DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE

QUARTERLY UPDATE, OCTOBER 2016

By

Mark C. Mao, Ronald I. Raether, Jr. and Sheila M. Pham

TROUTMAN SANDERS

troutmansanders.com

I. INTRODUCTION

Fall 2016 will be remembered as a critical chapter in the development of privacy law in the United States. Although a great deal of proposed legislation and regulations are still in the works, the urgent need for more uniform rules and reasonable guidance is widely felt.

The most important developments are in the area of civil case law. Courts have proceeded to address class certification issues, in addition to answering the applicability of *Spokeo v. Robins* to cases outside of the Fair Credit Reporting Act context. There are now additional strategies for defendants to consider, both in anticipation of and during litigation.

On the regulatory front, regulators have begun taking sides on certain advertisement and financial technologies, which were previously left alone. It would be premature to say whether the regulators have exceeded their authority, as some critical challenges to enforcement actions still need to be played out in the courts.

For U.S.-based multi-national organizations, the landscape is even less clear. Although the U.S. and European Union have entered into a new "Privacy Shield" to replace the prior safe harbor for trans-Atlantic data transfers, the fact that companies would be signing on to abide by European rules is problematic. Various EU regulators have increasingly taken draconian views on the use of data, even though data innovation has proven to be a powerful impetus for the growth of American technology. Europe's bureaucracy has instead stifled the growth of emerging technologies, and no U.S.-based company looks forward to being held back like their European competitors.

II. LEGISLATION & REGULATIONS

Because data privacy law in the United States remains sector-based, legislators and regulators continue to patch one industry at a time. The resulting mishmash of privacy laws is less organized than the general directives of the European Union, so U.S. companies must carefully monitor developments across all industries with which they might be involved.

A. New Regulations

In March 2016, the Federal Communications Commission (FCC) issued a notice of proposed rulemaking (an NPRM), which proposed "rules that would give broadband customers the tools they need to make informed decisions about how their information is used by their internet service providers (ISPs), and whether and for what purposes their ISPs may share their customers information with third parties."[1] NPRM 16-39 outlined 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) "expressive, 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.[4] The purpose of the revisions was to bring the FCC more in alignment with the FTC. Under the new rules:

- ISPs would be required to request opt-ins for information that would be considered "sensitive information," such as geo-location, children's information, health information, financial information, social security numbers, web browsing history, application usage history, and the content of communications.
- All other personally identifiable information was to be considered non-sensitive, and use and sharing of such information would require an offer to opt out, which is typically less intrusive.
- ISPs are still 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.
- As under the original NPRM 16-39, the revised rules would impose security requirements and breach notification obligations.[5]

Additional details of the rules that were approved should be made public within the next few months.

B. Proposed Regulations

1. 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. The regulation has a number of requirements that are not atypical, including: (a) setting up a comprehensive cybersecurity program (Section 500.02), (b) adhering to a written cybersecurity policy and incident response plan (Sections 500.03 and 500.16), (3) appointing a chief information security officer (Section 500.04), (4) requiring multi-factor authentication and encryption (Sections 500.12 and 500.15), (5) conducting regular penetration, vulnerability, and risk assessments (Sections 500.05 and 500.07), (6) limiting access privileges (Section 500.07), (7) requiring vendor controls and written assurances (Section 500.11), and (8) limiting data retention (Section 500.12).[6]

Some also view the NY DFS proposals as very onerous, however. For example, some have pointed out that the definition of a "Cybersecurity Event" is "any act or attempt, successful or *unsuccessful*, to gain unauthorized access to, disrupt or misuse an Information System."[7] The regulation further provides that

1. The industry previously questioned the FCC's authority to regulate broadband; but see *US Telecom Ass'n v. FCC*, D.C. Cir. Case No. 15-1063 (Jun. 14, 2016) (potentially resolving issues on FCC authority to regulate neutrality).
2. Press Release, *FCC Proposes to Give Broadband Consumers Increased Choice Transparency and Security For Their Personal Data* (FCC, Mar. 31, 2016).
3. Ebersole, *FCC Sets Out Revised Rules For Broadband Carriers* (Law360, Oct. 6. 2016).
4. Ebersole, *FCC Sets New Privacy Framework For Broadband Providers* (Law360, Oct. 27, 2016).
5. Press Release, *FCC Adopts Privacy Rules to Give Broadband Customers Increased Choice, Transparency And Security For Their Personal Data* (FCC, Oct. 27, 2016), available at: http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1027/DOC-341937A1.pdf.
6. 23 NYCRR 500 *et al.*
7. 23 NYCRR 500.1(d) (emphasis added).

notice to the NY DFS superintendent must be made within 72 hours of an event "(that) has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information."[8] A narrow reading of the regulation is that the DFS may require the reporting of commonly occurring attacks that are ultimately unsuccessful, while unnecessarily raising regulatory scrutiny.

Others also point out that the written assurances required of vendors will make negotiations near impossible. No vendor will promise that its offerings are "free of viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's Information Systems."[9]

As a result, the proposals from the NY DFS have received fierce opposition and public outcry. If unaltered, the regulations will become final after a 45-day comment period, and will be effective January 1, 2017. Covered entities have 180 days from the effective date of the regulation to get into compliance and must begin submitting to the superintendent a "certificate of compliance" as of January 15, 2018.

2. The National Association of Insurance Commissioners' Insurance Data Security Model Law

The National Association of Insurance Commissioners includes commissioners from fifty states, five territories, and the District of Columbia. On August 17, it published a draft model law to regulate the data security practices of insurance entities, requesting further public comment. If adopted in a licensee's state, the law would affirmatively require insurance entities to implement information security programs designed to protect the security of confidentiality of personal information that would match the size and complexity of the licensee, the nature and scope of its activities, and the sensitivity of the personal information. As the draft currently stands, licensees must provide written reports regarding any data breach within 72 hours of the incident occurrence.[10]

3. The Federal Trade Commission's "Follow the Lead" Workshop

Nearly one year after the FTC issued its report on "Big Data,"[11] the FTC issued a report entitled "'Follow the Lead' Workshop: Staff Perspective," in September 2016. The staff report discussed 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.[12]

In assessing the life cycle of such products using the example of short-term loans, the FTC indicated 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 engaged in similar analysis.[13] Online financial services should view the staff report as demonstrative of how the FTC intends to apply the principles it had laid out in its prior big data report against all of those who participate in the use of online lead generation.

4. Joint Advanced Rulemaking For Enhanced Cyber Risk Management Standards

In October 2016, the Board of Governors for the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued a joint advanced notice of proposed rulemaking (ANPR) that would apply to entities with total consolidated assets of $50 billion or more. The purpose of the ANPR was to try to "increase covered entities' operational resilience" against cyber attacks, establish better cybersecurity rules and practices for financial institutions, and secure "critical functions" of the financial sector.[14]

Although much of the ANPR was still in the form of issue spotting and request for input, some of the proposed rules included:

- "Enhanced cyber risk management standards" for covered entities, which include: (1) cyber risk governance, (2) cyber risk management, (3) controlling internal dependencies "on an enterprise-wide basis," (4) external vendor and resource dependency management, and (5) incident response, cyber resilience, and situational awareness; and
- A "two-tiered" approach, with "an additional, higher set of expectations…applying to those systems of covered entities that are critical to the financial sector."

8. 23 NYCRR 500.17(a).
9. Finch, *New York Sets Uncomfortable Cybersecurity Precedent* (Law360, Sept. 20, 2016).
10. White, *Insurance Data Security Model Law Released For Comment* (IAPP, Sept. 8, 2016).
11. "Big Data – a Tool For Inclusion or Exclusion," p. 16-17 (FTC January 2016)
12. *"Follow the Lead" Workshop: Staff Perspective* (FTC, Sept. 2016).
13. See *"Follow the Lead" Workshop: Staff Perspective*, p. 5-8.
14. http://assets.law360news.com/0854000/854423/2016-10-19_notice_dis_a_fr.pdf

Interested parties have until January 17, 2017 to weigh in on the ANPR.[15]

5. The Department of Transportation's Car Cybersecurity Proposal

The Department of Transportation (DoT) and the National Highway Traffic Safety Administration (NHTSA) issued its "Cybersecurity Best Practices For Modern Vehicles," in October 2016.[16] The NHTSA mentioned that the guidance, although voluntary, is "best practices" for compliance with the National Traffic and Motor Vehicle Safety Act.

In the guidance, the NHTSA urges the automotive industry follow the Cybersecurity Framework promulgated by the National Institute of Standards and Technology (NIST), structured around the concepts of "identify, protect, detect, respond, and recover," in addition to considering standards such as ISO 27000.[17] In addition, as with the Food and Drug Administration and the emerging connected medical devices industry, the NHTSA encourages that the industry agree to share information regarding cyber threats, standardize vulnerability and breach reporting, in addition to agree to self-auditing.[18] Self-auditing should include risk assessments, penetration tests, and documented organizational decisions.[19]

Specifically, the NHTSA recommends that developers and manufacturers take into account the following 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.[20]

In addition, the NHTSA expressed particular concern about after-market devices and the need for protections during automobile servicing.[21]

C. Self-Regulatory Efforts On The "Internet-of-Things"

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 the "internet-of-things (IoT)." A plethora of industry efforts and consortiums have been initiated, but no clear winners have appeared.[22] Nonetheless, a number of efforts are noteworthy:

- In February 2016, the Groupe Speciale Mobile Association (GSMA) promulgated both "IoT Security Guidelines" and "IoT Connection Efficiency Guidelines."[23] 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. The GSMA is trying to promote its standards by allowing self-assessment and submission to the GSMA.[24]

- In April 2016, Underwriters Laboratories (UL) launched a new "UL 2900" series of standards that offers 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.[25] Controls include access controls, secure data storage, cryptography, key management, authentication, integrity, and confidentiality of data received and transmitted.[26]

---

15. Grande, *Feds' Cybersecurity Plan Gives Boards, Vendors Bigger Role* (Law360, Oct. 21, 2016).
16. http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016.
17. Cybersecurity Best Practices For Modern Vehicles (NHTSA, Oct. 2016), at Section 5.2.
18. *Id.* at Sections 6.3 through 6.6.
19. *Id.* at Section 6.1.1 through 6.1.3.
20. *Id.* at Sections 6.7.1 through 6.7.11.
21. *Id.* at Sections 8 and 9.
22. See Rector, *"Internet of Things" Protocols: Past And Future Trends* (Law360, Oct. 12, 2016).
23. http://www.gsma.com/connectedliving/future-iot-networks/
24. http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
25. http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/
26. https://standardscatalog.ul.com/standards/en/outline_2900-2-2_1

- In July 2016, the NIST issued a publication entitled "Networks of Things," which purports to "provide a basic model aimed at helping researchers better understand the Internet of Things (IoT) and its security challenges."[27] Although the publication is more akin to a framework for understanding IoT as opposed to a specification of standards, it provides a useful reference for organizing the components that typically form an IoT ecosystem, while providing foresight into likely reliability and security scenarios.[28]

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 also 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."[29]

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."[30] 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 FCRA litigation, but also for data breach and data misuse litigation.

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

Following 2015 trends, courts are still divided on what is required for plaintiffs to demonstrate Article III standing in the context of privacy litigation.[31] In two separate controversial rulings, the Sixth and Seventh Circuit Courts cited to *Remijas v. Neiman Marcus Group* to reverse motions to dismiss granted by lower courts on the basis of no Article III standing.[32] Some district courts have likewise denied motions to dismiss, finding the damage theories espoused by plaintiffs sufficient.[33]

In addition to trying to change the post-*Clapper v. Amnesty International* landscape, plaintiffs have made some other interesting and noteworthy moves this year.[34] 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.[35]

---

27. https://www.nist.gov/news-events/news/2016/07/nists-network-things-model-builds-foundation-help-define-internet-things
28. See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
29. *Spokeo, Inc. v. Robins,* 578 U.S. ___, at *7-10 (May 16, 2016).
30. *Id.*, at *8-10.
31. See Solomon, *Post-Spokeo, Standing Challenges Remain Unpredictable* (Law360, Oct. 26, 2016).
32. *Galaria (Hancox) v. Nationwide Mut. Ins. Co.*, 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); *Lewert v. P.F. Chang China Bistro*, 819 F.3d 963, 966-967 (7th Cir. 2016) (reversed district court, citing to *Remijas v. Neiman Marcus Group*, 794 F.3d 688 (7th Cir. 2015)).
33. See e.g., *Bohannan v. Innovak Int'l, Inc.,* 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.* 2016 U.S. Dist. LEXIS 100198, *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.*, 2016 U.S. Dist. LEXIS 70594 (May 27, 2016) (permitting various contract theories to survive); *Irwin v. Jimmy John's Franchise*, 2016 U.S. Dist. LEXIS 48162, *7-9 (C.D. Ill. March 29, 2016) (dismissing most causes of action, but permitting some causes of action to survive, including one based on "implied contract").
34. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013)
35. See e.g., *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2016 U.S. Dist. LEXIS 100198, *39-41, *53-54 (D. Or. Aug. 1, 2016) (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 (N.D. Cal. May 27, 2016) (permitting various contract theories to survive); see also *Irwin v. Jimmy John's Franchise*, 2016 U.S. Dist. LEXIS 48162, *7-8 (C.D. Ill. March 29, 2016) (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").

Second, plaintiffs have continued to try to push novel theories of liability, such as using FCRA provisions requiring consumer reporting agencies to ensure that "consumer reports" are delivered to the intended recipients. Plaintiffs now argue that implicit in such requirements is a security obligation as well.[36] These developments suggest that plaintiffs will continue to explore additional theories of liability with the courts.

Regardless, many courts continue to grant motions to dismiss on the basis of lack of Article III standing, particularly where no Personal Information ("PI") misuse was alleged, where the alleged misuse is not credible, or where there are only limited instances of misuse.[37] 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.[38] 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).[39]
- 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.[40]
- Where plaintiffs' claims are heavily dependent on arguments relating to a written privacy policy, and where defendant's terms and conditions apply sound limitations of damages clauses to the privacy policy, the economic loss rule may apply.[41]

---

36. See e.g., *Galaria (Hancox) v. Nationwide Mut. Ins. Co.*, 2016 U.S. App. LEXIS 16840 (6th Cir. Sept. 12, 2016) (remanding to district court to decided 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.*, 2016 U.S. Dist. LEXIS 123030, *43-44 (Consolidated 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").

37. *In re Zappos.com, Inc. Custom Data Security Litigation*, 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*, 2016 U.S. Dist. LEXIS 105480, *15-17 (D.D.C. Aug. 10, 2016) (granting motion to dismiss, finding no "plausible harm" alleged and *accord Chambliss*, *infra*); *Torres v. The Wendy's Company*, 2016 U.S. Dist. LEXIS 96947, *6-9 (M.D. Fla. Jul. 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*, 2016 U.S. Dist. LEXIS 89992, *17-18 (E.D. Mo. Jul. 12, 2016) (no misuse alleged resulting from hack, and over two years have passed); *Bradix v. Advance Stores Co.*, 2016 U.S. Dist. LEXIS 87368 (E.D. La. Jul. 5, 2016) (finding allegations of two "as yet identified" attempts to secure vehicle financing insufficient); *Khan v. Children Nat'l Health Sys.*, 2016 U.S. Dist. LEXIS 66404, *15-16 (D. Md. May 19, 2016) (finding no allegations of misuse, even where there are allegations of compromise); see *Chambliss v. CareFirst, Inc.*, 2016 U.S. Dist. LEXIS 70096, *11-13 (D. Md. May 27, 2016) (granting motion to dismiss, finding no harm alleged); *Patton v. Experian Data Corp.* 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.*, 2016 U.S. Dist. LEXIS 2592 (D. Minn. Jan. 7, 2016), *11-19 (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.*, 2015 U.S. Dist. LEXIS 172152, *14-15 (E.D.N.Y. Dec. 28, 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).

38. *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, *43-44 (Consolidated MDL, N.D. Ala. Sept. 12, 2016) (dismissing claims of some plaintiffs, because allegations of actual harm must be "fairly traceable" to alleged breach); *Attias v. Carefirst*, 2016 U.S. Dist. LEXIS 105480, *15-16 (D. D.C. Aug. 10, 2016) (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 v. Experian Data Corp.* 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016) (granting motion to dismiss, noting that allegations of future harm must be "credible").

39. *In re Barnes & Nobles Pin Pad Litig.*, 2016 U.S. Dist. LEXIS 137078, *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).

40. *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, *37-40 (Consolidated MDL, S.D. Ala. Sept. 12, 2016) (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 Security Litigation*, 2016 U.S. Dist. LEXIS 604053, *26-28 (D. Nev. May 6, 2016), affirmed, 2016 U.S. Dist. LEXIS 115598 (Aug. 29, 2016); see also *Baum v. Keystone Mercy Health Plan And Amerihealth Mercy Health Plan*, 2016 Pa. Super. Unpub. 1358, *8-9 (Pa. Super. Ct. Apr. 26, 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).

41. See *Longenecker-Wells v. Benecard Serv.*, 2016 U.S. App. LEXIS 15696, *5-8 (3rd Cir. Aug. 25, 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.*, 2016 U.S. Dist. LEXIS 149958, *36-39 (in data misuse case, court applies economic loss rule to bar negligence claims under New York and California law for negligence).

Just as importantly, while the Seventh and Ninth Circuits had appeared more plaintiff-friendly in 2015, the legal landscape has begun shifting toward the defense. In both Circuits, courts are again granting motions to dismiss, particularly where plaintiffs' allegations of harm are more attenuated.[42]

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 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.

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 Rules of Civil Procedure Rule 12(b)(6) may sometimes present a higher bar for the harm that plaintiffs must plead, when compared to Federal Rules of Civil Procedure Rule 12(b)(1). For almost all causes of action, actual out-of-pocket loss is required to survive a Rule 12(b)(6) challenge.

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 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.[43]

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.[44] Instead, questions on the standard of care and the situations in which plaintiffs can obtain class certification are now the focus.

B. Data Misuse Litigation: Where Technicalities Matter

That it is increasingly important for data privacy professionals to have a deeper appreciation for the workings and intricacies of technology is even more evident in cases involving alleged data misuse. Although privacy law in the United States has traditionally been sectorial, courts are beginning to discuss privacy expectations as if fundamental rights are implicated. Thus, when plaintiffs cannot state a cause of action pursuant to a statute, they state their claims using contract and quasi-contract theories, arguing that a promise or convention has been breached.

In response, motions to dismiss have been generally successful when the alleged misuse is relatively simple and only involves a defendant that had originally collected the data pursuant to a permissible purpose.[45] Dismissals have also been routinely granted when the party collecting and disseminating the data did not obtain the data as part of some service for a fee.[46]

However, where data analytics and targeted advertising involve multiple ecosystems, layers, and stakeholders, courts often have difficulty properly apportioning responsibility and

42. *In re Barnes & Nobles Pin Pad Litig.*, 2016 U.S. Dist. LEXIS 137078, *25 (N.D. Ill. Oct. 3, 2016), *supra*; *Patton v. Experian Data Corp.* 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016) (granting motion to dismiss for failure to allege that alleged breach led to any unlawful access of PI).
43. But see *Longnecker-Wells v. Benecard Serv.*, 2016 U.S. App. LEXIS 15696, *5-8 (3rd Cir. Aug. 25, 2016) (applying economic loss rule even where no written contracts are at issue).
44. See e.g., *Bradix v. Advance Stores Co.*, 2016 U.S. Dist. LEXIS 87368 (E.D. La. Jul. 5, 2016); *Khan v. Children Nat'l Health Sys.*, 2016 U.S. Dist. LEXIS 66404, *15-16 (D. Md. May 19, 2016); also *Patton v. Experian Data Corp.* 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016).
45. See e.g., *Braitberg v. Charter Communs, Inc.*, 2016 U.S. App. LEXIS 16477, *11-13 (8th Cir. Sept. 8, 2016) (affirming lower court's dismissal of claims against Charter, for retaining PI of former customers longer than allegedly permitted by the Cable Communications Policy Act); *Gubala v. Time Warner Cable, Inc.*, 2016 U.S. Dist. LEXIS 79820, *13-14 (E.D. Wis. Jun. 17, 2016) (affirming lower court's dismissal of claims against Time Warner, for retaining PI of former customers longer than allegedly permitted by the Cable Communications Policy Act).
46. See *In re: Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152-154 (3rd Cir. Nov. 10, 2015) (in case alleging that Google overrode user opt-out preferences, affirming district court's dismissal of all but one state court claim for failure to allege damages); *In re Facebook Internet Tracking Litig.*, 140 F.Supp.3d 922, 932 (N.D. Cal. Oct. 23, 2015) (on a motion to dismiss in pre-*Spokeo* lawsuit alleging Facebook misuses persistent cookies, court cites to *In re: Google Inc. Cookie Placement Consumer Privacy Litig.* and finds no harm alleged sufficient to confer Article III standing); *In re Google Privacy Policy Litig.*, 2015 U.S. Dist. LEXIS 92736, *13-19 (N.D. Cal. Jul. 15, 2015) (in pre-*Spokeo* case alleging Google contravened its own privacy policies by allowing developers to access Google Wallet user PI, granting motion to dismiss and finding no actual concrete injury); but see *Svenson v. Google, Inc.*, 2015 U.S. Dist. LEXIS 43902 (N.D. Cal. Apr. 1, 2015) (reaching contrary result on motion to dismiss from *In re Google Privacy Policy Litig.*)

fault. Surveying the legal landscape, organizations engaged in e-commerce and mobile advertising should be aware of a number of important recent trends:

1. 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.[47]

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.[48] Furthermore, courts may take into consideration how the privacy statements of third parties affect user expectations. In *Opperman v. Path,* 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.[49]

On the other hand, the inconsistent experience of users across an ecosystem may be used to defeat class certification. In *Corley v. Google*, 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.[50]

In the case of *In re Facebook Privacy Litigation*, plaintiffs alleged that Facebook disclosed URL-headers containing Facebook IDs to third parties, which would allow third parties to re-identify users, in contravention of 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.[51]

2. Disclosing "Non-Personal Information" Can Sometimes Be Problematic.

Third parties may request that organizations disclose to them certain "non-personal information (non-PI)," which appears relatively innocuous. However, the ability of aggregators to re-identify individuals by collecting large pools of information across wide networks has made disclosing non-PI for otherwise regulated data increasingly problematic, particularly when dealing with statutory schemes where the definition of "personal information" is vague. Organizations involved in the provision of streaming videos and written periodicals need to take extra care in assessing how and what non-PI is disclosed.[52]

Even where no statute is directly on point, businesses that inadvertently disclose non-PI may find themselves embroiled in litigation in jurisdictions that recognize unique and extraordinary theories of recovery. For example, in *In re Facebook Privacy Litigation*, plaintiffs alleged that Facebook inadvertently disclosed URL-headers which would allow third parties to re-identify users who access their websites through Facebook browsers, in contravention of Facebook's own privacy assurances. Although the Northern California District Court indicated skepticism regarding plaintiffs' ability to prove actual damages, it permitted the claims to survive motions to

47. See *Opperman v. Path, Inc. et al.*, 2016 U.S. Dist. LEXIS 92403, *51 (N.D. Cal. Jul. 26, 2016) (partially granting class certification against Apple, on basis of aiding and abetting theory and for "nominal damages").
48. See e.g., *Svenson v. Google, Inc.*, 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. Mar. 23, 2015) (denying defendants' motions to dismiss, partially on basis of Apple's advertising campaign regarding privacy).
49. *Opperman v. Path, Inc. et al.*, 2016 U.S. Dist. LEXIS 122578, *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").
50. *Corley v. Google, Inc.*, 2016 U.S. Dist. LEXIS 111076, *147-148 (N.D. Cal. Aug. 19, 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. et al.*, 2016 U.S. Dist. LEXIS 92403, *supra*.
51. *In re Facebook Privacy Litig.*, 2016 U.S. Dist. LEXIS 119293, *25-31 (N.D. Cal. Sept. 2, 2016) .
52. See *Boelter v. Advance Magazine Publrs.*, 2016 U.S. Dist. LEXIS 134484, *14-15 (S.D.N.Y. Sept. 28, 2016) (finding "personal reading information" for the purposes of the purposes of Michigan's Preservation of Personal Privacy Act because the PI may combined and re-identified by third parties and magazine publisher); *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486-487, *8-9 (1st Cir. Apr. 29, 2016) (finding GPS coordinates "personally identifiable information" for the purposes of the Video Privacy Protection Act, because they may be recombined with device information); but see *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 289-290 (3rd Cir. Jun. 27, 2016) (recognizing *Yershov*, but finding that the drafters of the Video Privacy Protection Act intended to cover "readily identifiable" information, and not information that may be recombined).

dismiss on the recognition of "nominal damages" in the Ninth Circuit.[53]

3. 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 Google to advertise and install third party cookies, which then tracked the user through the Doubleclick advertisement network. Plaintiffs sued both Viacom and Google, claiming that they impermissibly tracked Viacom users as a third party. Although the Third Circuit agreed that Google should be dismissed from the case, it found the allegations against Viacom for intrusion upon seclusion sufficient to survive its motion to dismiss, based on the allegations in the Complaint that Viacom had promised parents regarding the tracking of children.[54]

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 software development kits (SDKs) in 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 remains the best defense against privacy violation claims for the use of SDKs.[55]

4. 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 remains the most powerful defense for businesses leveraging data collection and analytics.[56] As demonstrated herein, courts are more carefully assessing the adequacy of disclosures.[57] They are more skeptical of the generalized disclosures that dominated the market years before. When possible, 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.[58] 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. The cases wherein Google and Facebook defeated class certification[59] demonstrate that individualized user experiences make defeating class certification more likely. 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.

Courts may find overbroad class arbitration waivers invalid in the context of privacy class actions, especially when the claims arise from data use after services have ended.[60]

---

53. *In re Facebook Privacy Litig.*, 2016 U.S. Dist. LEXIS 84766, *15-20 (N.D. Cal. Jun. 28, 2016); but see *In re Facebook Privacy Litig.*, 2016 U.S. Dist. LEXIS 119293 (N.D. Cal. Sept. 2, 2016) (eventually denying class certification).
54. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 294-295 (3rd Cir. Jun. 27, 2016) .
55. See e.g., *Carlsen v. Gamestop*, 2016 U.S. App. LEXIS 14999 (8th Cir. Aug. 16, 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).
56. See e.g., *Carlsen v. Gamestop*, 2016 U.S. App. LEXIS 14999 (8th Cir. Aug. 16, 2016) (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.*, 2016 U.S. Dist. LEXIS 149958, *63-64 (while granting class certification, noting that implied consent may have created individualized questions); see also *Corley v. Google, Inc.*, 2016 U.S. Dist. LEXIS 111076, *147-148 (N.D. Cal. Aug. 19, 2016) (finding that some privacy statements of Google may show consent to scanning of emails for targeted advertising); also *In re Sling Mediabox Advertising Litig.*, 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).
57. *Opperman v. Path, Inc. et al.*, 2016 U.S. Dist. LEXIS 122578, *22-25 (N.D. Cal. Sept. 8, 2016) (discussing "effective" consent).
58. See e.g., *Svenson v. Google, Inc.*, 2015 U.S. Dist. LEXIS 43902, *supra*; *Opperman v. Path, Inc.*, 84 F.Supp.3d 962, *supra*.
59. *In re Facebook Privacy Litig.*, 2016 U.S. Dist. LEXIS 119293, *25-31 (N.D. Cal. Sept. 2, 2016) ; *Corley v. Google, Inc.*, 2016 U.S. Dist. LEXIS 111076, *147-148 (N.D. Cal. Aug. 19, 2016); see also see also *In re Lenovo Adware Litig.*, 2016 U.S. Dist. LEXIS 149958, *63-64 (noting in dicta that implied consent may have created individualized questions).
60. *Wexler v. AT&T Corp.*, 2016 U.S. Dist. LEXIS 135695 (E.D.N.Y. Sept. 30, 2016) (denying motion to compel arbitration in case involving allegations of violation of the Telephone Consumer Protection Act, where former customer continued to get texts after her services terminated).

IV. 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, absence of written security plans, and 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 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).[61] Undaunted, the FTC appealed the decision. On July 28, 2016, the Commission reversed the administrative judge. 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."[62] LabMD has since appealed the opinion of the FTC commissioners to the federal courts.

- The FTC has 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."[63]

- In a luncheon audience at the Technology Policy Institute in Aspen, Colorado on August 29, 2016, FTC Chairwoman Edith Ramirez took a very expansive interpretation of what may be personally identifiable information (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.[64]

- In October 2016, the FTC released its "Data Breach Response: A Guide For Business."[65] Interestingly, although the guide discusses how 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.[66] 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.[67]

B. HIPAA Enforcement

The U.S. Department of Health and Human Services (HHS) has come under increasing fire due to high-profile data breaches. In fact, 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.[68]

---

61. FTC ALJ Docket No. 9357 (Nov. 13, 2015); and Press Release, *Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc.* (FTC, Nov. 19, 2015).
62. *In re the Matter of LabMD*, 2016 FTC LEXIS 128, *25 (Jul. 28, 2016); see also Maldoff, *LabMD And The New Definition of Privacy Harm* (IAPP, Aug. 22, 2016).
63. Arias, *The NIST Cybersecurity Framework And The FTC* (FTC, Aug. 31, 2016).
64. Waterman, *FTC's Ramirez: New Tech's Complexity Leaves Privacy Basics Unchanged* (Fedscoop.com, Aug. 23, 2016), available at http://fedscoop.com/edith-ramirez-ftc-aspen-institute-august-2016
65. https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.
66. *Id.* at p. 8-9.
67. *Id.* at p. 7.
68. Slabodkin, *HHS Security, Privacy Guidance Said to Fall Short of Fed. Guidelines* (Health Data Management, Sept. 27, 2016), available at http://www.healthmanagementdata.com/

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.[69]

- 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.[70]

- 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.[71]

- 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 health information, failed to limit access, and failed to obtain a written agreement with a business associate to safeguard electronic information.[72]

- On September 23, 2016, the Care New England Health 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.[73]

- 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.[74]

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. The aggressive posture undertaken by the HHS is similar to those of other regulators.

C. The Security Exchange Commission

Some regulators may be even harsher than the FTC and HHS, however. 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 that it did not hold the bank responsible for. In fact, the FTC found that bank had "established and implemented comprehensive policies designed to protect against insider theft of personal information." Nonetheless, the SEC required that bank pay $1 million by way of a settlement.[75]

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, for over $100,000, the SEC fined the broker-dealer 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.[76]

D. State Enforcement Actions

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

- 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.[77]

69. Sieniuc, *Catholic Nonprofit to Pay $650k Settlement In HIPAA Breach* (Law360, Jun. 30, 2016).
70. Lidgett, *Ore. Health System Pays $2.7M to Settle Data Breach Probes* (Law360, Jul. 15, 2016).
71. Bryant, *UMMC to Pay $2.75 Million Fee In Federal Settlement* (Hattiesburg American, Jul. 22, 2016).
72. Overley, *Ill. Hospital Chain Inks Record $5.5M HIPAA Deal* (Law360, Aug. 4, 2016).
73. Sieniuc, *New England Health System Fined By HHS Over Data Loss* (Law360, Sept. 26, 2016).
74. Greene, *St. Joseph to Pay $2.1M Over Leaked Patient Records* (Law360, Oct. 18, 2016).
75. Maldoff, *'Not Unfair' May Still Be Unreasonable: The Ramifications of The SEC's Morgan Stanley Settlement* (IAPP, Jul. 20, 2016).
76. See Press Release, *Broker-Dealer and Principals Charged With Violations Related to The Protection of Confidential Customer Information And Use of Personal Email* (SEC, Apr. 12, 2016).
77. *A.G. Schneiderman Announces $100k Settlement With E-Retailer After Data Breach Exposes Over 25k Credit Card Numbers* (Targeted News Services, Aug. 5, 2016).

- 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 to go after companies for their allowance of third-party cookies, tags, and frontline behavioral advertising.[78]

- 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.[79]

V. INTERNATIONAL DEVELOPMENTS

Although many organizations rushed to apply for the new "Privacy Shield" EU-U.S. safe harbor program, for 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.

A. The New "Privacy Shield"

On July 27, 2016, the Department of Commerce (DOC) 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.[80] 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."[81]

Applicants are required to do the following:

1. Designate a corporate representative for "all things Privacy Shield";[82]
2. Provide detailed disclosures, including on 3rd 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";[83]
3. Account for more expansive definitions of "sensitive personal information," and adopt more requests for "affirmative express consent" per European law;[84]
4. Adopt specific requirements for "onward transfers" and third-party processors, which are increased accountability and documentation requirements for controllers,85 including for when data is transferred to those who claim to be "mere processors";[86]

78. 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* (NY AG, Sept. 13, 2016).
79. Davis, *App. Developer Boosts Privacy For Kids to End Texas' Claims* (Law360, Oct. 4, 2016).
80. https://www.privacyshield.gov/welcome
81. US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles, (6) Self-Certification, Subsection (e): https://www.privacyshield.gov/article?id=6-Self-Certification.
82. US Businesses, How to Join Privacy Shield, Self Certification Information: https://www.privacyshield.gov/article?id=Self-Certification-Information.
83. US Businesses, Requirements of Participation, Privacy Shield Principles, (1) Notice: https://www.privacyshield.gov/article?id=1-NOTICE.
84. US Businesses, Requirements of Participation, Privacy Shield Principles, (2) Choice: https://www.privacyshield.gov/article?id=2-CHOICE.
85. US Businesses, Requirements of Participation, Privacy Shield Principles, (3) Accountability For Onward Transfers: https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER.
86. 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.

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;[87]

6. Agree to provide independent and free recourse mechanisms for disputing data subjects;[88] and

7. Commit to "cooperat(ing) with European Union data processing authorities (DPAs)."[89] 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.[90]

Notably, there are additional requirements for certain types of information and industries.[91]

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 General Data Protection Regulation (GDPR) (Regulation EU 2016/679), which is to be fully implemented by no later than mid-2018.[92]

B. Emerging Challenges For U.S.-Based Companies In Europe

How signing onto the Privacy Shield program will force U.S.-based companies onto 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 Ct. of Justice of the European Union (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."[93] 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 personal information (PI). In Breyer, the issue was whether even a dynamic IP address can be PI because the internet service provider (ISP) can re-identify the address assigned.[94] 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,[95] 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 lead to additional disclosure and consent requirements, all of which will 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.

87. US Businesses, Requirements of Participation, Privacy Shield Principles, (8) Access: https://www.privacyshield.gov/article?id=6-ACCESS.
88. US Businesses, Requirements of Participation, Privacy Shield Principles, (7) Recourse, Enforcement, and Liability: https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY.
89. 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.
90. 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.
91. See US Businesses, Requirements of Participation, Privacy Shield Supplemental Principles.
92. See Article 29 Working Party, Press Release dated 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.
93. Kelleher, *Kelleher: McFadden v. Sony's Implications Can't Be Ignored* (Oct. 14, 2016).
94. Grande, *IP Addresses Fall Under EU Privacy Law, Top Court Says* (Law360, Oct. 19, 2016).
95. Kelleher, *In Breyer Decision Today, Europe's Highest Court Rules On Definition of Personal Data* (IAPP, Oct. 19, 2016).

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 is known as the interpreter between the business and information technology, guiding both parties to the best result. In this role, Ron has assisted companies in navigating federal and state privacy laws for almost twenty years. Ron's experience with technology related issues, including data security, patent, antitrust, and licensing and contracts, helps bring a fresh and creative perspective to novel data compliance issues. Ron has been involved in seminal data compliance cases, assisting one of the first companies required to provide notice of a data breach and successfully defending companies in over 75 class actions. Ron also has represented companies in hundreds of individual FCRA cases involving CRAs, resellers, furnishers, users, and public record vendors. Ron has developed a reputation for assisting companies not traditionally viewed as subject to the FCRA or with FCRA compliance questions where the law remains uncertain or unresolved.

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.