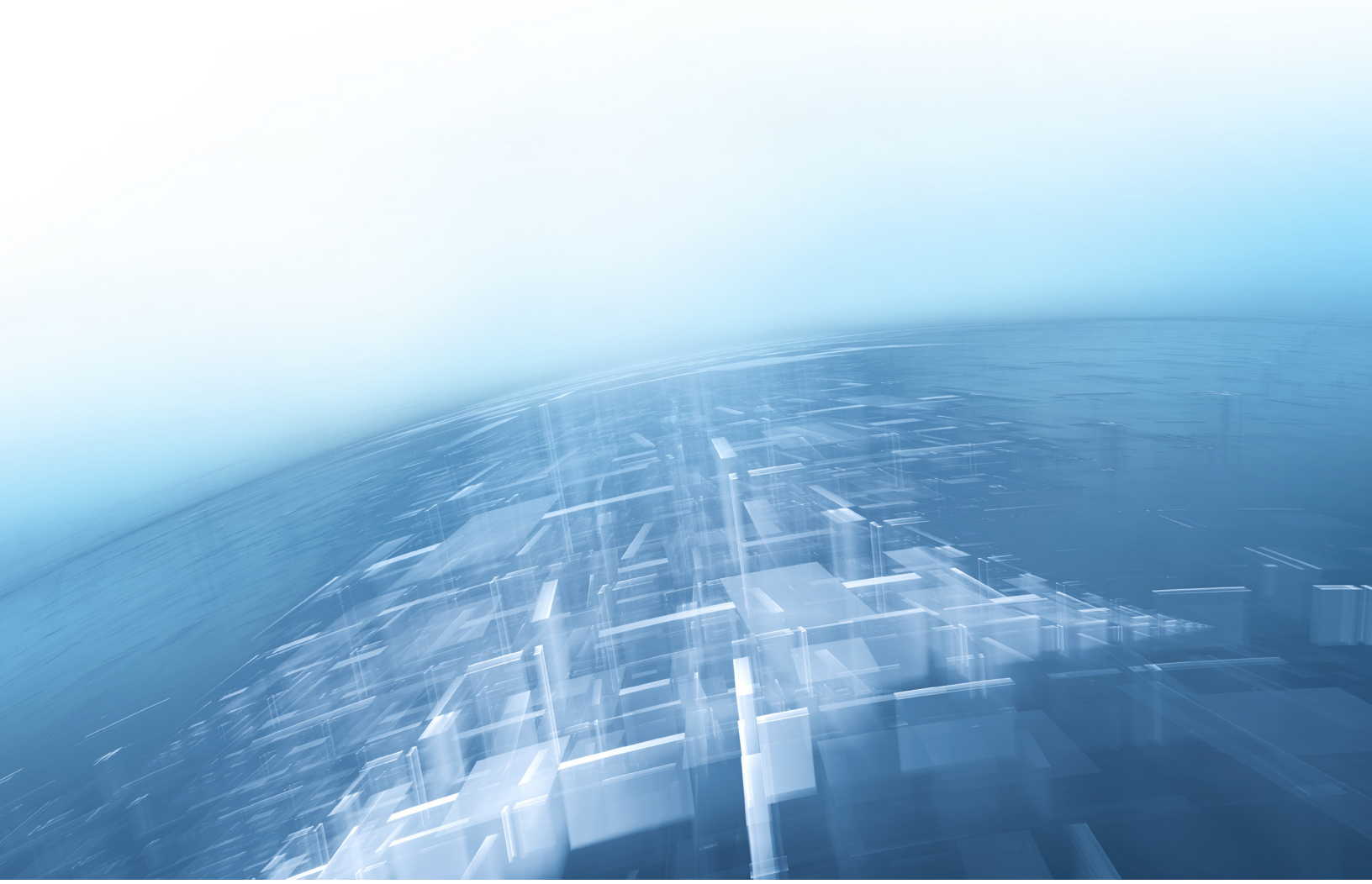


DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE

ANNUAL EDITION, FEB. 10, 2017

By

Mark C. Mao, Ronald I. Raether, Jr., Sheila M. Pham, Jonathan Yee,
Megan C. Nicholls and Melanie M. Witte

TROUTMAN SANDERS

troutmansanders.com

I. INTRODUCTION

The year 2016 was filled with new regulations and industry guidance that affect emerging technologies such as the internet of things (IoT), autonomous cars, and health wearables. Not only do these new rules define the boundaries of what is permissible, but they will also help create the new paradigms of human communication and experience.

While the Federal Communication Commission (FCC) issued one of its biggest sets of rules on how "telecommunications carriers" may use customer data, with the ascension of the Trump Administration and its new appointees, it is unclear whether the rules are here to stay. The recent opinions from the Federal Trade Commission (FTC) certainly suggest that the long battle between technology enthusiasts and privacy "advocates" is imminent.

Nonetheless, it has been exciting to review new proposals from the Department of Transportation (DOT) on the connected car industry, particularly with regard to communications protocols and cybersecurity. When read in conjunction with the industry commentary provided, the proposals signal important shifts in automobile technology and security paradigms, where there will be plenty of room for new players.

Organizations need to pay close attention to the flurry of new guidance from the National Institute of Science and Technology (NIST), as it gives closer attention to connective technologies and the supply chain process. Companies that used earlier versions of NIST guidance may need to review and reassess their existing plans and relationships.

And although the legal landscape is still divided with regard to privacy litigation, there are better examples now of what types of data and cybersecurity practices are likely to leave companies vulnerable to litigation. Likewise, while some companies have done well businesswise by taking on more aggressive postures on data use, case law suggests that some data practices are simply less likely than others to lead to litigation or regulatory investigation.

In 2017, organizations need to pay particular attention not only to continued developments in the United States, but also to what is happening in the European Union and China as well. As our world survey shows, a great divergence is emerging between the U.S. and other major parts of the world, particularly in how the U.S. is typically more encouraging of the development of connective technologies.

In reviewing and assessing developments in this advisory, we strove to break down the developing law in ways that will accord with how technology actually works, what organizations actually do and how they will develop products.

II. NEW LEGISLATION, REGULATIONS, AND INDUSTRY GUIDANCE

A. FCC Rules For Broadband and IoT

1. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (FCC 16-148)

In March 2016, the FCC issued a notice of proposed rulemaking (an NPRM), which proposes "rules that would give broadband customers the tools they need to make informed decisions about how their information is used by 'telecommunications carriers,' and whether and for what purposes their carriers may share their customers information with third parties."[1] NPRM 16-39 outlines three levels of consent: (1) no consent is necessary for "[c]ustomer data necessary to provide broadband services and for marketing the type of broadband service purchased by a customer," including for purposes such as public safety; (2) opt-outs "for the purposes of marketing other communications-related services and to share customer data with their affiliates that provide communications-related services"; and (3) "express, affirmative" opt-ins for "[a]ll other uses and sharing of consumer data."[2]

After strong criticism from industry groups and the FTC, FCC Chairman Tom Wheeler announced revised rules on October 6,[3] which were adopted on October 27 as FCC 16-148.[4] The purported purpose of the revisions was to align the FCC with the views of the FTC.

FCC 16-148 characterizes personal information using the following model:

- "Customer proprietary information ('customer PI')" includes (1) customer proprietary network information (CPNI), (2) personally identifiable information (PII), and (3) the "content[s] of communications" themselves, the categories of which are not mutually exclusive.[5]

- CPNI is defined to include "the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[6] CPNI includes network unique identifier headers (UIDH)[7] and dynamic IP addresses,[8] which remain CPNI regardless of whether it is available to others.[9]

- PII is defined as personal information "linked or reasonably linkable to an individual or device."[10] As such, MAC addresses, IP addresses, and other device identifiers are PII.[11]

- "De-identified data" is not considered de-identified unless "the carrier (1) determines that the information is not reasonably linkable to an individual or device; (2) publicly commits to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data; and (3) contractually prohibits any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data."[12] Again, the prohibition is against re-linking to customer devices.[13]

As for obtaining customer consent and providing privacy notices detailing the use of CPNI, carriers are required to:

- Notify consumers about the types of information they were collecting, how and for what purposes they were being used and shared, and the identity of entities with which the ISP shared the information.[14]

- Make their privacy notices available on their websites in addition to "any application supplied to customers by the provider."[15] Regular "periodic notices" are not required,[16] but advanced notice of "material changes" is required.[17]

1. The industry previously questioned the FCC's authority to regulate broadband; *but see US Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016) (potentially resolving issues on FCC authority to regulate neutrality).
2. Press Release, Federal Comm'cns Comm'n, FCC Proposes to Give Broadband Consumers Increased Choice Transparency and Security For Their Personal Data (Mar. 31, 2016), https://www.fcc.gov/document/fcc-proposes-broadband-consumer-privacy-rules.
3. Jenna Ebersole, *FCC Sets Out Revised Rules For Broadband Carriers,* Law360 (Oct. 6. 2016), https://www.law360.com/articles/849021/fcc-sets-out-revised-privacy-rules-for-broadband-providers.
4. Jenna Ebersole, *FCC Sets New Privacy Framework For Broadband Providers*, Law360 (Oct. 27, 2016), https://www.law360.com/articles/856450/fcc-sets-new-privacy-framework-for-broadband-providers.
5. Federal Comm'cns Comm'n, FCC 16-148, Report and Order, ¶ 85 (Oct. 27, 2016).
6. *Id.* ¶ 47.
7. *Id.* ¶¶ 51,77.
8. *Id.* ¶71.
9. *Id.* ¶82.
10. *Id.* ¶¶ 89-91.
11. *Id.* ¶¶93-94, 115.
12. *Id.* ¶ 106.
13. *Id.* ¶ 114.
14. *Id.* ¶¶ 140, 147.
15. *Id.* ¶ 141.
16. *Id.* ¶ 143.
17. *Id.* ¶¶ 156-158.

- Request opt-ins for customer PI that would be considered "sensitive information," including "at a minimum, financial information; health information; Social Security numbers; precise geo-location information; information pertaining to children; content of communications; call detail information; and a customer's web browsing history, application usage history, and their functional equivalents."[18] Using a number of examples, the FCC provides an expansive reading of what would fall within each of these categories,[19] and notes that "there are other types of information that…could [be] add[ed] to the list of sensitive information" in the future "as technologies and businesses evolve…"[20]

- Provide opt-outs to the customer for use and sharing of all other customer PI, which are generally considered non-sensitive.[21] The FCC thereby rejected an implied first-party use by the carriers.[22]

- Provide opt-ins for "[material] changes to the use and sharing of both sensitive and non-sensitive information," particularly where the carrier seeks to use "data in a manner materially different than claimed at the time of collection."[23]

- Solicit opt-ins and opt-outs at the point-of-sale, although the carrier may also seek permissions after the point-of-sale.[24] The choice mechanisms "must be persistently available on or via the carrier's website; on the carrier's app, if it provides one for account management purposes; and on any functional equivalents of either."[25]

- Not offer service contingent on the consumer's surrender of privacy rights, given the importance of services currently provided by ISPs.[26]

Notably, "no additional customer consent is needed to use customer PI to provide the telecommunications services from which it is derived, and services necessary to, or used in the telecommunications service."[27] Explaining this with reference to what it has "historically recognized," the FCC indicates that although it refuses to "enumerate a definitive list," such services include the use and sharing of non-sensitive customer PI "to market other communications services commonly marketed with the telecommunications service to which the customer already subscribes."[28] The exception also includes what are traditionally known as "adjunct-to-basic" services.[29]

As under the original NPRM 16-39, the revised rules impose "context-driven" security requirements[30] and "harm-based" breach notification obligations.[31] Importantly, the FCC recognizes that "what constitutes 'reasonable' data security is an evolving concept."[32]

Although it is unclear if FCC 16-148, as promulgated under the Obama Administration, will survive under the Trump Administration, the rules embody an important summary of contemporary views by other administrative arms of the government, including the FTC.

2. <u>Cybersecurity Risk Reduction (FCC White Paper)</u>

Following the FTC, the FCC has begun issuing its own white papers on cybersecurity and best practices. The FCC's "Cybersecurity Risk Reduction" paper issued on January 18, 2017 provided the FCC's views on cybersecurity, with a strong focus on emerging technologies such as G5 networks and IoT.

In the whitepaper, the FCC discusses its efforts on reducing cybersecurity risks, including by focusing on standards and best practices, situational awareness, security by design, reduction of risks for small and medium providers, real-time cyber threat information sharing, and supply chain risk management.[33] As further discussed below, good supply chain risk management – in addition to other forms of acquisitions and corporate convergence – is becoming an increasingly critical part of good cybersecurity risk management.

18. *Id.* ¶¶ 167, 177.
19. *Id.*¶¶ 177-190.
20. *Id.* ¶ 191.
21. *Id.* ¶ 167.
22. *Id.* ¶ 199.
23. *Id.* ¶ 195 (citation omitted).
24. *Id.*¶ 222.
25. *Id.* ¶¶ 228, 232.
26. *Id.* ¶¶ 295-297.
27. *Id.* ¶ 203.
28. *Id.* ¶¶ 204-205.
29. *Id.* ¶ 206.
30. *Id.* ¶¶ 238-247.
31. *Id.* ¶¶ 261-274.
32. *Id.* ¶ 236.
33. Public Safety & Homeland Security Bureau, Federal Commc'ns Comm'n, FCC White Paper: Cybersecurity Risk Reduction (Jan. 18, 2017).

B. FTC Guidance On e-Commerce and IoT

1. "Follow the Lead" Workshop

Nearly one year after the FTC issued its report on "Big Data,"[34] the FTC issued a report titled, "Follow the Lead' Workshop: Staff Perspective," in September 2016. The staff report discusses how financial product leads are collected online by website publishers and affiliates, transmitted to aggregators, sold to end-buyer merchants, and then verified and supplemented for other transactions.[35]

In assessing the life cycle of such products using the example of short-term loans, the FTC indicates that the financial products may have been underwritten using inaccurate data, thereby adversely affecting certain types of consumers. Although the FTC does not directly discuss the Fair Credit Reporting Act or equal opportunity laws as it did in its prior report on the use of big data analytics, the FTC engages in similar analyses.[36] Online financial services should view the staff report as demonstrative of how the FTC intends to apply the principles it laid out in its big data report against all who participate in the use of online lead generation.

2. Cross-Device Tracking: An FTC Staff Report

Noting that the Digital Advertising Alliance will begin enforcing its cross-device tracking in February 2017, the FTC published its own cross-device tracking report with recommendations. In particular, the FTC recommends:

- "As to the cross-device tracking companies, staff recommends that they provide truthful disclosures, to consumers *and* to the first party companies on whose websites and apps they appear, so that these first parties can, in turn, make truthful disclosures to consumers." The FTC notes that "failure to provide truthful information about tracking practices could violate the FTC Act," without specifying whether the violation would be against the cross-device tracking company, first-party companies, or both.[37]

- As to promises about 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." The FTC notes that 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."[38]

- With regard to opt-outs, the FTC indicates that it continues to take the position that the consumer's exercise of an opt-out in one form requires that the company affirmatively honor the opt-out in other contexts and forums. The FTC recommends that consumer-facing companies and the 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."[39]

- The FTC refers to its comments in support of FCC 16-106 to emphasize its position that "health, financial, and children's information" are all "sensitive data" in need of affirmative opt-in consent before use.[40] The comments show that at least as of the end of the Obama Administration, the views of the FCC and FTC are in general accordance.

C. NIST's Special Publications on IoT

Although the NIST is not a regulatory agency with enforcement powers, most authorities have considered its publications as a national standard. The NIST was particularly prolific in 2016 when it came to providing guidance on the development and security of IoT as the technology became increasingly popular among consumers.

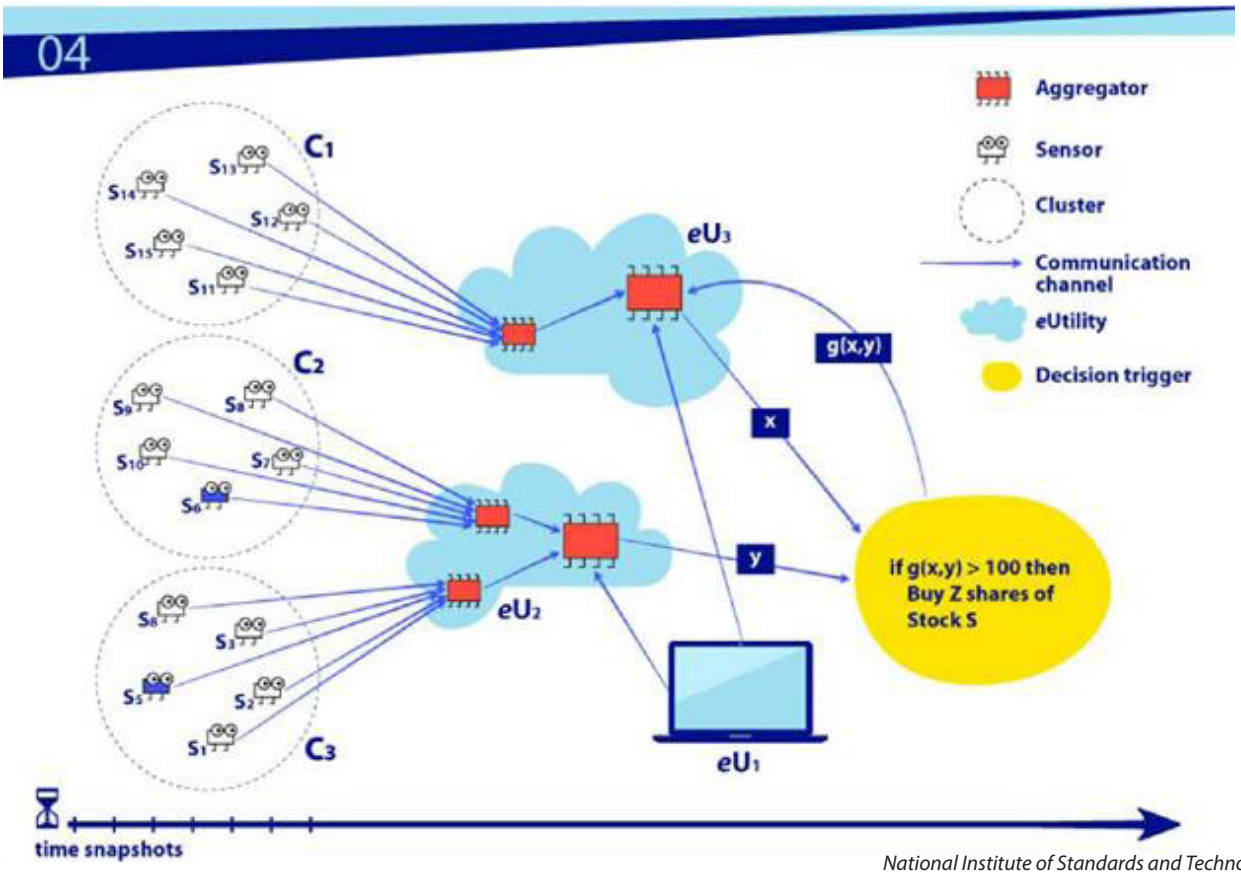
1. Network of 'Things' Guide (Special Publication 800-183)

Until recently, attorneys have been trying to describe IoT using language and terms reserved for the internet and mobile devices. But how we describe how something behaves affects our ability to spot issues, and the terms used to describe older paradigms are therefore insufficient.

34. Federal Trade Comm'n, "Big Data – a Tool for Inclusion or Exclusion? Understanding the Issues" (Jan. 2016).
35. Federal Trade Comm'n, "Follow the Lead" Workshop: Staff Perspective (Sept. 2016).
36. *Id.* at 5-8.
37. Federal Trade Comm'n, Cross-Device Tracking: An FTC Staff Report, 12 (Jan. 2017).
38. *Id.* at 12-13.
39. *Id.* at 14.
40. *Id.* at 15-16.

With Special Publication 800-183, the NIST sought to provide a more effective way to describe how the "distributed" IoT ecosystems "behave."[41] IoT is explained by way of a combination of "Primitives" and "Elements." The Primitives are (1) sensors; (2) aggregators; (3) communications channels; (4) external utilities (e-utilities); and (5) decision triggers:

- A "sensor" is an electronic utility that measures physical properties. Sensors may be paired into abstract groupings of "sensor clusters," whose composition may be dependent on what mechanisms are employed to aggregate data.[42]
- An "aggregator" is a software implementation based on mathematical functions that transform groups of raw data into intermediate, aggregated data. Aggregators may use artificial intelligence to modify clusters and the "weight" of data as appropriate.[43]
- A "communication channel" is the medium by which data is transmitted, which can be physical or virtual. For example, the latter may be a communication protocol.[44]
- An "e-utility" is an external utility in the form of a software or hardware product or service that executes processes or feeds data into the overall workflow of IoT. This includes products and services on cloud and also human beings.[45]
- A "decision trigger" is a conditional expression that triggers an action, fulfilling the results needed to satisfy the purpose, specification, and requirements of a specific IoT. Analytics may be implemented within decision triggers, which may be at any part of the IoT workflow and may feed its output back into the IoT network, creating a "feedback loop."[46]



National Institute of Standards and Technology

41. Jeffrey Voas, National Inst. of Standards and Tech., NIST 800-183, Networks of 'Things', §6 (July 2016).
42. *Id.* § 2.2.1.
43. *Id.* § 2.2.2.
44. *Id.* § 2.3.
45. *Id.* § 2.4.
46. *Id.* § 2.5.

The publication states that there may be some IoT devices that do not contain all of these elements, but that would be rare.[47]

In addition to Primitives, IoT ecosystems also include "Elements," comprised of the following: (1) environment; (2) costs; (3) geographic location; (4) owner; (5) Device_ID; and (6) snapshot. A "Device_ID" is the "unique identifier for a particular sensor, communication channel, aggregator, decision trigger, or e-Utility," whereas a "snapshot" is "an instant in time" for a distributed system where "different events, data transfers, and computations occur at different snapshots."[48]

With both Primitives and Elements in mind, one can assess the pedigree, reliability, and security risks of IoT systems, in addition to increasing their testability.[49]

2. Systems Security Engineering Guide (Special Publication 800-160)

The NIST touts its recent "Special Publication 800-160, Systems Security Engineering: Considerations For a Multidisciplinary Approach In The Engineering of Trustworthy Secure Systems" as its "flagship publication in a series of planned system security engineering publications." It is meant "to be used in conjunction and as a supplement to International Standard ISO/IEC/IEEE 15288,[50] *Systems and software engineering – System life cycle processes*."[51] As this is one of the NIST's newest and most thorough publications, organizations should consider using Publication 800-160 as one of their baselines for cybersecurity and product quality control.

Although not expressly stated within the publication, Publication 800-160 is carefully attuned to address the proliferation of new risks associated with IoT.[52] As NIST Fellow Ron Ross states, "[i]f we look at the Internet of Things and this vast productivity, [the guidance] will allow us then, for all of those devices, to assign a level of trustworthiness to each one of those components."[53]

While the publication states that its primary target is engineers, it actually provides a framework for how an organization may show "adequate security." The publication demonstrates that the "reasonableness" of security is measured by how organizations arrived at their ultimate cybersecurity decisions, and not by whether their defenses are impenetrable.

a. Chapter 1 – Introduction

The introduction acknowledges that the NIST understands that no organization can achieve perfect security, as opposed to "adequate security." The NIST states that:

> Trustworthy secure systems are less susceptible, but not impervious to, the effects of modern adversity that includes attacks orchestrated by an intelligent adversary…the basic architecture and design of systems can make those systems inherently less vulnerable, provide an increased level of penetration resistance, and offer engineered-in tolerance and resilience that can be leveraged by system owners and operators...[54]

Thus, organizations should not read the NIST 800-160 as requiring that their cybersecurity designs be perfect. Instead, organizations are expected to reduce risk using sound design.

b. Chapter 2 – Fundamentals

Chapter 2 will likely be the most instructive of all sections for attorneys. Section 2.1 on "Systems Security Engineering" discusses how the publication's approach is interdisciplinary. Thus, an organization may need to document how its information security program is assembled by a number of its institutional stakeholders, and not just one department or person.

Section 2.2 on "System and System Elements" demonstrates how the publication is meant to apply to IoT. The section defines a "system" as "a set of interacting elements (i.e., system elements) organized to achieve one or more stated purposes," which includes connected and human elements. In addition, "system of interest" defines "the set of system elements, system element interconnections, and environment that is the focus of the engineering effort." These terms describe not only an IoT environment but also the enabling and supporting elements necessary for IoT.

Section 2.3.1 on "Protection Capability and Security" describes how security is "a trade space decision or judgment driven by objective and priorities of stakeholders." In addition, "adequate

47. *Id.* § 2.
48. *Id.* § 3.
49. *Id.* §§ 4(3),4(4).
50. International Standard ISO/IEC/IEEE 15288 was issued in 2015, as "a common framework of process descriptions for describing the life cycle of systems for humans," which can be used when "acquiring and supplying systems." Available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711.
51. Ron Ross, Michael McEvilley & Janet Carrier Oren, National Inst. of Standards and Tech., NIST 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, ix (Nov. 2016).
52. Mark Rockwell, *NIST's New Take On IOT Security*, FCW (Nov. 15, 2016), https://fcw.com/articles/2016/11/15/nist-iot-security-rockwell.aspx.
53. Carten Cordell, *NIST Unveils Internet of Things Cybersecurity Guidance*, The Federal Times (Nov. 15, 2016), http://www.federaltimes.com/articles/nist-unveils-internet-of-things-cybersecurity-guidance.
54. Ron Ross, Michael McEvilley & Janet Carrier Oren, National Inst. of Standards and Tech., NIST 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2 (Nov. 2016).

security" recognizes "contradicting, competing, and conflicting needs and constraints." This section strongly suggests that properly documenting this "trade space decision" process will be one of the most important requirements for demonstrating reasonable cybersecurity.

Section 2.3.4 on "Beyond Verification and Validation – Demonstrating System Security" is another strong hint on the importance of proper documentation. The publication instructs:

> "The ultimate objective is to be able to claim with sufficient evidence or assurance, that the system is adequately secure relative to all stakeholder's objectives, concerns, and associated constraints – and to do so in a manner that is meaningful to stakeholders and that can be recorded, traced, and evolved as variances occur throughout the system life cycle. There will never be absolute assurance, however, because of the inherent asymmetry in system security – that is, things can be declared insecure by observation, but there is no observation that allows one to declare an arbitrary system secure."[55]

Section 2.4 on "System Security Engineering Framework" provides the overall "how" on proper documentation. As illustrated by the publication's Figure 3, during the "problem" phase, organizations must define and document their objectives, requirements, measures, and life cycles. During the "solution" phase, organizations must define and realize solutions, again documenting their efforts. Lastly, during the "trustworthiness" phase, organizations must develop, then demonstrate, their "assurance case."

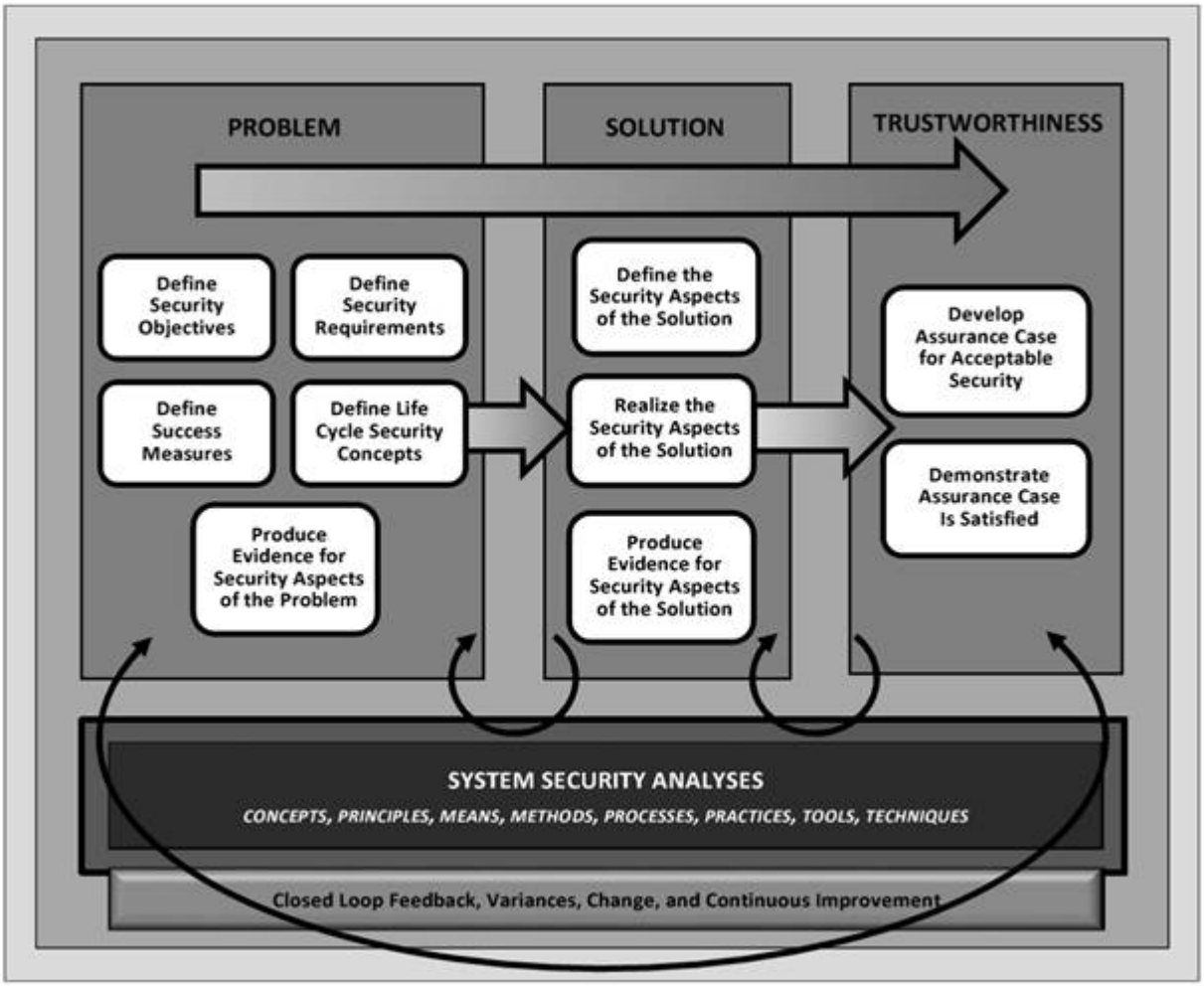


FIGURE 3: SYSTEMS SECURITY ENGINEERING FRAMEWORK

National Institute of Standards and Technology

55. *Id.* at 19.

Notably, Section 2.4.3 on "Trustworthiness Context" again speaks of how "[t]he specific form of an assurance case and the level of rigor and formality in acquiring the evidence required by the assurance case is a trade space consideration." The NIST states that "[a]ssurance cases also provide reasoned, auditable artifacts that support the contention that a claim or set of claims is satisfied, including systematic argumentation and its underlying evidence and explicit assumption that support the claims."

c. Chapter 3 – System Life Cycle Processes

The next section is primarily targeted toward an organization's various engineers and procedural gatekeepers, but there are still important lessons for lawyers both in-house and in private practice. First, Figure 4 should act as a checklist for practitioners looking to make sure that the organization has assessed its cybersecurity practices against each of the processes.

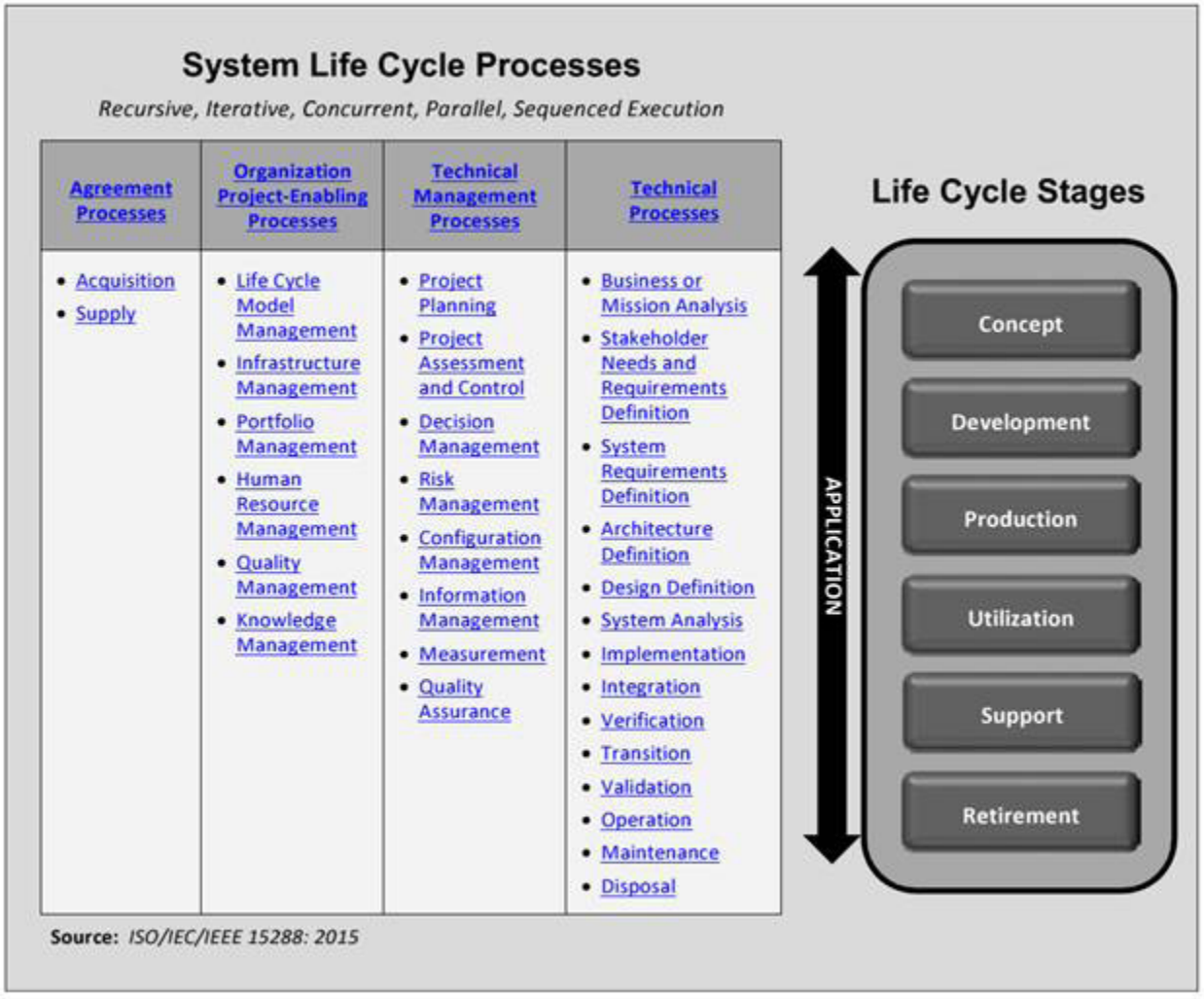


FIGURE 4: SYSTEM LIFE CYCLE PROCESSES AND LIFE CYCLE STAGES

National Institute of Standards and Technology

Notably, Figure 4 presents another way of looking at cybersecurity implementations as stages in a "life cycle" instead of "phases."

Again, the section stresses the importance of documentation to show "adequate security." Footnote 36 states that "[t]he objective is to have a body of evidence that is sufficient to convince stakeholders that their assurance needs are satisfied. The assurance level is an engineering trade space factor that must be planned and executed with the appropriate fidelity and rigor."

Although the publication then becomes much more technical, it is still important for attorneys to note each of the following:

- "Agreement Processes" in Section 3.1 will be very important to attorneys, who are often involved in asset acquisition and supply negotiations. But the

section is even more noteworthy in that it includes requirements for the organization both where it is vetting a vendor and where it is acting as the supplier. For example, Requirements AQ-1 and AQ-2 contemplate documenting the security requirements for the acquisition before the source is actually selected. Requirement AQ-3 states that a written agreement should be negotiated and entered into with the supplier, taking into consideration potential cybersecurity issues. On the other hand, Requirement SP-1 also requires that as a supplier, the organization must assess the likely security risks and document such risks before it furnishes supplies. Where a security need is not supplied by the buyer, Requirement SP-1.1 requires that the supplier make a "derivation of such criteria where it is not explicit." Requirement SP-3.2 also requires security risks reassessments by the organization as a supplier where "there may be security-related impact regardless of the basis for change."

- Section 3.2.1 on "Life Cycle Model Management Process" talks about how it is important that "assurance and trustworthiness objectives" are accomplished by applying "life cycle policies, procedures, processes, and models…using effective, proven methods and tools." In short, organizations should have consistent and measured policies that can be used to measure "assurance." Section 3.2.6 provides for requirements on a "Knowledge Management Process," where the organization would be required to develop, keep, maintain, and update security information and documentation for internal use.

- For "Technical Management Processes" in Section 3.3, Requirement PL-1 seeks to have organizations "define the security aspect of the project." Where an organization provides consumer-facing products or services, it is advisable to always include in the documentation discussions on how the privacy rights of end-users would be protected. Requirements DM-2 and DM-3 instruct the organization to document the "trade" process of often competing and conflicting objectives and obstacles. The requirements again stress documentation.

- The "Technical Processes" in Section 3.4 will be important for any organization implementing security to run through one technical requirement at a time. Notably, Section 3.4.1 on "Business or Mission Analysis Process" includes risk assessment requirements even when business *opportunities* are being explored and not just when there are risks.

Earlier in 2016, the FTC commented that complying with the NIST standards may not necessarily demonstrate reasonable cybersecurity practices.[56] The NIST's use of the term "adequate security" in Publication 800-160 is arguably a response to what would be considered "reasonable." The publication repeatedly stresses the importance of multidisciplinary and stakeholder dialogue and focuses heavily on the documentation of "better security" as opposed to "perfect security." Although the NIST's previous standards were also very much comprised of checklists, the term "adequate" implies that the NIST has taken a stance on what would evidence reasonable safeguards by the organization. Thus, it is more important than ever for large organizations to properly document their processes with savvy in-house teams and sophisticated outside counsel.

Lastly, the publication demonstrates the incremental merger of law on data use and law on cybersecurity. The NIST 800-160 contains requirements that affect an organization's outward-facing products and services, in addition to requirements that affect an organization's consideration of new business opportunities. Especially where the publication frames the security of "systems" within a framework of "enabling systems" and "systems-of-interest," data usage and cybersecurity will only be even more inextricably intertwined in the connected world.

3. (Proposed Revisions to) Framework for Improving Critical Infrastructure Security (Redlined v1.1)

In January 2017, the NIST released a "redlined Version 1.1" of its Publication 800-183, "Framework for Improving Critical Infrastructure Security." The publication was originally released in 2014 as a "voluntary guideline" in response to an Executive Directive from the Obama Administration for greater cybersecurity readiness. It purports to set forth a "Framework [that] provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally," which has since been widely used across all industries. Version 1.1 continues to explain that its guidelines can be used to "identify and prioritize" different goals within an organization, and among its different services.[57]

56. Andrea Arias, Federal Trade Comm'n, The NIST Cybersecurity Framework and the FTC (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.
57. National Inst. of Standards and Tech., Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, § 2.0 (Jan. 10, 2017), https://www.nist.gov/cyberframework/draft-version-11.

Figure 1: Framework Core Structure

National Institute of Standards and Technology

Version 1.1 revises the original guideline to account for additional concerns raised by the distributed systems of IoT and emerging technologies. This "Core" of Version 1.1 continues to be divided logically amongst four elements: (1) Functions; (2) Categories; (3) Subcategories; and (4) Informative References:

- "Functions" organize cybersecurity at its highest level: as "Identify, Protect, Detect, Respond, and Recover."
- "Categories" are subdivisions of a function, organized as "groups of cybersecurity outcomes closely tied into programmatic needs and particular activities," such as asset management, access control, and detection processes.
- "Subcategories" then "further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievements of outcomes in each Category." Examples include "data-at-rest is protected," and "notifications from detection systems are investigated."
- "Informative references" refer to "specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory." The guidance provides illustrative but not exhaustive cross-sector standards.[58]

Those who have been involved in cybersecurity implementations will continue to be familiar with Version 1.1, as the Core of the guidelines remains intact. Version 1.1 continues to center around creating a well-reasoned checklist using the Core elements. The five Functions continue to require that organizations: (1) "identify" and manage cybersecurity risks to systems, assets, data, and capabilities; (2) "protect" by developing and implementing "the appropriate safeguards to ensure delivery of critical infrastructure services"; (3) "detect" by developing and implementing "the appropriate activities to identify the occurrence of a cybersecurity event"; (4) "respond" by developing and implementing "the appropriate activities to take action regarding a detected cybersecurity event"; and (5) "recover" by developing and implementing "the appropriate activities to maintain plans for resilience and to restore any capabilities and services that were impaired."[59]

Organizations would continue to create their "Framework Profiles" by assessing the framework "Categories" and "Subcategories" against their "business drivers and a risk assessment." The purpose is to move from a "Current Profile" to a "Target Profile."[60]

58. *Id.* § 2.1.
59. *Id.*
60. *Id.* §§ 1.1, 2.3.

What has changed in Version 1.1, however, is a much greater focus on the "appropriate" vetting of the supply chain process via robust "cyber supply chain risk management (SCRM)." Each implementation "Tier" for organizations now includes a Tier-appropriate consideration for "Cyber Supply Chain Risk Management," the requirements of which depend on the cyber-sophistication, rigor, and business needs of the organization. The higher the Tier, the more quickly and efficiently risk management is expected with external and internal "suppliers, partners, and individual and organizational buyers."[61] Version 1.1 encourages the "communicating and verifying cybersecurity requirements among stakeholders" as one aspect of SCRM.[62]

Continuing the theme of Publication 800-160, Version 1.1 also advocates the "reasonableness" of an organization's cybersecurity as the product of putting in place an appropriate process for documentation and measurement.[63] Those familiar with the previous Framework Core will find a more robust and supplemented "Table 3" in the Appendix, containing updated Informative References, including new SCRM references.[64]

The NIST is soliciting comments to its currently proposed Version 1.1 until April 10, 2017.

D. DOT/NHTSA Guidance for Connected and Autonomous Cars

1. Cybersecurity Best Practices for Modern Vehicles

The DOT and the National Highway Traffic Safety Administration (NHTSA) issued their "Cybersecurity Best Practices For Modern Vehicles," in October 2016.[65] The NHTSA mentions that the guidance, although voluntary, offers "best practices" for compliance with the National Traffic and Motor Vehicle Safety Act.

In the guidance, the NHTSA urges the automotive industry to follow the Cybersecurity Framework promulgated by the NIST, structured around the concepts of "identify, protect, detect, respond, and recover," in addition to considering standards such as ISO 27000.[66] In addition, as with the Food and Drug Administration (FDA) and the emerging connected medical devices industry, the NHTSA encourages the industry to agree to share information regarding cyber threats, to standardize vulnerability and breach reporting, and to agree to self-auditing.[67] Self-auditing should include risk assessments, penetration tests, and documented organizational decisions.[68]

Specifically, the NHTSA recommends that developers and manufacturers take the following into account during the manufacturing process:

- Limit developer/debugger access, cryptographic and access keys, and vehicle maintenance diagnostic access;
- Limit access to firmware and the ability to modify firmware;
- Control the proliferation of network ports, protocols, and services;
- Use segmentation and isolation techniques in vehicle architecture design;
- Control internal vehicle communications, back-end server communications, and wireless interfaces; and
- Log events.[69]

In addition, the NHTSA expresses particular concern about after-market devices and the need for protections during automobile servicing.[70]

2. NPRM Regarding Federal Motor Vehicle Safety Standards; V2V Communications (82 Fed. Reg. 3,854)

Although not a cybersecurity document, the NHTSA and DOT's NPRM for autonomous and connected cars "proposes to establish a new Federal Motor Vehicle Safety Standard (FMVSS)" to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions. The V2V communications focus heavily on the use of "dedicated short-range radio communications (DSRC)" devices to transmit "Basic Safety Messages (BSM) about a vehicle's speed, heading, brake status, and other vehicle information to surrounding vehicles, and receiving the same information from them." The NHTSA claims that without such a protocol, the auto industry itself will be unable to move forward together meaningfully.[71]

61. *Id.* § 2.2.
62. *Id.* § 3.3.
63. *Id.* § 4.
64. *Id.* at Appendix.
65. Nat'l Highway Traffic Safety Admin., Cybersecurity Best Practices for Modern Vehicles (Oct. 2016).
66. *Id.* § 5.2.
67. *Id.* §§ 6.3 - 6.6.
68. *Id.* §§ 6.1.1 - 6.1.3.
69. *Id.* §§ 6.7.1 - 6.7.11.
70. *Id.* §§ 8 - 9.
71. Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3,854, 3,855 (proposed Jan. 12, 2017) (to be codified at 49 C.F.R. pt. 571).

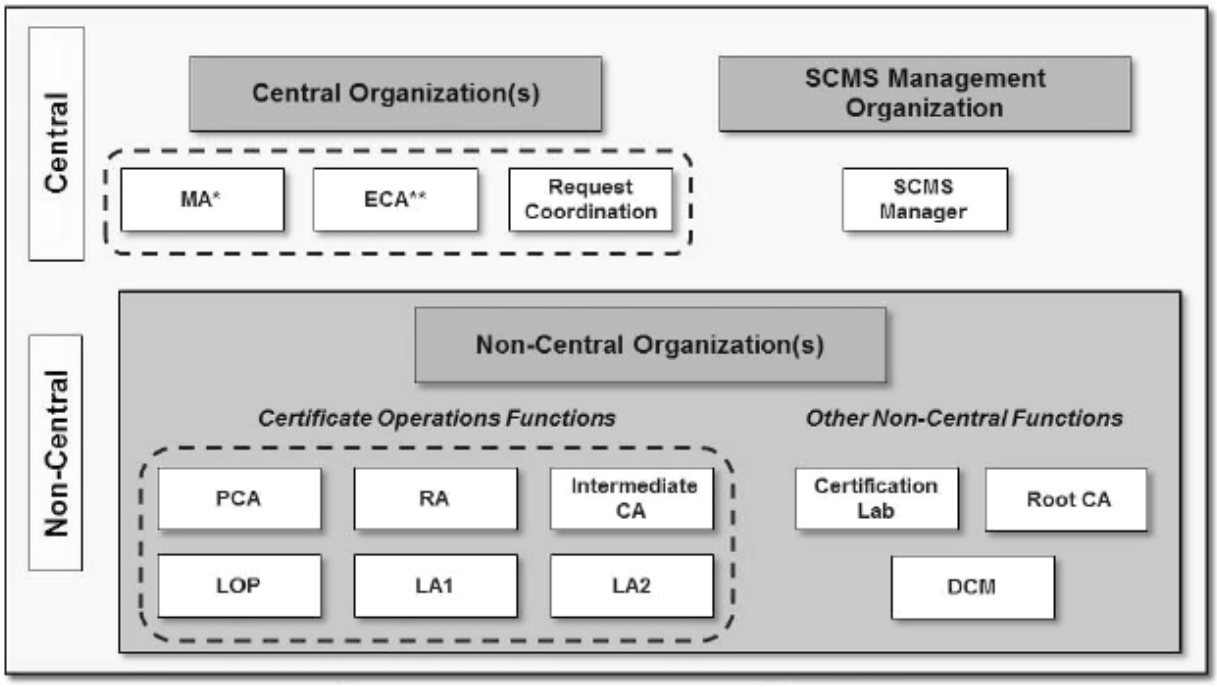
82 Fed. Reg. 3,854 is critical for the cybersecurity industry and all who intend to enter into connected cars as it describes a proposal for a new paradigm of data communications that will have important and persistent privacy implications. First, the proposal is for vehicles to deploy "omnidirectional radio signals that provide 360 degree coverage along with the ability to 'see' around corners and 'see' through other vehicles," supplemented by information from other nearby vehicles. Vehicles would communicate parameters such as speed, heading, trajectory, and other information under the BSM protocol proposed – all of which is relatively weather-proof due to the nature of DSRC. Second, using DSRC allows the industry to leverage off of existing technologies, thus allowing for earlier and more wide-spread deployment than other proposals. The NHTSA and DOT hope that the use of more readily adaptable technologies such as DSRC will allow for wider and quicker industry support and adoption of their proposal, in turn helping to save lives and preserve public safety.[72]

There are a number of critical proposals of which privacy professionals need to take note:

- The NHTSA "proposes to exclude from V2V transmitting information that directly identifies a specific vehicle or individual regularly associated with a vehicle, such as an owner's or driver's name, address, or vehicle identifying numbers, as well as data 'reasonably linkable' to an individual," citing to the FTC.
- The "NHTSA proposes V2V devices sign and verify their basic safety messages using a Public Key Infrastructure (PKI) digital signature algorithm…for BSM transmission and the signing of BSMs."
- The "NHTSA proposes to mandate requirements that would establish procedures for communicating with a Security Credential Management System to report misbehavior; and learn of misbehavior by other participants."
- The "NHTSA proposes that V2V equipment be 'hardened' against intrusion (FIPS-140 Level 3) by entities attempting to steal its security credentials."
- "V2V systems would be required to be designed from the outset to minimize risks to consumer privacy." The publication also imposes a number of other requirements on manufacturers.[73]

In addition to the peer-to-peer BSM communications, the NHTSA is requesting comments for two innovative proposals for V2V device credentialing, both of which would complement the use of PKI.[74] The first approach is the "Federated Security Credential Management (SCMS)" model, which envisions a system "established, funded, and governed primarily by one or more private entities – possibly a consortium of automobiles and V2V device manufacturers."[75] It would include the following functions in the issuance, management and revocation of short-term certificates for vehicle transmissions: (1) SCMS managers; (2) registration authorities (RAs); (3) root certificate authorities (Root CAs); (4) intermediate certificate authorities (Intermediate CAs); (5) pseudonym certificate authorities (PCAs); (6) linkage authorities (LAs); (7) misbehavior authorities (MAs); (8) location obscurer proxies (LOPs); and (9) request coordination.[76] Each of these functions is envisioned to be part of a system wherein "certificate management entities (CMEs) would manage "short-term certificates" for participating vehicles, with both "centralized" CMEs and federated CMEs.

72. *Id.* at 3,863 - 66.
73. *Id.* at 3,866-69.
74. The NHTSA notes that it believes that PKI alone, at least as currently used, cannot fulfill the needs of emerging connected car technologies. *Id.* at 3,934.
75. *Id.* at 3,935.
76. *Id.* at 3,935-36.



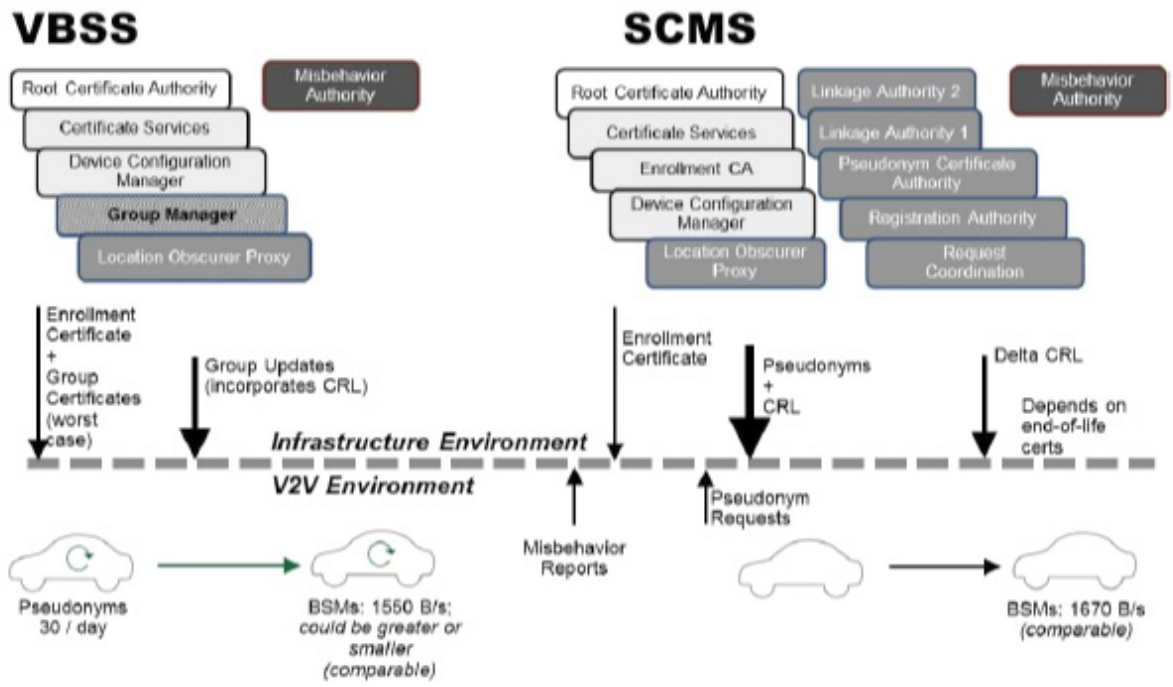
Department of Transportation and National Highway Traffic Safety Administration

As the NHTSA's figure above shows, only a few CMEs should handle "central functions," whereas many CMEs can compete and handle "non-central" functions. The CMEs with central functions would likely need to work with the NHTSA and be subject to future rulemaking.[77] Notably, by dividing identifying information amongst different CMEs – centralized and federated – the hope is that safety is achieved with little compromise of security and PII. The NHTSA compares its proposed paradigm to that of the multi-stakeholder Internet Corporation for Assigned Names and Numbers (ICANN).[78]

The NHTSA is also considering a "Vehicle Based Security System (VBSS)" as an alternative to SCMS, which has a single security certification root. The major difference is in the "generation of short-term certificates." 82 Fed. Reg. 3,854 states:

> The SCMS approach relies on individual vehicles to periodically request pseudonym certificates from infrastructure-based entities (most notably a Pseudonym Certificate Authority, or PCA) which in turn generates and signs short-term certificates. Vehicles then download batches of certificates which are used to digitally sign BSM messages. In contrast, the VBSS concept calls for delegating this authority to individual vehicles, and as a result the communications with the infrastructure are reduced.

77. *Id.* at 3,937-38.
78. *Id.* at 3,950-52.



Department of Transportation and National Highway Traffic Safety Administration

A number of functions required under SCMS are thereby eliminated, and the whole process is simplified. Instead, "VBBS establishes a Group Manager/Group Managers (GM) to provide credentials that make it possible for each vehicle to act as a [subordinate] certificate authority – an entity that can generate short-term certificates." "All member signing keys for a particular group are associated with a single group certificate." The NHTSA indicates that the VBBS is currently further behind SCMS because "while Group-based signature schemes are an active area of research they are evolving and much less mature than other cryptography systems."[79]

The public comments period for 82 Fed. Reg. 3,854 will end on April 12, 2017.

E. FDA's Postmarket Management of Cybersecurity in Medical Devices

On December 28, 2016, the FDA issued its "nonbinding recommendations" guidance for addressing postmarket cybersecurity vulnerabilities in medical devices under the title "Postmarket Management of Cybersecurity in Medical Devices."[80] The recommendations are for a "risk-based framework for assessing when changes to medical devices for cybersecurity vulnerabilities require reporting to the Agency and outlines circumstances in which FDA does not intend to enforce reporting requirements."[81]

By its terms, the Guidance applies to: "1) medical devices that contain software (including firmware) or programmable logic, and 2) software that is a medical device, including mobile medical applications." It applies to legacy devices, in addition to those going onto the market.[82]

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 to monitor, identify, and address cybersecurity threats to medical devices, including for emerging connected medical devices.

A few points in the guidance stand out in particular:

- A good cybersecurity risk management program includes: (1) monitoring cybersecurity information sources for identification and detection of risks; (2) maintaining robust software lifecycle processes that include monitoring third-party software, and

79. *Id.* at 3,954-55.
80. 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.
81. *Id.* at 4.
82. *Id.* at 8.

verification and validation for software updates and patches; (3) establishing and communicating processes for vulnerability intake and handling; (4) using threat modeling; (5) adopting a coordinated vulnerability disclosure policy and practice; and (6) deploying mitigation strategies.[83] The FDA recommends that manufacturers "incorporate elements consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity."[84]

- The guidance concedes that "medical devices and the surrounding network infrastructure cannot be completely secured."85 But the focus of the program is on "the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria."[86]
- The FDA further urges manufacturers to characterize cybersecurity vulnerabilities as "acceptable or unacceptable" and "controlled or uncontrolled."[87] Uncontrolled risks are those that are "present when there is unacceptable residual risk of patient harm due to insufficient risk mitigations and compensating controls." While uncontrolled risks need to be reported to the consumers and the FDA, the FDA does not intend to enforce reporting requirements where: (1) there are no serious adverse effects; (2) the manufacturer provides interim and remediating controls to customers within 30 days; (3) the manufacturer fixes the vulnerability within 60 days; and (d) the manufacturer actively participates in an information sharing analysis organization (ISAO) that shares vulnerabilities and threats.[88]

F. New York State Department of Financial Services' Cybersecurity Requirements for Financial Services Companies

In September 2016, the New York State Department of Financial Services (NY DFS) proposed cybersecurity requirements that would generally apply to banks, insurers, and other financial institutions operating in the State of New York. Many commentators complained that the requirements were overreaching and too onerous, and as a result, the rules were revised to be more congruent with other existing cybersecurity regulations.

As revised, 23 NYCRR 500 would require that covered entities: (1) set up a comprehensive cybersecurity program (Section 500.02); (2) adhere to a written cybersecurity policy and incident response plan (Sections 500.03 and 500.16); (3) appoint a chief information security officer (Section 500.04); (4) require multi-factor authentication and encryption (Sections 500.12 and 500.15); (5) conduct periodic penetration, vulnerability, and risk assessments (Sections 500.05 and 500.07); (6) limit access privileges (Section 500.07); (7) require vendor controls and written assurances (Section 500.11); and (8) limit data retention (Section 500.12). In addition, "cybersecurity events" may need to be reported to the NY superintendant if (a) the event requires "notice…to be provided to any government body, self-regulatory agency or any other supervisory body, and (b) the event has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" (Section 500.17).[89]

The public comments period for 23 NYCRR 500 ended on January 27, 2017.

G. Miscellaneous Industry Guidance and Self-Governance on IoT

After many years of discussion, neither regulators nor industry groups are yet able to agree on any general framework for privacy and security standards for IoT. A plethora of industry efforts and consortiums have been initiated, but no clear winners have appeared.[90] Nonetheless, a number of efforts are noteworthy:

- In February 2016, the Groupe Speciale Mobile Association (GSMA) promulgated both "IoT

83. *Id.* at 13-14.
84. *Id.* at 14.
85. *Id.*
86. *Id.* at 15.
87. *Id.*
88. *Id.* at 12, 22 - 23.
89. N.Y. State Dept. of Financial Servs., Proposed 23 NYCRR 500: Cybersecurity Requirements for Financial Services Companies (Dec. 28, 2016).
90. *See* Susan D. Rector, *"Internet of Things" Protocols: Past And Future Trends* Law360 (Oct. 12, 2016), https://www.law360.com/articles/850593/internet-of-things-protocols-past-and-future-trends.

Security Guidelines" and "IoT Connection Efficiency Guidelines."[91] The GSMA effort is noteworthy because it represents the interests of mobile operators worldwide, boasting more than 800 participating operators and 250 companies in the broader mobile ecosystem. As to the IoT Security Guidelines, the GSMA purports that it "has delivered a set of security guidelines to promote best practices for the secure design, development and deployment of IoT services," primarily targeting IoT service providers, device manufacturers, developers, and network operators. Although the GSMA guidelines are not discussed in the United States as often as they may be internationally, it is important to note:

1. The GSMA guideline on end-point security is one of the most comprehensive amongst IoT guidelines. As the GSMA notes, IoT presents additional security challenges as compared to traditional mobile devices due to less robust processing power and lower energy accessibility for end-point IoT devices.[92] The GSMA guidelines provide for a method of demonstrating that end-point security has been properly assessed and designed.[93]

2. The GSMA provides a separate guideline for the IoT service ecosystem, which lists critical, high-priority, medium-priority, and low-priority recommendations. Amongst the critical recommendations are "defining an organizational root of trust (certification)," creating an appropriate "bootstrap (credentialing) model" for the running of applications on top of a secure and high-quality platform, and defining a "security front-end" for public systems to "[e]nsure that both ingress and egress filtering are managed."[94]

The GSMA is trying to promote its standards by allowing self-assessment and submission to the GSMA.[95]

- In April 2016, Underwriters Laboratories (UL) launched a new "UL 2900" series of standards that offer cybersecurity test criteria for network-linked products and systems as part of its UL Cybersecurity Assurance Program. The program is noteworthy because UL is well-recognized for product safety certification. The standard purports to prescribe minimum requirements for security controls in addition to describing testing and verification. 96 Controls include access controls, secure data storage, cryptography, key management, authentication, integrity, and confidentiality of data received and transmitted.[97]

- In November 2016, the Broadband Internet Technical Advisory Group (BITAG) issued its "Internet of Things [IoT] Security and Privacy Recommendations." After discussing issues in IoT and its observations, BITAG provided 10 major recommendations, including:

  1. "IoT devices should be restrictive rather than permissive in communicating." In short, "[w]hen possible, devices should not be reachable via inbound connections by default." (Section 7.3.)

  2. "IoT devices should continue to function if internet connectivity is disrupted." (Section 7.4.)

  3. "IoT devices should continue to function if the cloud back-end fails." (Section 7.5.)

  Notably, BITAG recommends that manufacturers require "automatic and mandatory security updates," which some in the industry have indicated can present a security risk in itself. In response, BITAG suggests that in cases where there should be a consumer choice allowed, the user should instead be afforded an opt-out. (Section 7.1)[98]

- On January 5, 2017, the Online Trust Alliance (OTA) updated its "IoT Trust Framework – Resource Guide." Although the OTA "recognize(s) that there is no perfect security or privacy state," it provides 37 principles organized under the headings of (1) security principles, (2) user access & credentials, (3) privacy, disclosures & transparency, and (4) notifications & related best practices. Although not mandatory, organizations

91. *See* Groupe Speciale Mobile Ass'n, IoT Security Guidelines (Feb. 2016), http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/; and Groupe Speciale Mobile Ass'n, IoT Connection Efficiency Guidelines (Feb. 2016), http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/.
92. Groupe Speciale Mobile Ass'n, CLP.13 – IoT Security Guidelines For Endpoint Ecosystems, § 2 (Nov. 2016).
93. *Id*, § 7.
94. Groupe Speciale Mobile Ass'n, CLP.12 – IoT Security Guidelines for IoT Service Ecosystem, §§ 5.2-5.4 (Nov. 2016).
95. Groupe Speciale Mobile Ass'n, IoT Security Guidelines (Feb. 2016), http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/.
96. Press Release, Underwriters Labs., UL Launches Cybersecurity Assurance Program (Apr. 5, 2016), http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/.
97. Underwriters Labs., UL 2900-2-2, Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems (Mar. 30 2016), https://standardscatalog.ul.com/standards/en/outline_2900-2-2_1.
98. Broadband Internet Technical Advisory Grp., Internet of Things (IoT) Security and Privacy Recommendations (Nov. 2016), https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php.

involved in e-commerce are encouraged to assess their practices against the list (and the authorities cited therein), with attention to practices less often mentioned such as:

1. Organizations "must have a mechanism for automated safe and secure methods to provide software and/or firmware updates, patches and revisions." (Principle No. 5.)
2. "Design devices to minimum requirements necessary for operation." (Principle No. 9.)
3. "Disclose the duration and end-of-life security and patch support…Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase." (Principle No. 16.)
4. "Disclose what features will fail to function if connectivity or backend services become disabled or stopped…" (Principle No. 18.)
5. "IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services." (Principle No. 20.)
6. "Publicly post the history of material privacy notice changes for a minimum of two years." (Principle No. 28.)
7. Provide users the ability to wipe their data with finality, both with the provider and on the device, upon the discontinuance of service or use. (Principle Nos. 29 and 30.)
8. End-user communications should incorporate authentication protocols to help prevent spear phishing and spoofing. (Principle No. 31.)
9. "Implement measures to help prevent or make evident any physical tampering of devices." (Principle No. 34.)[99]

99. Online Trust Alliance, IoT Trust Framework – Resource Guide (Jan. 5, 2017), https://otalliance.org/initiatives/internet-things.

III. EVOLVING CASE LAW

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 arguably suffered no injury-in-fact may nonetheless have Article III standing for a statutory procedural violation. The Court held that the "injury-in-fact requirement requires a plaintiff to allege an injury that is both 'concrete *and* particularized.'" A "concrete" injury must "actually exist," while a "particularized" injury "must affect the plaintiff in a personal and individual way." Noting that the lower court focused its analysis only on the latter, the Court emphasized that "Article III standing requires a concrete injury even in the context of a statutory violation." Importantly, the Court held that the plaintiff may not allege a "bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III" because "[a] violation of one of the FCRA's procedural requirements may result in no harm."[100]

However, the *Spokeo* Court remanded the case back for further determination by the Ninth Circuit consistent with the Court's ruling, while indicating that "intangible injuries" may nonetheless be "concrete."[101] By not providing clear guidance on what may nonetheless be "concrete" despite being "intangible," the lower courts are now in discord not only for the purposes of the Fair Credit Reporting Act (FCRA) litigation but also for data breach and data misuse litigation.

A. Data Breach Litigation: A Divided Post-*Spokeo* Landscape

Continuing with 2015 trends, the circuit courts remained divided on what is required for plaintiffs to demonstrate Article III standing. Although most of the courts continue to hold a high bar for data breach cases, some plaintiffs can survive motions to dismiss.[102]

For example, the Seventh Circuit had handed down a pair of appellate decisions holding "concrete and particularized" injuries were met by allegations of increased threat of fraud and identity theft after data had been stolen, and by the time and money spent trying to resolve such issues. The circuit court reversed separate lower Illinois courts in *Remijas* and then in *P.F. Chang*. 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.[103]

The Third and Sixth Circuit Courts have since cited to *Remijas v. Neiman Marcus Group* in support of their refusal to affirm lower district court's dismissal of data breach class actions for lack of Article III standing.[104] Some district courts have likewise denied motions to dismiss, finding the damage theories espoused by plaintiffs sufficient.[105]

In addition to trying to change the post-*Clapper v. Amnesty International*[106] landscape, plaintiffs have made some other interesting and noteworthy moves this year. First, as mirrored in the data misuse cases further discussed below, plaintiffs are increasingly taking advantage of situations where defendants have multiple applicable privacy statements, arguing that the policies are ambiguous taken altogether and that the "agreements" on consumer privacy should incorporate additional terms and expectations.[107] Second,

100. *Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1545-1550 (2016) (citations omitted).
101. *Id.* at 1549.
102. See Ronnie Solomon & Tyler Newby, *Post-Spokeo, Standing Challenges Remain Unpredictable,* Law360 (Oct. 26, 2016), https://www.law360.com/articles/854898/post-spokeo-standing-challenges-remain-unpredictable.
103. *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*).
104. *In re Horizon Healthcare Servs. Inc. Data Breach Litig.,* No. 15-2309, 2017 U.S.App. LEXIS 1019 (3rd Cir. Jan. 20, 2017) (finding standing in case involving stolen laptops involving PII); *Galaria v. Nationwide Mut. Ins. Co.*, Nos. 15-3386/3387, 2016 U.S. App. LEXIS 16840, *9-13 (6th Cir. Sept. 12, 2016) (reversing granting of motion to dismiss by lower district court, finding that (a) increased threat and mitigation costs incurred were sufficient, disagreeing with *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3rd Cir. 2011), and (b) that Article III standing only requires "fairly traceable" causation and not "proximate cause" causation).
105. See e.g., *Adams v. Congress Auto Ins. Agency, Inc.*, 90 Mass. App. Ct. 761 (2016) (alleges employee's improper access of insurer's DMV records of plaintiff); *Hapka v. CareCentrix*, No. 16-2372, 2016 U.S. Dist. LEXIS 175346 (D. Kan. Dec. 19, 2016 (denying Article III challenge in case involving hacked employee W-2s where fraudulent tax returns were allegedly filed); *Bohannan v. Innovak Int'l, Inc.,* No. 16-CV-272, 2016 U.S. Dist. LEXIS 102496 (M.D. Ala. Aug. 4, 2016) (SaaS portal flaw for 2 years, with only allegations of false tax filings and mitigation efforts taken); see also *In re Premera Blue Cross Customer Data Sec. Breach Litig.* No. 15-MD-2633, 2016 U.S. Dist. LEXIS 100198, at *48-53 (D. Or. Aug. 1, 2016) (discussing how loose unjust enrichment and lost time allegations may be sufficient to withstand motion to dismiss); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-2617, 2016 U.S. Dist. LEXIS 70594 (May 27, 2016) (permitting various contract theories to survive); *Irwin v. Jimmy John's Franchise*, 175 F. Supp. 3d 1064, 1070-1071 (C.D. 2016) (dismissing most causes of action, but permitting some causes of action to survive, including one based on "implied contract"); *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2016 U.S. Dist. LEXIS 22472 (N.D. Ill. Feb. 23, 2016) (denying motion to dismiss on last remaining contract cause of action, after having dismissed other causes of action, in case alleging unsecured employee PII on publicly available website).
106. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).
107. See e.g., *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2016 U.S. Dist. LEXIS 100198, at *39-41, *53-54 (recognizing quasi-contract remedy of unjust enrichment, and granting leave to amend on contract causes of action); see also *In re Anthem, Inc. Data Breach Litig.*, 2016 U.S. Dist. LEXIS 70594 (permitting various contract theories to survive); see also *Irwin* 175 F. Supp. 3d at 1070-1071 (dismissing most causes of action, but permitting some causes of action to survive, including one based on an "implicit agreement to safeguard the customer's information to effectuate the contract").

plaintiffs have continued to try to push novel theories of liability, such as arguing that because the FCRA requires that consumer reporting agencies assure that "consumer reports" are delivered only to the intended recipients, implicit in such a requirement is a security obligation as well.[108] These developments suggest that plaintiffs will continue to explore additional theories of liability to address the standing issue.

Regardless, many courts continue to grant motions to dismiss on the basis of lack of Article III standing, particularly where no PII misuse is alleged, where the alleged misuse is not credible, or where there are only limited instances of misuse.[109] In addition, defendants have been increasingly successful with other preliminary challenges that are not entirely reliant on a *Clapper*-Article III challenge:

- Defendants have successfully argued that plaintiffs have not plausibly alleged actual harm.[110] More specifically, defendants have successfully argued that where courts are not inclined to grant a dismissal for lack of Article III standing pursuant to Federal Rules of Civil Procedure Rule 12(b)(1), defendants may nonetheless still demonstrate lack of damages for each cause of action pursuant to Federal Rules of Civil Procedure Rule 12(b)(6).[111]

- Defendants have successfully argued that the proposed class definitions are too overbroad and encompass members who have not suffered any actual damage. Such claims were subject to a motion to dismiss or motion to strike.[112]

---

108. See e.g., *In re Horizon Healthcare Servs. 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*, 2016 U.S. App. LEXIS 16840 (remanding to district court to decide whether plaintiffs' sufficiently stated a cause of action under the FCRA, where plaintiffs alleged that they submitted insurance and financial applications to Nationwide created duty by Nationwide to secure PI pursuant to FCRA); but see *In re Cmty. Health Sys.*, No. 15-CV-222, 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," court refused to find neither defendant a "consumer reporting agency").

109. *Beck v. MacDonald*, 2017 U.S. App. LEXIS 2095 (4th Cir., Feb. 6, 2017) (finding no Article III standing for lost laptop at a veteran medical center, affirming lower court and citing *Clapper*-analysis); *Dittman v. Univ. of Pittsburgh Med.Ctr.*, 2017 Pa. Super. 8 (2017) (affirming lower court ruling that employers do not have a general duty to secure PII, and the economic loss rule applied); *Welborn v. IRS*, No. 15-1352, 2016 U.S. Dist. LEXIS 151673 (D.D.C. Nov. 2, 2016) (granting motions to dismiss because PII has no inherent value and fear and anxiety are insufficient); *In re Zappos.com, Inc. Customer Data Sec. Litig.*, Nos. 12-cv-325, MDL No. 2357, 2016 U.S. Dist. LEXIS 115598 (D. Nev. Aug. 29, 2016) (affirming previous order to dismiss claims where no actual damage is alleged); *Attias v. Carefirst*, No. 15-cv-882, 2016 U.S. Dist. LEXIS 105480, at *15-17 (D.D.C. Aug. 10, 2016) (granting motion to dismiss, finding no "plausible harm" alleged), *accord Chambliss*, *infra*; *Torres v. Wendy's Co.*, No. 16-cv-210, 2016 U.S. Dist. LEXIS 96947, at *6-9 (M.D. Fla. July 15, 2016) (dismissing complaint with leave to amend, where plaintiffs alleged malicious malware gained access at different locations, but alleges only two fraudulent credit card charges that were reported by him to authorities, and which he fails to allege were not reimbursed thereafter); *Duqum v. Scottrade, Inc.*, No. 15-CV-1537, 2016 U.S. Dist. LEXIS 89992, at *17-18 (E.D. Mo. July 12, 2016) (no misuse alleged resulting from hack, and over two years have passed); *Bradix v. Advance Stores Co.*, Civ. Action No. 16-4902, 2016 U.S. Dist. LEXIS 87368 (E.D. La. July 5, 2016) (finding allegations of two "as yet identified" attempts to secure vehicle financing insufficient); *Khan v. Children Nat'l Health Sys.*, Civ. Action No. 15-2125, 2016 U.S. Dist. LEXIS 66404, at *15-16 (D. Md. May 19, 2016) (finding no allegations of misuse, even where there are allegations of compromise); see *Chambliss v. CareFirst, Inc.*, 189 F. Supp. 3d 564,(D. Md. 2016) (granting motion to dismiss, finding no harm alleged); *Patton v. Experian Data Corp.* No. SACV 15-1871, 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016) (granting motion to dismiss and remanding to state court, for failure to allege that alleged breach led to any unlawful access of PI); *In re SuperValu, Inc.*, No. 14-MD-2586, 2016 U.S. Dist. LEXIS 2592, at *11-19 (D. Minn. Jan. 7, 2016) (citing *Whalen*, *infra*, amongst others, noting that "only one unauthorized credit card charge (of an unspecified date and amount) is alleged to have occurred in the fifteen-month time period following the Data Breach that affected over 1,000 of Defendants' stores. This singular incident from one named Plaintiff over the course of more than a year following the Data Breach is not sufficient to 'nudge' Plaintiffs' class claims of data misuse or imminent misuse 'across the line from conceivable to plausible'"); *Whalen v. Michael Stores, Inc.*, 153 F. Supp. 3d 577, 583 (E.D.N.Y. 2015) (refusing to apply *Remijas v. Neiman Marcus Group*, 794 F.3d 688, 691-694 (7th Cir. 2015), and noting that plaintiffs only alleged that the putative class representative was affected, but even then, she did not suffer out-of-pocket losses).

110. *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, at *43-44 (dismissing claims of some plaintiffs, because allegations of actual harm must be "fairly traceable" to alleged breach); *Attias*, 2016 U.S. Dist. LEXIS 105480, at *15-16 (granting motion to dismiss, finding no "plausible harm" alleged because the harm alleged was denial of tax refund, but court points out complaint fails to allege loss of social security number, which is necessary for interference with any tax filings); *Patton*, 2016 U.S. Dist. LEXIS 60590 (granting motion to dismiss, noting that allegations of future harm must be "credible").

111. *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2016 U.S. Dist. LEXIS 137078, at *25 (N.D. Ill. Oct. 3, 2016) (while conceding that plaintiff has demonstrated Article III standing under *Remijas*, *supra*, finding motion to dismiss should still be affirmed because plaintiffs allege no out-of-pocket damages sufficient to state a viable cause of action for the purposes of a Fed. Rule Civ. Proc. Rule 12(b)(6) challenge).

112. *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, at *37-40 (dismissing claims of some plaintiffs, where the claims lacked allegations of misuse, and where the mitigation efforts were coupled to claims that lacked allegations of misuse); *In re Zappos.com, Inc. Custom Data Sec. Litig.*, Nos. 12-cv-325, MDL No. 2357, 2016 U.S. Dist. LEXIS 604053, at *26-28 (D. Nev. May 6, 2016), *aff'd*, 2016 U.S. Dist. LEXIS 115598 (Aug. 29, 2016); see also *Baum v. Keystone Mercy Health Plan*, 145 A.3d 793 (Pa. Super. Ct. 2016) (affirming court of common plea's denial of class certification, and expressing in dicta its doubt that plaintiffs would be able to show *reliance* amongst the class).

- The economic loss rule may bar data breach claims in cases where an express or implied agreement is alleged.[113]

Just as importantly, while the Seventh and Ninth Circuits had appeared more plaintiff-friendly for a few months, the legal landscape has again begun shifting toward the defense. In both Circuits, courts are again granting motions to dismiss, particularly where plaintiffs' allegations of harm are more attenuated.[114]

Assessing the legal landscape, organizations on the defense should take note of a number of important lessons:

1. The business and technological sophistication of breach counsel is more important than ever. Courts are increasingly drawing inferences from how organizations handled their response to data incidents and technologically competent counsel will be able to better help organizations navigate through events. Counsel lacking familiarity with technology are often unable to effectively articulate the difference between system vulnerability and data compromise. Competent breach counsel will use their technical skills to deter and minimize the scope of potential litigation, and to understand which technical differences require individual treatment of potentially affected consumers and thus mitigate the risks of a putative class action.

2. Even if an organization has suffered a data incident, there may be no viable claims against it if there is insufficient evidence of actual data misuse or if there are only a few isolated instances of misuse. Especially in the case of the latter, early challenges to strike broad class pleadings will reduce the value of a case drastically.

3. Federal Rule of Civil Procedure 12(b)(6) may sometimes present a higher bar for the harm that plaintiffs must plead, when compared to Federal Rule of Civil Procedure 12(b)(1). For almost all causes of action, actual out-of-pocket loss is required to survive a Rule 12(b)(6) challenge. Knowledge of potential statutory claims by defense counsel, such as the FCRA, becomes critical in this context.

4. Although there are still no cases clarifying what standards of care an organization must adopt with regard to data security, courts will likely assess a defendant's practices against its privacy statement, or other consumer-facing documents such as a terms of use, even at the pleading stage, as if "agreements" had been made. In extreme cases, a court may attempt to incorporate some regulatory or social expectations as part of an "implied agreement." But in such cases where plaintiffs are relying heavily on contract and quasi-contract theories of liability, the application of the economic loss rule should be explored.[115]

5. Motions to dismiss may no longer be the sole battleground for data breach cases. This is particularly true where a successful motion to dismiss in federal court may merely lead to the case being remanded back to state court if the case was initially filed in state court.[116] Instead, questions on the standard of care and the situations in which plaintiffs can obtain class certification are now the focus.

6. In light of the Third Circuit's decision in Horizon Healthcare Servs. Data Breach Litigation, defendants should expect a much greater post-breach focus on organizations that may be deemed to be "credit reporting agencies" pursuant to the FCRA.

---

113. See *Dittman*, 2017 Pa. Super. 8 (affirming lower court ruling that employers do not have a general duty to secure PII, and the economic loss rule applied); *Longenecker-Wells v. Benecard Serv.*, 658 Fed. App'x 659, 661-662 (3rd Cir. 2016) (breach of employer computer system case, affirming lower court's dismissal of claims on basis of economic loss rule, and finding failure to state cause of action for implied contract to safeguard PI); see also *In re Lenovo Adware Litig.*, No. 15-md-2624, 2016 U.S. Dist. LEXIS 149958, at *36-39 (N.D. Cal. Oct. 27, 2016) (in data misuse case, court applies economic loss rule to bar negligence claims under New York and California law for negligence).

114. *In re Barnes & Noble Pin Pad Litig.*, 2016 U.S. Dist. LEXIS 137078, at *25; *Patton*, 2016 U.S. Dist. LEXIS 60590 (granting motion to dismiss for failure to allege that alleged breach led to any unlawful access of PI).

115. But see *Longenecker-Wells v. Benecard Serv.*, 658 Fed. App'x at 661-662 (3rd Cir. Aug. 25, 2016) (applying economic loss rule even where no written contracts are at issue).

116. See e.g., *Bradix*, 2016 U.S. Dist. LEXIS 87368; *Khan*, 2016 U.S. Dist. LEXIS 66404, at *15-16; also *Patton*, 2016 U.S. Dist. LEXIS 60590; but see *Benton v. Clarity Serv.*, No. 16-cv-6583, 2017 U.S. Dist. LEXIS 10537 (N.D. Cal. Jan. 24, 2017) (in FCRA case, court refusing to remand FCRA cause of action to state court).

B. Product (Data) Defect Litigation: The Next Frontier?

In 2016, Plaintiffs filed a number of product defect cases based on alleged software vulnerabilities, alleging that businesses breached their promises to consumers because the products were susceptible to cyber attacks.[117] These cases have been initiated mostly by plaintiffs' firms responsible for data breach class actions, hoping to use favorable rulings from one type of case for the other.

Nonetheless, such product defect cases face numerous obstacles. For example, in mid-2016 the Ninth Circuit affirmed a district court's dismissal of a consumer class action against Symantec, in which the plaintiffs alleged that Symantec hid an antivirus software defect that exposed users to cyber attacks.[118] The appellate court openly criticized the lack of specificity in the appellants' fraud allegations, and that the cause of action on "implied contract" failed to allege contract formation and receipt of money by Symantec.

Recycling the same theory, Plaintiffs are also hoping for reversal by the Ninth Circuit of their claims against three car manufacturers based on the "hackability" of their connected cars, where the lower court had dismissed the case because "plaintiffs do not allege that any consumer, outside the realm of controlled experiments, has ever been a victim of vehicle hacking"[119]

These "product defect cases" will need to be carefully monitored due to their potential effect on data breach litigation, where plaintiffs typically argue that the defendant failed to follow its own promises of cybersecurity, thereby allegedly committing fraud or breaching some "implied contract," despite the lack of out-of-pocket damages. As the world becomes increasingly data-dependent, it will be interesting to watch whether security becomes a marketing point for connected technologies such as IoT. Particularly where a "promise" on security often becomes the basis for various contract and quasi-contract causes of action,[120] companies will need to more carefully vet consumer-facing documents.

C. Other Litigation Arising From Data Breaches

In addition to product liability litigation, cyber vulnerabilities have led to litigation between business partners and shareholder derivative actions. Although there have been a handful of derivative actions filed thus far on the basis of data breaches, none have yet to be successfully brought against the directors and officers of the breached organization.[121]

On the other hand, a multitude of claims may arise between business partners and their vendors. Most of such litigation between businesses have thus far been resolved on the force of the contracts between them, even when Payment Card Industry (PCI) rules applied – whether by way of settlement or in front of the courts.[122]

D. Data Misuse Litigation: Where Technicalities Matter

Compared to data breach cases, there is arguably greater disparity amongst the data misuse cases. Even where data collection is an essential part of the service provided, and where such practices are arguably covered by the terms and conditions of the service, plaintiffs continue to use creative legal theories of liability against organizations that rely on data as a part of their businesses.

The cases in this section are divided into different types of "common practices":

1. Cases on Web and Online Tracking and Aggregation

Most data misuse cases have lagged for years in the courts. Some of these cases still involve data analytics and advertising

117. See e.g., Steven Trader, *Drivers in Fiat Car Hacking Suit Say Their Injuries Are Real*, Law360 (Mar. 22, 2016), https://www.law360.com/articles/774475/drivers-in-fiat-car-hacking-suit-say-their-injuries-are-real (on hackable car case, *Flynn v. FCA US LLC*, No. 15-00855 (S.D. Ill. 2016)); see also Cara Salvatore, *ADT Says Alarm Hackability Suit Fails For Lack of Examples*, Law360 (June 6, 2016), https://www.law360.com/articles/804130/adt-says-alarm-hackability-suit-fails-for-lack-of-examples (on hackability of home security services, Def.'s Mot. to Dismiss, *Edenborough v. ADT LLC,* No. 16-02233 (N.D. Cal. June 3, 2016).

118. *Haskins v. Symantec Corp.*, 654 Fed. App'x 338 (9th Cir. 2016).

119. Emily Field, *GM Urges 9th Cir. to Put Brakes On Car Data Hacking Suit*, Law360 (Sept. 29, 2016), https://www.law360.com/articles/846398/gm-urges-9th-circ-to-put-brakes-on-car-data-hack-suit (reporting on hackable car case, *Cahen v. Toyota Motor Corp.*, No. 16-15496 (9th Cir. 2016)).

120. See ongoing cyber-based product defect cases which all include contract-based claims, such as *Cheatem v. ADT*, D. Az. Case No. 15-02137; *In re VTech Data Breach Litig.*, E.D. Ill. Case No. 15-10889; *Edenborough v. ADT*, N.D. Cal. Case No. 16-02233.

121. See e.g., Order, *Davis v. Steinhafel*, D. Minn. Case No. 14-203, ECF 88 (July 7, 2016) (dismissing claims against board of directors of Target Corporation).

122. See e.g., *Schnuck Markets v. First Data Merchant Servs. Corp.*, No. 15-3804, 2017 U.S. App. LEXIS 809 (8th Cir., Jan. 13, 2017) (affirming liability cap despite PCI rules, based on contract between market and merchant bank); see also *Community Bank of Trenton v. Schnuck Mkts.*, Inc., 2016 U.S. Dist. LEXIS 133482 (S.D. Ill. Sept. 28, 2016) (dismissing tort causes of action in grocer breach, including negligence and negligence per se, and refusing to follow cases such as *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304 (D. Minn. 2014)).

for a more "classic" online environment, although mobile technologies have required companies to evolve and find new advertising solutions. Nonetheless, keeping track of cases on more traditional technologies will be important, as they will inevitably serve as precedents to guide courts dealing with the mobile and IoT environment:

- For Online Gaming – In *Carlsen v. Gamestop, Inc.*, 8th Cir. Case No. 15-2453, plaintiffs alleged that Gamestop improperly shared PII with Facebook, through Gamestop using Facebook's software development kit (SDK) on its "Gameinformer" website, in contravention of its own privacy statements. While the court found the allegations of the breach of the privacy statement sufficient to permit plaintiff to survive an Article III challenge, the court also found that the same privacy policy was unambiguous and it barred the main causes of action.[123] *Carlsen* teaches that a well-written consumer-facing privacy statement requires a careful examination of all third-party technologies.

- For Online Gaming – In *Vigil v. Take-Two Interactive Software*, S.D.N.Y. Case No. 15-8211, plaintiff alleged that a basketball video game captured, stored, and disseminated face geometry in open internet multi-player mode without consent. In granting the motion to dismiss for failure to show damages, the court found that the language of "any aggrieved party" under the Illinois Biometric Information Protection Act (BIPA) requires a showing of damages. Where the avatars were created for multi-player play, the intended play and terms and conditions demonstrate that there was no harm as contemplated by BIPA.[124] The Court likened *Vigil* to be more akin to a case involving excessive first-party use of PI, as opposed to an impermissible disclosure of PI to third parties.[125]

- For Online Media – In *Boelter v. Advance Magazine Publishers (Condé Nast)*, S.D.N.Y. Case No. 15-05671, plaintiffs alleged that publisher Condé Nast sold customer PI in the form of "personal reading information" without consent, in contravention of Michigan's Preservation of Personal Privacy Act (PPPA). The court denied the company's motion to dismiss, arguing that plaintiffs had sufficiently alleged for standing purposes that the PPPA may require customer consent when Condé Nast combines and recombines customer PI with third party data and analytics because the recombination of PI requires the data to be exposed to third parties.[126]

- For Video and Streaming – In re *Nickelodeon Consumer Privacy Litigation*, 3rd Cir. Case No. 15-1441, plaintiffs alleged that Viacom and its advertising partner Google violated the Video Privacy Protection Act (VPPA) on Nick.com by tracking users, including their IP addresses and "browser fingerprints," and combining such information with other PI. In both affirming and reversing the district court's rulings on a motion to dismiss, the Third Circuit held that: (1) although the court takes an open view toward what may be PI, IP addresses and browser fingerprints, even when they can be combined and recombined to form information about individuals, were not PI for the purposes of the VPPA; (2) the VPPA prohibits certain disclosures by "video tape service providers," and not the recipients (i.e., Google and its ad-network); (3) for the other causes of action at issue where consent is a defense, the fact that children may be at issue does not prohibit consent from being asserted; and (4) the court advised that companies think more carefully about their disclosures.[127] (But see *Yershov v. Gannett Satellite Info. Network, infra*, in Section III(D)(2), Cases on Mobile Tracking and Aggregation.)

- For Video and Streaming – In a pair of cases, *Braitberg v. Charter Communications,* 8th Cir. Case No. 14-1737 and *Gubala v. Time Warner Cable, Inc.*, 7th Cir. Case No. 16-2613, the two Circuit Courts held that where broadband allegedly kept CPNI after the closure of customer accounts, there must be economic injury, which is lacking where there is no allegation that defendants disclosed the CPNI to third parties.[128]

- For Video and Streaming – *In re Vizio, Inc., Consumer Privacy Litigation*, C.D. Cal. Case No. 16-02693, involves a consolidated complaint alleging impermissible aggregation by Vizio through its smart television offerings. A ruling on defendants' motion to dismiss is expected shortly.

- For Website Data and Advertisement Exchanges – *In re Facebook Privacy Litigation*, N.D. Cal. Case No. 10-02389, involves allegations that Facebook shared PI in the form of referrer-headers (via hyperlinks) in contravention of their own privacy statements. Although the court allowed plaintiffs to survive a motion to dismiss on the basis of the Ninth Circuit doctrine of "nominal damages" (as differentiated from demonstrable damages),[129] the court later denied class certification due to the lack of predominance in how referrer header

123. *Carlsen v. Gamestop, Inc.*, No. 15-2453, 2016 U.S. App. LEXIS 14999, at *14 (8th Cir. Aug. 16, 2016).
124. *Vigil v. Take-Two Interactive Software*, No. 15-cv-8211, 2017 U.S. Dist. LEXIS 12295, at *50 (S.D.N.Y. Jan. 30, 2017).
125. *Id.* at *25.
126. *Boelter v. Advance Magazine Publishers (Conde Nast)*, No. 15 Civ. 5671, 2016 U.S. Dist. LEXIS 134484 (S.D. N.Y. Sept. 28, 2016).
127. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3rd Cir. 2016).
128. *Gubula v. Time Warner Cable, Inc.*, No. 16-2613, 2017 U.S. App. LEXIS 1058, at *4 (7th Cir. Jan. 20, 2017) (holding that the Cable Communications Policy Act requires actual injury because it uses the term "aggrieved"); *Braitberg v. Charter Commc'ns.*, No. 14-1737, 2016 U.S. App. LEXIS 16477 (8th Cir. Sept. 8, 2016) (finding no concrete injury).
129. *In re Facebook Privacy Litig.*, No. 10-cv-2389, 2016 U.S. Dist. LEXIS 84766, at *17-20 (N.D. Cal. Jun. 28, 2016). But see *Svenson v. Google, Inc.*, *infra*.

information may have been altered and deleted when "shared" (i.e., when clicked).[130]

- For Website Data and Advertisement Exchanges – The Supreme Court refused to take up the appeal in *In re Google Cookie Placement Consumer Privacy Litigation*.[131] The Third Circuit had dismissed all causes of action against Google for its use and alleged impermissible installation of cookies, except for a singular California "invasion of privacy claim" that would have likely not been certifiable for class purposes. The lower court had dismissed plaintiff's other claims for violation of the federal wiretap statute (where Google was allegedly a party to the communication), the Stored Communications Act (SCA) (for lack of a "protected facility"), and the Computer Fraud and Abuse Act (CFAA) (for lack of "damage" or "loss").[132]

- For Website Data and Advertisement Exchanges – In *Facebook, Inc. v. Power Ventures*, 9th Cir. Case No. 13-17102, Facebook sued Power Ventures (a social media aggregator), which scraped data using user credentials which its users (also Facebook users) provided. Facebook alleged that Power Ventures thereby contravened its agreement with Facebook when it used these credentials to "scrape" Facebook's website. On appeal, the Ninth Circuit reversed the lower court in part and affirmed in part. Most notably, the court found that there might be CFAA violation where (a) Facebook incurs damages by having to spend time to "respond to an offense, conducting a damages assessment, and restoring the data, program, system, or information…," and (b) Facebook expressly told Power Venture that it had violated its terms and conditions for access.[133] The court noted, however, that the mere violation of Facebook's terms and conditions, without more, cannot be the basis for a CFAA claim.[134]

- For Website Data and Advertisement Exchanges – There are two cases involving Facebook's advertising network that should be carefully watched in 2017. In In re *Facebook Internet Tracking Litigation*, N.D. Cal. Case No. 12- 02314, plaintiffs allege that Facebook continues to impermissibly track users after they log off, using cookies and web pages with Facebook "like" and "share" buttons. In *Smith v. Facebook, Inc.*, N.D. Cal. Case No. 16-01282, plaintiffs allege that Facebook, through various online sites, impermissibly tracked users and contravened privacy policies and the Health Insurance Portability and Accountability Act (HIPAA). Important rulings for both cases are expected in 2017.

2. <u>Cases on Mobile Tracking and Aggregation</u>

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

- For APIs and SDKs – In *Henson v. Turn, Inc.*, N.D. Cal. Case No. 15-01497, plaintiffs alleged that Turn, a mobile advertisement exchange platform on the demand-side, impermissibly tracked users in contravention to its web privacy policy, because Turn continued to track via mobile applications and use the mobile carrier's identification technologies. The Court granted Turn's motion to compel arbitration based on plaintiffs' subscription contract with the mobile carrier, pointing out that third party beneficiaries to arbitration provisions are permissible under New York and California law.[135] (See also *infra*, Section IV, Regulatory Enforcement Actions.)

- For Mobile Ecosystems – In *Opperman v. Path, Inc.*, N.D. Cal. Case No. 13-00453, plaintiffs alleged that while the owner of the operating system cared deeply about the security of its devices and the privacy of its users, its partners and application developers improperly accessed end-users' PI and private address books. First, where the claim for intrusion upon seclusion was against the main developer Path, and the claim for "aiding and abetting" was against the ecosystem owner, the court certified the class on the basis of a unique interpretation of "nominal damages" under California law.[136] (But see *Svenson v. Google*, *Inc., infra*.) Second, on developer Yelp's motion for summary judgment, the court held that: (a) "[i]t is unclear whether hyperlinked, off-screen terms in the Privacy Policies provided users with constructive notice such that they could effectively consent to anything contained off-screen. In fact, Ninth Circuit precedent suggests otherwise…";[137] and (b) accessing an end-user contact list by uploading it to a remote

130. *In re Facebook Privacy Litigation*, No. 10-cv-2389, 2016 U.S. Dist. LEXIS 119293, at *26-31 (N.D. Cal. Sept. 2, 2016).
131. *Gourley v. Google, Inc.*, 137 S. Ct. 36 (2016).
132. *In re Google, Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3rd Cir. 2015).
133. *Facebook, Inc. v. Power Ventures, Inc.*, Nos. 13-17102 & 13-17154, 2016 U.S. App. LEXIS 21944, at *14-17 (9th Cir. Dec. 9, 2016).
134. *Id.* at *16-17 ("[o]nce permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability").
135. *Henson v Turn, Inc.*, No. C 15-1497, 2016 U.S. Dist. LEXIS 49138, at *7-8 (N.D. Cal. Mar 14. 2016).
136. *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 92403, at *49-51 (N.D. Cal. July 15, 2016).
137. *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 122578, at *24 (N.D. Cal. Sept. 8, 2016).

server and accessing it locally on the mobile device may be materially different for the purposes of "community norms of privacy" for an invasion of privacy claim.[138] *Opperman* is an important case because plaintiffs' allegations have relied heavily on the alleged differences in statements made to end-users about their privacy by different players in the same mobile ecosystem.

- For Mobile Ecosystems – In *In re Lenovo Adware Litigation*, N.D. Cal. Case 15-02624, plaintiffs allege that Superfish's "VisualDiscovery" software for targeted advertising and analytics were installed on various laptop devices. Plaintiff alleges two groups of plaintiffs: one class for unauthorized access claims (*e.g.*, for CFAA, federal wiretapping, Cal. Invasion of Privacy Act (CIPA)), and a second class for consumer protection claims based on state statutes. In October 2016, both a motion to dismiss and a motion for class certification were decided. Although the motion to dismiss was only granted in part, the court found that as to the wiretap claim, the hardware manufacturer cannot generally be liable secondarily for an application it did not design or run.[139] On the motion for class certification, the court declined to certify a class of "direct purchasers (from the manufacturer)" from outside of California, due to too many individualized questions as to whether unauthorized access had actually occurred – particularly where at least 10% of users uninstalled Superfish's Visual Discovery software immediately.[140] Amongst cases involving alleged "spyware," this case is promising for defendants due to its focus on individualized questions regarding actual access and installation.

- For Mobile Ecosystems – In *Svenson v. Google, Inc.*, N.D. Cal. Case No. 13-04080, plaintiff alleged that Google impermissibly shared contents of Google Wallet to third parties such as YCDroid, contravening its own privacy statements. After denying a motion to dismiss in 2015,[141] the court granted Google summary judgment in late 2016, on the remaining claims for breach of contract and unfair business practices. The court made a number of rulings which will have important implications for both data misuse and breach cases, including that: (1) there was no evidence that YCDroid actually accessed the PI at issue, (2) benefit of the bargain damages requires a showing of actual as opposed to theoretical access,[142] (3) an award of "nominal damages" requires an actual showing of damages, citing to *Opperman v. Path, Inc.*, *supra*.[143] The court concurrently denied class certification.[144] *Svenson* is particularly important in that it cleared up the requirements for a request for "nominal damages" to be feasible in California.

- For Mobile Videos – In *Yershov v. Gannett Satellite Info. Network, Inc.*, 1st Cir. Case No. 15-1719, plaintiffs alleged that Gannett violated the VPPA by sharing with Adobe user-PI obtained through its video application in exchange for data analytics and online advertising services. In reversing the district court's granting of a motion to dismiss, the First Circuit found that GPS coordinates of users' mobile devices were PI of the users.[145]

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

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

- For Real Time Beacon Tracking – Two cases being closely watched are *Satchell v. Sonic Notify, Inc.*, N.D. Cal. Case No. 16-04961 and *Rachermann v. Lisnr*, D. Mass. Case No. 16-12326, which allege the improper real-time geo-tracking using Bluetooth and audible beacons in conjunction with sports applications while in the team stadiums.

- For New Kinds of Technologies and Use of Identifiers – In *In re Facebook Biometric Information Privacy Litigation*, N.D. Cal. Case No. 15-3747, plaintiffs alleged that "tag suggestions" on Facebook is data collection of "facial geometry" biometric data without their consent, and therefore contrary to BIPA. While the user agreement provided for application of California law, the court noted that California has generally erred on the side of the enforceability of "clickwrap" agreements as opposed to "browserwrap" (where the user is forced to go through all terms before he can click "I agree").[146] The court denied summary judgment for Facebook and refused on the basis of public policy to apply the choice of law to preclude the applicability of Illinois law.[147] The court also denied Facebook's motion to dismiss on the basis that allegations of Facebook's technology using "face geometry," if taken as true, would be covered by BIPA.[148]

138. *Id* at *22, *41.
139. *In re Lenovo Adware Litig.* No. 15-md-2624, 2016 U.S. Dist. LEXIS 149958, at *30-32 (N.D. Cal. Oct. 27, 2016).
140. *Id.* at *64, *68-69.
141. *Svenson v. Google, Inc.,* No. 13-cv-4080, 2015 U.S. Dist. LEXIS 43902 (N.D. Cal. Apr. 1, 2015).
142. *Id.* at *17.
143. *Id.* at *17-18.
144. *Id.* at *31.
145. *Yershov*, 820 F.3d 482.
146. *In re Facebook Biometric Info. Privacy Litig.*, No. 15-c-3747, 2016 U.S. Dist. LEXIS 60046, at *22-23 (N.D. Cal. May 5, 2016).
147. *Id.* at *35-36.
148. *Id.*, at *40-41.

- For New Kinds of Technologies and Use of Identifiers – In *McCollough v. Smarte Carte, Inc.*, N.D. Ill. Case No. 16-03777, plaintiff alleged that defendant's "smart (public) lockers" collected and retained fingerprints without any disclosures whatsoever, in contravention of BIPA. In granting defendant's motion to dismiss based on lack of Article III standing, the court noted that despite the lack of a consumer-facing privacy statement and written consent, as arguably required by BIPA, the statute requires actual harm due to its use of the term "[a]ny person aggrieved," and the plaintiff only alleges first-party misuse, not disclosures to a third party.[149]

- For New Kinds of Technologies and Use of Identifiers – In *Martinez v. Snapchat, Inc.*, C.D. Cal. Case No. 16-05182, plaintiff tried to avoid an Article III standing challenge by filing first in state court, alleging that Snapchat's "lenses" feature violated BIPA by impermissibly collecting and storing user facial templates. Plaintiff attempted to get the case remanded back to state court by alleging that Snapchat must concede that plaintiff had Article III standing to keep the case in federal court. The court disagreed, finding no such obligation by defendants in law, thereafter denying the motion for remand.[150]

- For New Kinds of Technologies and Use of Identifiers – In *Cole v. Gene by Gene*, D. Ala. Case No. No. 14-0004, plaintiffs allege that defendant genetics testing company impermissibly shared genetics testing information with third-party community administrators of "projects" to connect to the same genetic tree, in violation of the Alaska Genetic Privacy Act. Currently, cross-motions for dismissal and class certification are pending.

4. Cases on Email and Message Scanning

Despite having enjoyed some success in getting past motions to dismiss, plaintiffs alleging the improper scanning of emails and peer-to-peer messages within applications (*e.g.*, for marketing purposes) are still having difficulty obtaining class certification. For example, in *Campbell v. Facebook, Inc.*, N.D. Cal. Case No. 13-5996, plaintiffs alleged improper scanning of messages between Facebook users, and the court denied the Fed. Rules of Civ. Proc., Rule 23(b)(3) class, due to the difficulty of ascertaining damages.[151] Similarly, in *Corley v. Google, Inc.*, N.D. Cal. Case No. 16-00473, where plaintiffs alleged that Google was scanning student emails for marketing purposes, the court granted a motion for severance between the class members because the privacy policies and disclosures amongst universities could have differed substantially.[152]

One of the most notable cases on the interception of emails is *Luis v. Zang*, 6th Cir. Case No. 14-3601. In *Luis*, the plaintiff brought wiretapping claims not only against her husband but also against Awareness Technologies, a software company that designed a product named "WebWatcher" for the purpose of intercepting emails. In holding Awareness liable for the spouse's interception of emails, the court held that a company that intentionally builds a tool for wiretapping may itself be liable for wiretapping.[153]

5. Lessons Learned

As the data misuse cases of 2016 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:

a. 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*, such as 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. Nonetheless, at least one court has indicated that it is open to holding platform owners potentially liable for "aiding and abetting" alleged privacy violations by its third-party developers, even if owners received repeated assurances of compliance.[154]

Instead of assessing privacy statements in isolation, courts are also looking at what users may expect across a defendant's entire line of potentially applicable products.[155] Furthermore, courts may take into consideration how the privacy statements of third parties affect user expectations. In *Opperman v. Path,*

149. *McCollough v. Smarte Carte, Inc.*, No. 16 C 3777, 2016 U.S. Dist. LEXIS 100404 (N.D. Ill. Aug. 1, 2016).
150. *Martinez v. Snapchat, Inc.*, No. 16-cv-5182, 2016 U.S. Dist. LEXIS 113382, at *2 (C.D. Cal. Aug. 24, 2016).
151. *Campbell v. Facebook, Inc.*, No. 13-cv-5996, 2016 U.S. Dist. LEXIS 66267, at *47-50 (N.D. Cal. May 18, 2016).
152. *Corley v. Google, Inc.*, 316 F.R.D. 277, 286-287 (N.D. Cal. 2016).
153. *Luis v. Zang*, No. 14-3601, 2016 U.S. App. LEXIS 15003, at *40-41 (6th Cir. Aug. 16, 2016).
154. See *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 92403, at *51 (N.D. Cal. July 15, 2016) (partially granting class certification against Apple, on basis of aiding and abetting theory and for "nominal damages").
155. See, *e.g.*, *Svenson v. Google, Inc.*, No. 13-cv-4080, 2015 U.S. Dist. LEXIS 43902 (N.D. Cal. Apr. 1, 2015) (denying motion to dismiss where plaintiffs argued that Google Wallet's privacy policy should be considered in conjunction with Google's general privacy policy); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 982-983 (N.D. Cal. 2015) (denying defendants' motions to dismiss, partially on basis of Apple's advertising campaign regarding privacy).

Inc., for example, the court denied defendants' motions for summary judgment and dismissal, finding triable issues of fact as to whether there were "effective" and consistent privacy statements from the platform owner to the third-party application developers.[156]

On the other hand, different but interacting ecosystems may be used to defeat class certification. In *Corley v. Google, Inc.*, for example, student plaintiffs alleged that Google impermissibly scanned their emails for targeted advertising purposes. The court granted Google's motion for severance, finding that the different privacy policies provided by and through the universities raised viable defenses based on consent and that individualized inquiries may be necessary.[157]

Another example can be found in *In re Facebook Privacy Litigation*, where plaintiffs alleged that Facebook disclosed URL-headers containing Facebook IDs to third parties, which would allow third parties to re-identify users, in contravention to Facebook's privacy policy. After permitting the case to proceed past motions to dismiss, the court denied plaintiffs' motion for class certification, finding lack of ascertainability because different technologies on the user side may affect whether the URL-header information was available at all to third parties.[158]

b. 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 thereafter.

For example, in *In re Nickelodeon Consumer Privacy Litigation*, plaintiffs claimed that Viacom permitted third parties to advertise and install third party cookies, which then tracked the user through the Doubleclick advertisement network. The Third Circuit found that the allegations against Viacom for intrusion upon seclusion were sufficient to survive its motion to dismiss, based on the allegations in the Complaint that Viacom had made certain promises to parents regarding the tracking of children.[159]

In re Nickelodeon Consumer Privacy Litigation suggests that hosting organizations must carefully assess how advertising partners use their space and applications to advertise. Smaller and less reputable advertisers may be particularly aggressive in how they use banner space, and owners may inadvertently lose control over their own space and product to third party piggybacking.

Similarly, 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.[160]

c. Strong Defenses Require More Refinement 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 should consider the following:

- Disclosure and consent remain the most powerful defense for businesses leveraging data collection and analytics.[161] As demonstrated herein, courts are more carefully assessing the adequacy of disclosures.[162] They are more skeptical of the generalized disclosures that dominated the market years before. When possible,

156. *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 122578, at *22-25 (N.D. Cal. Sept. 8, 2016) (denying motion for summary judgment filed by Yelp, finding triable issues of fact as to whether Yelp's privacy statement was "effective").
157. *Corley v. Google, Inc.*, 316 F.R.D. 277, 286 (N.D. Cal. 2016) (in case alleging that Google impermissibly scanned student emails, granting motion to sever, finding that privacy statements may provide viable defenses based on consent, but requiring individualized analysis); contrast with *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 92403, *supra*.
158. *In re Facebook Privacy Litig.*, No. 10-cv-2389, 2016 U.S. Dist. LEXIS 119293, at *25-31 (N.D. Cal. Sept. 2, 2016) .
159. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 294-295 (3rd Cir. Jun. 27, 2016) .
160. See, *e.g.*, *Carlsen v. Gamestop, Inc.*, 833 F.3d 903 (8th Cir. 2016) (finding no viable privacy violation alleged, in case alleging that Gamestop violated its own privacy statement by sharing data through the Facebook SDK integrated into Gamestop's "Game Informer" website).
161. See, *id.* (finding no violation in case alleging Gamestop shared PI with Facebook, in contravention of Gamestop's privacy statement); see also *In re Lenovo Adware Litig.*, No. 15-md-2624, 2016 U.S. Dist. LEXIS 149958, at *63-64 (N.D. Cal. Oct. 27, 2016) (granting class certification, while also noting that implied consent may have created individualized questions); see also *Corley v. Google, Inc.*, 316 F.R.D. 277, 286 (N.D. Cal., 2016) (finding that some privacy statements of Google may show consent to scanning of emails for targeted advertising); also *In re Sling Media Slingbox Advert. Litig.*, No. 15-cv-5388, 2016 U.S. Dist. LEXIS 112240 (S.D.N.Y. Aug. 12, 2016) (finding no violation in case alleging that Slingbox violated its own privacy statements with in-stream advertisement).
162. *Opperman v. Path, Inc.*, No. 13-cv-453, 2016 U.S. Dist. LEXIS 122578, at *22-25 (N.D. Cal. Sept. 8, 2016) (discussing "effective" consent).

businesses should try to be as specific as possible regarding their data practices.

- 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.[163] Organizations need to do a better job of strong data classification and mapping (internally and 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.

- In an environment where motions to dismiss are unlikely to be granted, creating a record of the consent process throughout the ecosystem may help organizations defeat class certification. Individualized user experiences were at issue in the cases wherein Google and Facebook defeated class certification.[164] A well-crafted user interface that tactfully obtains consent throughout the process should help organizations create a better record of individualized experiences and how different sets of data were actually collected and used.

163. See e.g., *Svenson v. Google, Inc.*, No. 13-cv-4080, 2015 U.S. Dist. LEXIS 43902, *supra*; *Opperman v. Path, Inc.*, 84 F.Supp.3d 962, *supra*.
164. *In re Facebook Privacy Litig.*, No. 10-cv-2389, 2016 U.S. Dist. LEXIS 119293, at *25-31 (N.D. Cal. Sept. 2, 2016); *Corley v. Google, Inc.*, 316 F.R.D. 277, 286 (N.D. Cal. 2016); see also *In re Lenovo Adware Litig.*, No. 15-md-2624, 2016 U.S. Dist. LEXIS 149958, at *63-64 (noting in dicta that implied consent may have created individualized questions).

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 for the last 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.

Regardless, regulatory wrath remains focused on the failure to use encryption, the absence of written security plans, and the lack of adequately disclosed privacy practices. Keeping track of recent developments will be critical in steering organizations safely away from the regulators as the legal environment increasingly tightens.

A. The Federal Trade Commission

In 2016, the FTC took action on a number of matters that should be of interest to technology companies and aggregators:

In re Gigats.com: In the FTC's first enforcement action against an education lead generator, Gigats.com agreed to settle charges that it was "pre-screening" job applications for hiring employers when it was gathering information for other purposes, including lead generation for post-secondary schools and career training programs. The FTC alleged that many of the job openings listed were actually not current, that information collected purportedly for the openings was never sent to the employers, and that applicants were directed to call "independent education advisors" who then recommended only schools and programs that had agreed to pay the defendants fees for consumer leads.[165]

- *In re Oracle (Java SE)*: In March 2016, following a public comments period, the FTC approved its December 2015 settlement with Oracle over charges that it allegedly deceived customers regarding the security of the Java Platform, Standard Edition (Java SE) platform.[166] According to the FTC, when customers installed certain updates to Java SE in approximately 2010 or later, they received assurances of security when Oracle knew but did not inform them that the "update" did not remove prior versions of Java SE. This case, along with *In re Henry Schein Practice Solutions*, *infra*, demonstrates that the FTC is continuing to provide guidance to the software security market of best practices through settlements.

- *In re Very Incognito Technologies, Inc., dba Vipvape*: In May 2016, the FTC settled its charges against Vipvape for misrepresenting that it was a participant in the Cross-Border Privacy Rules (CBPR) program between the Asia-Pacific Economic Cooperation (APEC) countries and the EU. The CBPR facilitates the transfer of PII between APEC and EU countries. The FTC alleged that Vipvape deceived consumers by stating on its website that it was certified under the CBPR program when in fact, it was not. This case shows that the FTC is placing increasing importance on demonstrating to the EU authorities that it intends to diligently enforce the various EU-sanctioned data transfer programs.[167]

- *In re Henry Schein Practice Solutions, Inc.*: In May 2016, the FTC settled its claims against a software company for dental practices for allegedly falsely advertising that its software "provided industry-standard encryption of sensitive patient information."[168] The move was somewhat surprising, considering that encryption standards remain hotly contested even within the industry – although the software company's encryption standards probably did not meet some of the standards for encryption.

- *In re InMobi*: In June 2016, the FTC settled a case with advertising network InMobi, over charges that it tracked users' geolocation without their permission. The FTC alleged that InMobi had misrepresented that its advertising software would track consumer's locations only when they opted in and in a manner consistent with their devices' privacy settings. The FTC alleged that InMobi, in fact, tracked consumers, including children, regardless of whether they opted

165. Press Release, FTC Charges Education Lead Generator With Tricking Job Seekers By Claiming to Represent Hiring Employers (Apr. 28, 2016), https://www.ftc.gov/news-events/press-releases/2016/04/ftc-charges-education-lead-generator-tricking-job-seekers.
166. Press Release, FTC Approves Final Order In Oracle Java Security Case (Mar. 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-approves-final-order-oracle-java-security-case.
167. Press Release, Hand-Held Vaporizer Company Settles FTC Charges It Deceived Consumers About Participation In International Privacy Program (May 4, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/hand-held-vaporizer-company-settles-ftc-charges-it-deceived.
168. Press Release, FTC Approves Final Order In Henry Schein Practice Solutions Case (May 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-approves-final-order-henry-schein-practice-solutions-case.

in or denied permissions in their settings, through their wifi and network-mapping.[169] As with the FTC's proceedings against Nomi Technologies last year,[170] *In re InMobi* will have important implications for IoT. Accurate real-time tracking requires a pervasive network with a variety of means to track consumers. But as organizations automate the way they collect data, when they have a wide affiliate-network with a variety of collection tools, accurately honoring opt-outs across the entire affiliate-network may be difficult.

- *In re LabMD*: In November 2015, an FTC administrative law judge found that the FTC presented insufficient evidence and failed to show "likely substantial consumer injury" against respondent LabMD for "unfair practices" under Section 5 of the Federal Trade Commission Act (the FTC Act) arising from an alleged data breach.[171] Undaunted, the FTC appealed the decision. On July 28, 2016, the Commission reversed the administrative judge's decision. In its findings, the Commission lessened what was required to show "likely substantial injury," arguing that despite the scant evidence of harm, "[i]t is well established that substantial injury may be demonstrated by a showing of a small amount of harm to a large number of people, as well as a large amount of harm to a small number of people."[172] LabMD has since appealed the opinion of the FTC commissioners to the federal courts, and a recent ruling in November 2016 on LabMD's motion to stay enforcement of the FTC decision suggests that LabMD may ultimately prevail.[173]

- *In re AshleyMadison.com*: In December 2016, the FTC worked with 13 state Attorneys General (AGs) to settle with the operators of AshleyMadison.com for the massive data breach arising from its website vulnerabilities that affected 36 million users. The agreement included a multi-million dollar settlement that depended on the financial condition of the company, in addition to an agreement to implement a comprehensive data security program. As part of its effort, the FTC also cooperated with the investigators of Canada and Australia for their own investigations.[174]

- *In re Turn, Inc.,*: In December 2016, the FTC settled with ad-tech company Turn over allegations that it continued to track end-users using network unique identifier headers and to target users with mobile application advertisements, even though its privacy policy represented to consumers that they could block targeted advertising by using their web browser's settings to block or limit cookies. The decision demonstrates that the FTC will use the broadest construction of the privacy "promises" possible, and that as in *In re InMobi*, organizations need to be careful of continued tracking and targeting of end-users that may happen inadvertently because the wide variety tools it may have in place to collect data and target consumers automatically.[175]

- *In re D-Link*: In January 2017, the FTC filed suit against D-Link for the alleged cyber-vulnerabilities of its home routers and connected cameras. However, there was no evidence that any consumer was actually harmed by the alleged vulnerabilities. Fueled by the lack of harm, the advent of the Trump Administration, and the momentum of the challenge presented by LabMD, D-Link has decided to challenge the enforcement action brought by the FTC.[176]

The recent victories of LabMD and the challenge brought by D-Link, amidst the arrival of the Trump Administration may incite more companies to challenge the FTC's authority to

169. Press Release, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.
170. Press Release, FTC Approves Final Order In Nomi Technologies Case (Sept. 3, 2015), https://www.ftc.gov/news-events/press-releases/2015/09/ftc-approves-final-order-nomi-technologies-case.
171. Initial Decision, *In the matter of Lab MD, Inc.*, Docket No. 9357 (Fed. Trade Comm'n Nov. 13, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf; and Press Release, Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc. (Nov. 19, 2015), https://www.ftc.gov/news-events/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint.
172. *In re the Matter of LabMD, Inc.*, Docket No. 9357, 2016 FTC LEXIS 128, at *25 (July 28, 2016); see also Gabriel Maldoff, *LabMD And The New Definition of Privacy Harm,* Daily Dashboard (IAPP, Aug. 22, 2016), https://iapp.org/news/a/labmd-and-the-new-definition-of-privacy-harm/ .
173. Melissa Daniels, *LabMD Wins Stay From FTC Order At 11th Circ. In Data Row*, Law360, Nov. 10, 2016), https://www.law360.com/articles/861892/labmd-wins-stay-from-ftc-order-at-11th-circ-in-data-row.
174. Press Release, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach That Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.
175. Press Release, Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online And Through Their Mobile Devices (Dec. 20, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively.
176. Dorothy Atkins, *Cause of Action Institute to Fight FTC In Privacy Row*, Law360 (Jan. 10, 2017), https://www.law360.com/articles/879573/cause-of-action-institute-to-fight-ftc-in-privacy-row.

bring "unfair practices" claims under Article 5 of the FTC Act, especially in the absence of actual consumer harm.

A number of other statements by the FTC in 2016 are noteworthy:

- In anticipation of increased use of audio recordings across devices, the FTC issued a warning letter in March 2016 to developers using "Silverpush" code, which utilizes software that can monitor a device's microphone to listen for audio signals that are embedded in television advertisements. Although Silverpush recently withdrew its business from the United States, the FTC reminded developers that if they stated or implied to consumers that they were not recording and collecting sounds, but in fact were, the developers would be in violation of the FTC Act, Section 5.[177]

- The FTC had indicated that simply complying with the NIST's Cybersecurity Framework may not be enough. In an August 2016 online posting in response to a number of questions about the Cybersecurity Framework, the FTC staff indicated that "[t]he Framework is not, and isn't intended to be, a standard or checklist."[178]

- In a luncheon audience at the Technology Policy Institute in Aspen, Colorado on August 29, 2016, former FTC Chairwoman Edith Ramirez continued to reiterate an expansive interpretation of what may be PII. In stating that information is PII when "it can be reasonably linked to a particular person, computer, or device," Ramirez said, "[i]n many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers meet this test." When confronted with the expansive definition, Ramirez indicated that the broadening was still commensurate with basic privacy principles.[179]

- In October 2016, the FTC released its "Data Breach Response: A Guide For Business."[180] Interestingly, although the guidance discusses that victims should hire legal counsel, there is very little discussion regarding the potential application of privilege if counsel is hired early. Instead, the guide suggests that victims should immediately report their findings – even preliminary and interim ones – to the authorities.[181] On the other hand, the guidance may be helpful in breach litigation, as it indicates that ID-protection may only need to be offered for one year.[182]

- 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.[183] 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."[184]

- Notably, it is unclear which of the FTC's statements and policies promulgated by the Obama Administration would 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."[185]

B. The Federal Communications Commission

The Telecommunications Act of 1996 was originally interpreted to exclude broadband internet services from the definition of "telecommunications service," which was regulated by the FCC. In 2015, it was held that a mobile broadband provider could be a regulated "carrier," and therefore, the Telecommunications Act also regulates the right of wireless carriers to use "customer proprietary network information (CPNI)."[186] In June 2016, an appellate court affirmed the

177. Press Release, FTC Issues Warning Letters to App Developers Using "Silverpush" Code (Mar. 17, 2016) https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.
178. Andrea Arias, *The NIST Cybersecurity Framework and the FTC,* FTC Business Blog (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.
179. Shaun Waterman, *FTC's Ramirez: New Tech's Complexity Leaves Privacy Basics Unchanged,* Fedscoop.com (Aug. 23, 2016), http://fedscoop.com/edith-ramirez-ftc-aspen-institute-august-2016.
180. https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.
181. *Id.* at p. 8-9.
182. *Id.* at p. 7.
183. 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 (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.
184. Allison Grande, *FTC's Smart-TV Privacy Settlement Unlikely to See An Encore,* Law360 (Feb. 7, 2017), https://www.law360.com/articles/889449.
185. 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.
186. Report and Order on Remand, Declaratory Ruling, and Order, *In the Matter of Protecting And Promoting the Open Internet,* FCC GN Docket No. 14-28 (Mar. 12, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf .

FCC's classification of broadband as a telecommunications service, thereby applying common carrier regulations to such services.[187]

Continuing to demonstrate its interpretation of Section 222 of the Communications Act of 1934, the FCC announced in March 2016 that it entered into $1.35 million consent decree with Verizon, for the carrier's alleged use of unique identifier headers (UIDH) in its networks and with its partners for targeted advertising. The FCC consent decree alleged that Verizon's UIDH persisted even after users tried to clear their cache of cookies or opted to not be tracked, causing some commentators to call the UIDHs "supercookies" or "zombiecookies."[188]

Although the FCC and FTC have at times publicly criticized each other for overstepping their respective jurisdictions, they have also been increasingly working together. For example, in June 2016, several self-purported privacy groups urged the FCC and FTC to investigate broadband providers and how they have been using data.[189] The requests followed the FCC's announcement in May 2016 that it was partnering with the FTC to investigate how companies were releasing mobile security patches.[190]

C. HIPAA Enforcement

The Office of Civil Rights (OCR) and Department of Health and Human Services (HHS) obtained a number of large settlements for alleged HIPAA violations in Spring 2016:

- Feinstein Institute For Medical Research – $3.9 million for allegedly allowing a laptop with sensitive information on about 13,000 people to be stolen from a car.[191]
- New York Presbyterian Hospital – $2.2 million for allegedly allowing crew members from ABC to film patients without their consent.[192]
- North Memorial Health Care System – $1.55 million for allegedly failing to take security precautions, which led to the disclosure of data of nearly 300,000 patients.[193]
- Raleigh Orthopedic Clinic – $750,000 for allegedly failing to secure a business associate agreement before handing patient data over to a potential business partner.[194]

Amidst these sizeable settlements, the OCR announced in March 2016 that it will begin its much anticipated "Phase 2 Audits." Over 200 audits were planned, the majority of which would be "desk (remote) audits" that would require a response within 10 days.[195] It remains to be seen how audited business associate relationships will fare, especially since they have only been covered by HIPAA since 2013.[196]

Subsequently, the Government Accountability Office (GAO) stated in a report in September 2016, that the HHS' HIPAA guidelines "fail" to address all of the requirements suggested by the NIST in its Cybersecurity Framework.[197] As a result, settlements with the HHS are larger than ever, with a number of noteworthy decisions in the third quarter of 2016:

- On June 24, 2016, the Catholic Health Care Services of the Archdiocese of Philadelphia agreed to pay $650,000 to HHS for the theft of an unencrypted mobile device that allegedly compromised the health information of hundreds of nursing home residents.[198]

187. Wendy Davis, *Court Empowers FCC to Address Broadband Privacy, Data Caps*, MediaPostPolicyBlog (Jun. 14, 2016) (on *US Telecom Ass'n v. FCC*, D.C. Cir. Case No. 15-1063, Order on June 14, 2016), http://www.mediapost.com/publications/article/278144/court-empowers-fcc-to-address-broadband-privacy-d.html.
188. Order, *In the Matter of Cellco Partnership, dba Verizon Wireless*, FCC File No. EB-TCD-14-00017601 (Mar. 7, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf.
189. Daniel Frankel, *Comcast, Cablevision and AT&T Violating Privacy Through Addressable Advertising, Groups Say*, FierceCable (Jun. 9, 2016), http://www.fiercecable.com/cable/comcast-cablevision-and-at-t-violating-privacy-through-addressable-advertising-groups-say.
190. Nick Statt, *The FCC And FTC Are Investigating How Companies Release Mobile Security Patches*, The Verge (May 9, 2016), http://www.theverge.com/2016/5/9/11641124/fcc-ftc-inquiry-mobile-security-patches-google-android.
191. Press Release, Improper Disclosure of Research Participants' Protected Health Information Results In $3.9 Million HIPAA Settlement (Mar. 17, 2016), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/feinstein/index.html.
192. John Kennedy, *NY Hospital Will Pay $2.2M For Violating HIPAA On TV*, Law360 (Apr. 21, 2016), https://www.law360.com/articles/786777/ny-hospital-will-pay-2-2m-for-violating-hipaa-on-tv.
193. Press Release, $1.55 Million Settlement Underscores The Importance of Executing HIPAA Business Associate Agreements (Mar. 16, 2016), https://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html.
194. Jeff Lagasse, *An Orthopedic Clinic Pays $750,000 Over HIPAA Violation Surrounding Improper Patient Data Sharing*, HealthcareITNews (Mar. 15, 2016), http://www.healthcareitnews.com/news/orthopaedic-clinic-pays-750000-over-hipaa-violation-surrounding-improper-patient-data-sharing.
195. U.S. Dept. Health & Human Servs., OCR Launches Phase 2 of HIPAA Audit Program, available at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html
196. Jeff Overley, *Feds Launch Long-Awaited HIPAA Audits*, Law360 (Mar. 21, 2016), https://www.law360.com/topnews/articles/774290/feds-launch-long-awaited-hipaa-audits.
197. Greg Slabodkin, *HHS Security, Privacy Guidance Said to Fall Short of Fed. Guidelines*, Health Data Management (Sept. 27, 2016), http://www.healthdatamanagement.com/news/hhs-security-privacy-guidance-falls-short-of-fed-guidelines.
198. Kat Sieniuc, *Catholic Nonprofit to Pay $650k Settlement In HIPAA Breach*, Law360 (Jun. 30, 2016), https://www.law360.com/articles/812714/catholic-nonprofit-to-pay-650k-settlement-in-hipaa-breach.

- On July 15, 2016, the Oregon Health & Science University (OHSU) agreed to pay the HHS $2.7 million for two breaches in 2013. The first incident involved an unencrypted laptop, and the second incident involved employees using an internet-based information storage system. Despite reporting no harm done to any of the patients allegedly at risk, OHSU was forced to pay one of the largest settlements in HHS history.[199]

- On July 25, 2016, the University of Mississippi Medical Center agreed to pay $2.75 million after the theft of an unencrypted laptop involving over 10,000 patient records.[200]

- On August 4, 2016, the Illinois Advocate Health Care Network entered into a $5.5 million consent decree with the HHS for three separate data breaches. This was the largest settlement in HHS history. The HHS alleged that Advocate failed to adequately assess risks to electronic personal health information (ePHI), failed to limit access, and failed to obtain a written agreement with a business associate to safeguard electronic information.[201]

- On September 23, 2016, the Care New England Health System agreed to hand nearly $500,000 in total to the HHS for allegedly losing unencrypted backup tapes containing approximately 14,000 women's ultrasound studies.[202]

- Following one of the largest civil settlements per patient in litigation history, on October 18, 2016, St. Joseph's Health agreed to pay more than $2.1 million to HHS for allegedly inadvertently allowing customer health records to be available online for more than a year.[203]

- On November 22, 2016, the HHS settled with the University of Massachusetts Amherst for $650,000 the impermissible disclosure of ePHI, and failure to implement adequate safeguards and a thorough analysis.[204]

- On January 18, 2017, the HHS fined MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) a whopping $2.2 million for the loss of a USB data storage device in 2011, followed by failure to implement corrective measures as it had previously promised the HHS.[205]

- On Feb. 1, 2017, the Children's Medical Center of Dallas agreed to pay a $3.2 million penalty for failing to properly secure electronic health records until after an unencrypted laptop with HIPAA information about nearly 2,500 people stolen from its building. The HHS' OCR found that the medical center loss included failure to comply with its prior recommendations to implement controls and encrypt data.[206]

As the cases demonstrate, the HHS has been demanding very large fines, regardless of whether it can show that any patient was actually harmed by the vulnerabilities. In fact, the HHS has only become increasingly aggressive, taking its first settlement for failure to timely notify against St. Joseph Medical Center in Illinois, in the amount of $475,000 in January 2017.[207]

---

199. Adam Lidgett, *Ore. Health System Pays $2.7M to Settle Data Breach Probes*, Law360 (July 15, 2016), https://www.law360.com/articles/818095/ore-health-system-pays-2-7m-to-settle-data-breach-probes.
200. Mollie Bryant, *UMMC to Pay $2.75 Million Fee In Federal Settlement*, Hattiesburg American (July 22, 2016), http://www.hattiesburgamerican.com/story/news/local/2016/07/22/ummc-pay-fee-federal-settlement/87463870/.
201. Jeff Overley, *Ill. Hospital Chain Inks Record $5.5M HIPAA Deal*, Law360 (Aug. 4, 2016), https://www.law360.com/articles/825148/ill-hospital-chain-inks-record-5-5m-hipaa-deal.
202. Kat Sieniuc, *New England Health System Fined By HHS Over Data Loss*, Law360 (Sept. 26, 2016), https://www.law360.com/articles/844688/new-england-health-system-fined-by-hhs-over-data-loss-.
203. Kat Greene, *St. Joseph to Pay $2.1M Over Leaked Patient Records*, Law360 (Oct. 18, 2016), https://www.law360.com/articles/852849/st-joseph-to-pay-2-1m-over-leaked-patient-records.
204. Brian Amaral, *UMass Settles HIPAA Violation Probe After Malware Attack*, Law360 (Nov. 23, 2016), https://www.law360.com/articles/865828/umass-settles-hipaa-violation-probe-after-malware-attack.
205. 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.
206. 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.
207. 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.

D. The Security Exchange Commission

Other regulators, however, may be even harsher than the FTC and HHS. In June 2016, the Security and Exchange Commission (SEC) announced that Morgan Stanley Smith Barney agreed to pay a whopping $1 million for allegedly failing to secure client information systems from improper access by employees over approximately 13 years, including one incident that resulted in the exposure of 730,000 accounts by an insider who had originally intended to compile "the world's best cold-call list."[208]

Then, the SEC fined a major investment bank for an internal breach in July 2016, although the FTC had refused to impose any fines. The SEC took issue with an employee uploading the information of more than 730,000 clients in 2014. But prior to the fine, the FTC had also investigated the same incident and found that the access was due to a system glitch for which it did not hold the bank responsible. In fact, the FTC found that the bank had "established and implemented comprehensive policies designed to protect against insider theft of personal information." Nonetheless, the SEC required that the bank pay $1 million by way of a settlement.[209]

Notably, as with the FTC and the HHS, the SEC has also taken the position that consumer harm may not be necessary for it to impose fines. In the April 2016 consent decree entered into between the SEC and Craig Scott Capital, the SEC fined the broker-dealer over $100,000 for its alleged failure to adopt written policies and procedures reasonably designed to ensure client security and confidentiality. No harm was noted, and the SEC pointed mostly to procedural failures such as client information appearing in employee private emails and accounts.[210]

E. Other Administrative Enforcement Efforts

In addition to the FTC, FCC, SEC, and the OCR/HHS, a number of other regulators are increasing their efforts in the data privacy arena.

The Consumer Financial Protection Bureau (CFPB) has begun to regulate privacy practices under Sections 1031 and 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. On March 2, the CFPB announced its first consent decree, for alleged "deceptive acts and practices relating to false representations regarding…data-security practices." The CFPB alleged that the respondent payment technology company had "(mis)represented to consumers that its network and transactions were 'safe' and 'secure,'" and that it was PCI-compliant.[211]

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 May 2016, Paypal settled with the Texas AG over allegations that its payment service, Venmo, improperly accessed user contact lists without sufficient disclosures to grow its user base. Paypal agreed to pay the Texas AG $175,000 and to provide more detailed disclosures.[212]
- On August 5, 2016, the New York AG entered into a $100,000 settlement with EZcontactsUSA.com. Most notably, the AG noted that EZcontactsUSA.com did not maintain a written security policy.[213]
- On September 13, 2016, a number of major companies hosting some of the web's most popular online content for children agreed to enter into a settlement with the New York AG. The AG indicated that the settlement was part of its "Operation Child Tracker" was a project that was "first-of-its-kind," where the AG sought to shut down practices by websites of allowing third-party vendors, such as marketers and advertising companies, to track users by "piggy-backing." Citing to the opinions of the FTC, the AG alleged that the websites illegally used cookies to track users, in addition to permitting third parties to insert their tracking technologies and third-party cookies, in violation of the Children's Online Privacy Protection Act (COPPA). The AG required that the companies adopt procedures to vet third-party tracking technologies, regularly monitor these third party activities, and provide clear notice mechanisms regarding the third parties in a manner compliant with COPPA. The action is significant for being one of the first

208. Jody Godoy, *SEC Fines Morgan Stanley $1M For Data Security Failures*, Law360 (Jun. 8, 2016), https://www.law360.com/articles/805026/sec-fines-morgan-stanley-1m-for-data-security-failures.
209. Maldoff, *'Not Unfair' May Still Be Unreasonable: The Ramifications of The SEC's Morgan Stanley Settlement*, IAPP (July 20, 2016), https://iapp.org/news/a/not-unfair-may-still-be-unreasonable-the-ramifications-of-the-secs-morgan-stanley-settlement/.
210. Press Release, Broker-Dealer and Principals Charged With Violations Related to The Protection of Confidential Customer Information And Use of Personal Email (Apr. 12, 2016), https://www.sec.gov/litigation/admin/2016/34-77595-s.pdf.
211. Consent Order, *In the Matter of: Dwolla, Inc.*, CFPB File No. 2016-CFPB-0007 (Mar. 2, 2016), http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.
212. Jeff John Roberts, *Venmo Likely Investigated Over User Privacy Violations*, Fortune (May 24, 2016), http://fortune.com/2016/05/24/venmo-investigation/.
213. Press Release, A.G. Schneiderman Announces $100k Settlement With E-Retailer After Data Breach Exposes Over 25k Credit Card Numbers (Aug. 5, 2016), https://ag.ny.gov/press-release/ag-schneiderman-announces-100k-settlement-e-retailer-after-data-breach-exposes-over.

to go after companies for their allowance of third-party cookies, tags, and frontline behavioral advertising.[214]

- On October 3, 2016, Juxta Labs entered into a consent decree with the Texas AG, for its alleged failure to implement sufficient screening and disclosure mechanisms regarding its privacy practices as to children. The state argued that its mobile application games and social media were too easy for children of any age to access and that it needed better disclosure and consent mechanisms. Juxta agreed to be fined $30,000 and consented to compliance.[215]
- On November 10, 2016, 15 state AGs settled with Adobe over the 2013 hack into Adobe's servers for $1 million.[216]
- On January 26, 2016, the New York AG entered into a settlement agreement for $115,000 with Acer for a debugging-mode vulnerability on its company website, which left customer PI vulnerable.[217]

Looking at the state AG landscape, it is important to note that the states of New York and Texas have been much more active with public enforcement actions than others. This was not always the case. Organizations doing business in active states need to take heed.

214. Press Release, A.G. Schneiderman Announces Results of "Operation Child Tracker," Ending Illegal Online Tracking of Children AT Some of Nation's Most Popular Kids' Websites (Sept. 13, 2016), https://ag.ny.gov/press-release/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online.
215. Jess Krochtengel, *App. Developer Boosts Privacy For Kids to End Texas' Claims*, Law360 (Oct. 4, 2016), https://www.law360.com/articles/848223/app-developer-boosts-privacy-for-kids-to-end-texas-claims.
216. Kat Sieniuc, *Adobe, State AGs Settle Data Breach Claims In $1M Deal*, Law360 (Nov. 10, 2016), https://www.law360.com/articles/861686/adobe-state-ags-settle-data-breach-claims-in-1m-deal.
217. 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.

V. NOTABLE INTERNATIONAL DEVELOPMENTS

A survey of the other parts of the world reveal how data privacy laws in the U.S. are still amongst the most technology-friendly, however burdensome they may seem at first blush.

A. Developments in the European Union

1. The EU General Data Protection Regulation (GDPR)

The biggest international announcement of 2016 is the final passage of the General Data Protection Regulation (GDPR), which replaces the 1995 Data Privacy Directive in its entirety.[218] Set to take effect in 2018, the GDPR should further standardize data protection across all EU member states. The following should be noted about the GDPR.

a. Privacy-Friendly Design

- PI should only be collected for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[219]
- Generally, processing of data will only be allowed with explicit consent, to perform a contract or legal obligation, to protect the vital interests of the data subject, to perform a task in the public interest, or (in very limited circumstances) "for the purposes of legitimate interests pursued by the controller or by a third party."[220]
- Consent can be revoked at any time and cannot generally be presented as "take it or leave it."[221]

b. Accounts for Emerging Technologies

- Data subjects have the right to object to "automated profiling" that "produces legal effects concerning him or her."[222]
- Genetic and biometric data are "sensitive personal data," which are subject to stricter rules (i.e., a general prohibition with exceptions).[223]
- Encryption and anonymization are encouraged – as is the use of pseudonyms where possible – as part of good data security practice.[224]

c. Timely Accessibility, Portability, and Erasure

- Data subjects have very broad rights to access and control data collected regarding them from the controller, regardless of whether the data is collected by the controllers or from third parties.[225]
- Controllers have to provide any information they hold about a data subject free of charge within one month of the request.[226]
- Data subjects have the right to control their data through the "right of erasure" and "right of rectification."[227]

d. Tighter Controls on Controller-Processor Relationships

- Increased obligations on data controllers, including more detailed contractual vendor controls.[228]
- Vendors may not subcontract the service without the consent of the controller.[229]

e. New Internal Control Requirements

- Data protection officers (DPOs) are often mandated, and DPOs shall enjoy independence and not be terminated for exercising their duties.[230]
- Increased use of privacy impact assessments.[231]

---

218. Commission Regulation 2016/679 of Apr. 5, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119), http://ec.europa.eu/justice/data- protection/reform/files/regulation_oj_en.pdf
219. *Id.* at Article 5(1)(b), Article 6.
220. *Id.* at Article 6(1).
221. *Id.* at Article 7(1), (3)-(4).
222. *Id.* at Articles 21-22.
223. *Id.* at Article 9.
224. *Id.* at Article 32.
225. *Id.* at Article 15.
226. *Id.* at Article 15(3).
227. *Id.* at Articles 16-17.
228. *Id.* at Articles 24-26, 29.
229. *Id.* at Article 29.
230. *Id.* at Article 37.
231. *Id.* at Article 35.

f. More Forceful Breach Requirements and Enforcement

- Notification must be provided for any data breach that creates significant risk for the data subjects within 72 hours of discovery.[232]
- Data protection authorities (DPAs) would be empowered to fine organizations up to 4% of their annual revenue.[233]

2. The New EU-U.S. "Privacy Shield"

On July 27, 2016, the Department of Commerce (DOC) International Trade Administration (ITA) finally released its Privacy Shield Website for U.S.-based organizations looking to enjoy the same protections that they previously enjoyed under the Safe Harbor program for EU-U.S. data transfers.[234] Signing onto the program, however, means that the applicant is assuring both the FTC and European authorities that they are now "obligated to provide at least the same level of protection (to European data subjects) as is required by the (European) Principles."[235]

Applicants are required to do the following:

1. Designate a corporate representative for "all things Privacy Shield";[236]
2. Provide detailed disclosures, including on third-party and automated processing. For example, disclosures include "the type or identity of third parties to which it discloses personal information and the process for which it does so";[237]
3. Account for more expansive definitions of "sensitive personal information," and adopt more requests for "affirmative express consent" per European law;[238]
4. Adopt specific requirements for "onward transfers" and third-party processors, which are increased accountability and documentation requirements for controllers,[239] including for when data is transferred to those who claim to be "mere processors";[240]
5. Permit subject access and rectification. Organizations will need to provide data subjects access to their data and implement free-of-charge means for data subjects to correct and amend their data (i.e., Europe's infamous "right to be forgotten") where appropriate;[241]
6. Agree to provide independent and free recourse mechanisms for disputing data subjects;[242] and
7. Commit to "cooperat(ing) with European Union data processing authorities (DPAs)."[243] The full meaning of "cooperation" remains to be seen, although, for employment data in an employment relationship, it appears that applicants will be subjecting themselves to the authority of the DPAs directly.[244] Notably, there are additional requirements for certain types of information and industries.[245]

Once applied, the Privacy Shield controls *immediately*. Applicants should keep in mind that compliance will only become even more rigorous with the EU's recent ratification of the GDPR.[246] And we note that the security policies of the

232. *Id.* at Articles 33(1).
233. *Id.* at Article 83(3).
234. https://www.privacyshield.gov/welcome.
235. US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles, (6) Self-Certification, Subsection (e): https://www.privacyshield.gov/article?id=6-Self-Certification.
236. US Businesses, How to Join Privacy Shield, Self Certification Information: https://www.privacyshield.gov/article?id=Self-Certification-Information.
237. US Businesses, Requirements of Participation, Privacy Shield Principles, (1) Notice: https://www.privacyshield.gov/article?id=1-NOTICE.
238. US Businesses, Requirements of Participation, Privacy Shield Principles, (2) Choice: https://www.privacyshield.gov/article?id=2-CHOICE.
239. US Businesses, Requirements of Participation, Privacy Shield Principles, (3) Accountability For Onward Transfers: https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER.
240. US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles, (10) Obligatory Contracts for Onward Transfers, Subsection (a): https://www.privacyshield.gov/article?id=10-Obligatory-Contracts-for-Onward-Transfers.
241. US Businesses, Requirements of Participation, Privacy Shield Principles, (8) Access: https://www.privacyshield.gov/article?id=6-ACCESS.
242. US Businesses, Requirements of Participation, Privacy Shield Principles, (7) Recourse, Enforcement, and Liability: https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY.
243. US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles, The Role of Data Protection Authorities: https://www.privacyshield.gov/article?id=5-The-Role-of-the-Data-Protection-Authorities-a-b.
244. US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles, (9) Human Resources Data, Subsection (e): https://www.privacyshield.gov/article?id=9-Human-Resources-Data.
245. See US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles, https://www.privacyshield.gov/article?id=Requirements-of-Participation.
246. See Press Release, Article 29 Working Party Statement on the decision of the European Commission on the EU-US Privacy Shield (July 26, 2016), available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

Trump Administration are likely to affect the future of the Privacy Shield program. In addition, there may also be effects from the ongoing litigation between the U.S. government and technology companies holding information on cloud. As of the date of this publication, there appears to be a split amongst the Circuits as to the enforceability of government subpoenas on data held in data centers outside of the United States.[247]

Regardless, although many organizations rushed to apply for the new "Privacy Shield" EU-U.S. safe harbor program, as to trans-Atlantic data transfers, the repercussions for U.S.-based companies are much larger than they first appear. Certain European "rights," such as the much debated "right to be forgotten" and the right to be free from "automatic profiling," are currently only required in very limited circumstances in the United States. By signing on to the Privacy Shield, multi-national companies are averring that in the near future, they will comply with the much more stringent European requirements on international data transfers, which have thus far stifled technology innovation in Europe. Especially for larger organizations, promising to follow the European requirements will require substantial technological overhauls that will cost hundreds of millions for compliance.

On the other hand, it is not clear that organizations based in the U.S. have reasonable alternatives. Model clauses appear to also be under challenge. The Max Schrems-led privacy group, responsible for bringing the *Schrems* case that eventually led to the invalidation of the E.U.-U.S. Safe Harbor program, has petitioned to the Irish Data Protection Commissioner to consider how model clauses also do not prevent mass surveillance by U.S. intelligence, and therefore should be invalidated. The Irish Commissioner recommended referral of the case to the Court of Justice of the European Union (CJEU).[248] As of the date of this publication, Google announced that its services' contractual clauses were approved by the Article 29 Working Party.[249]

3. The Draft ePrivacy Regulation

A proposed draft of EU's ePrivacy Regulation (the "ePrivacy Reg") was released in January 2017, demonstrating how EU will take on emerging connective technologies with a perspective dramatically different from the U.S.[250] 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/anonymization obligations absent consent.
- *Limits end-user data collection through the "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.
- *Reminds providers of end-user rights notwithstanding consent:* Article 9(3) reminds providers of end-user rights to withdraw consent and requires a reminder at periodic intervals of six months.
- *Specifies software privacy settings:* Article 10 requires that "software placed on the market permitting electronic communications" include "the option to prevent third parties 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, the software shall inform the end-user about the privacy setting options and, to continue with the installation, require the end-user to consent to a privacy setting.[251]

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.[252]

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

247. Dan Packel, *Pa. Judge Says Google Must Turn Over Foreign Server Data*, Law360 (Feb. 6, 2017) (on *USA v. Information Associated With Google Accounts More Fully Described In Attachment A*), https://www.law360.com/articles/888696/pa-judge-says-google-must-turn-over-foreign-server-data.
248. Elaine Edwards, *Major Privacy Case to Open Before High Court In Dublin*, The Irish Times (Feb. 5, 2017), http://www.irishtimes.com/business/technology/major-privacy-case-to-open-before-high-court-in-dublin-1.2964424; Jedidiah Bracy, *Model Clauses In Jeopardy With Irish DPA Referral to CJEU*, The Privacy Advisor (May 25, 2016), https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/.
249. Marc Crandall, *EU Data Protection Authorities Confirm Compliance of Google Cloud Commitments For International Data Flows*, Google Blog (Feb. 6, 2017), https://blog.google/topics/google-cloud/eu-data-protection-authorities-confirm-compliance-google-cloud-commitments-international-data-flows/.
250. 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
251. *Id.*
252. 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/.

"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.[253]

4. Emerging Challenges for U.S.-Based Companies in Europe

How signing onto the Privacy Shield program will force U.S.-based companies to conform to a different set of rules should be evident from a number of cases and discussions currently ongoing in the EU:

- In *McFadden v. Sony*, Case No. C-484/14, in the CJEU, the CJEU held that network operators may have an obligation to retain some capability to identify their users. McFadden ran a business in Munich, Germany, which deliberately offered "anonymous access to a wireless local area network free of charge in the vicinity of his business." One user impermissibly made use of Sony's copyrighted works, and Sony asked McFadden to respect its rights. In its September 2016 ruling, the CJEU considered that "a measure consisting in password-protecting an internet connection may dissuade the users of that connection from infringing copyright or related rights, provided that those users are required to reveal their identity in order to obtain the required password and may not, therefore, act anonymously."[254] Although the ruling did not per se hold that all network providers must identify every user, the decision leaves one wondering what will happen with internet anonymity in Europe – which is currently alive and well in the U.S.
- In *Breyer v. Bundesrepublik Deutschland*, Case No. C-582/14, also in the CJEU, the CJEU held that dynamic IP addresses may be PI. In *Breyer*, the issue was whether even a dynamic IP address can be PI because the ISP can re-identify the address assigned.[255] In October 2016, the CJEU found that because German authorities could ultimately demand that the ISPs provide the identities of those who had used the dynamic IP address, such addresses are PI. The implication is potentially far-reaching, as dynamic IP addresses –by nature temporarily assigned– are nearly impossible to re-identify without the assistance of ISPs. The ruling will likely impact how anonymization and pseudoanonymization may be used as defenses under the GDPR,[256] which are currently viable defenses in the U.S. for data use.

Both *McFadden* and *Breyer* are critical lessons for organizations looking to apply for the Privacy Shield program. Although participation in the program is important for trans-Atlantic business, corporations must also consider the technologies they must implement to be compliant. *McFadden* and *Breyer* leave open questions on whether organizations must track every user and customer, which would lead to additional disclosure and consent requirements, and all of which would likely be part of costly technology upgrades. Given unique European "rights," such as the "right to be forgotten" and the right to be free from "automatic profiling," being GDPR-compliant in the long term will require that participants have very expensive data tracking and processes technologies. The Privacy Shield is just a prelude to a much larger problem with doing business in the EU in the long-term.

253. 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/.
254. Dennis Kelleher, *Kelleher: McFadden v. Sony's Implications Can't Be Ignored*, The Privacy Advisor (Oct. 14, 2016), https://iapp.org/news/a/kelleher-mcfadden-v-sonys-implications-cant-be-ignored/.
255. Allison Grande, *IP Addresses Fall Under EU Privacy Law, Top Court Says*, Law360 (Oct. 19, 2016), https://www.law360.com/articles/853437/ip-addresses-fall-under-eu-privacy-law-top-court-says.
256. Dennis Kelleher, *In Breyer Decision Today, Europe's Highest Court Rules On Definition of Personal Data*, The Privacy Advisor (Oct. 19, 2016), https://iapp.org/news/a/in-breyer-decision-today-europes-highest-court-rules-on-definition-of-personal-data/.

B. China's "Network Security Law"

On November 7, 2016, China enacted its Cybersecurity Law, which will come into force on June 1, 2017. Within it, a "Network Information Security" section sets forth requirements for the protection of PI in a framework that is similar to the GDPR:

- 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 collecting or using of their personal information.[257]

Ultimately, it is too early to tell how China will enforce this law. Nonetheless, U.S.-companies doing business in China must be aware of the law so that that they may plan accordingly.

257. 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/.

The Data Privacy team at Troutman Sanders LLP is multidisciplinary, drawing talent with backgrounds in intellectual property, regulatory enforcement & compliance, and class action litigation. Our team also includes certified technologists. The attorneys at Troutman Sanders have been involved in data privacy litigation for over a decade, and are currently engaged in some of the largest and most important data breach and use litigation in the United States.

CONTACTS

Ronald I. Raether Jr.
Orange County
949.622.2722
ronald.raether
@troutmansanders.com

Ron Raether leads the Cybersecurity, Information Governance and Privacy practice and is a partner in the Financial Services Litigation practice group at Troutman Sanders. Ron is known as the interpreter between businesses and information technology, and has assisted companies in navigating federal and state privacy laws for over twenty years. Ron's understanding of technology led him to be involved in legal issues that cross normal law firm boundaries, including experience with data security, data privacy, patent, antitrust, and licensing and contracts. This experience allows Ron to bring a fresh and creative perspective to data compliance issues with the knowledge and historical perspective of an industry veteran.

Ron's involvement in seminal data compliance and data use cases has helped define current standards in several areas of the law. He assisted one of the first companies required to provide notice of a data breach and has since successfully defended companies in over 100 class actions. Ron represents clients in a broad range of technology and data privacy matters including data aggregation and analytics, mobile applications, de-identification/anonymization, including correlating data from multiple connected devices, "connected-things (IoT)," electronic crash- and consumer-reporting systems, and payment technologies. Ron also advises on pre- and post-incident compliance concerns ranging from privacy policy preparation to development of incident response plans and workflows, addressing post-incident aftermath, and responding to regulatory inquiries. Balancing privacy, cyber security and business functionality, Ron's approach to data governance is uniquely designed with the industry in mind as it adapts to the ever-evolving technological and legal landscape.

Mark C. Mao
San Francisco
415.477.5717
mark.mao
@troutmansanders.com

Mark is certified by the International Association of Privacy Professionals (IAPP), for their ISO-approved programs, as a Certified Information Privacy Technologist (CIPT), and a Certified Information Privacy Professional in the United States (CIPP/US).

Mark's practice focuses primarily on emerging-technology companies, with a particular interest in their intellectual property and privacy ("cyber") law needs. He has substantial experience advising and litigating on behalf of companies across a broad spectrum of industries, including consumer and enterprise software, database applications, e-commerce, data brokers, advertisers, social networking, mobile applications, and payment technologies, in addition to hardware, bio-tech, "green"-tech, and renewable energy. Mark has successfully defended numerous organizations through difficult intellectual property disputes, insider/shareholder disputes, and consumer-class actions where the regulatory and legal issues continue to evolve rapidly, such as in the areas of Telephone Consumer Protection Act (TCPA) and Fair Credit Reporting Act (FCRA) litigation. Mark has advised companies throughout their product life cycles on emerging privacy law issues, in addition to handling their data breach needs.

During the dot-com era, Mark was an information technologies consultant with Arthur Andersen Consulting, implementing enterprise database software throughout the Silicon Valley. This helps him better serve clients where technical details are directly at issue.

Mark believes in litigating efficiently and effectively for his clients, so that organizations can focus on their growth while mitigating their risks. Mark was named a Rising Star in Super Lawyers Magazine in 2016.

REPUTATION FOR EXCELLENCE

Troutman Sanders is consistently listed among the best law firms internationally.

- Ranked #67 in the 2016 Am Law 100.
- BTI Client Service A-Team for 12 consecutive years.
- Recognized in 27 national and regional practices in Chambers USA 2016, and 75 lawyers earned 79 individual rankings in their respective practice areas. Firm practices and lawyers received top tier rankings in more than a dozen categories.
- Ranked #1 nationally in 39 practice areas and ranked #1 regionally in 80 practice areas in the 2016 edition of Best Law Firms.