DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE

QUARTERLY UPDATE, JUNE 2016

By

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

TROUTMAN SANDERS

troutmansanders.com

I. INTRODUCTION

Spring 2016 was an important quarter for privacy legislation and regulation. New legislative and regulatory proposals were unveiled for the energy sector, broadband providers, and automated cars, all purporting to improve data privacy for consumers and businesses. On the other hand, Congress continued to debate whether companies should be required to build encryption backdoors for law enforcement authorities.

The debates amongst legislators and regulators have done little to clarify the differing views amongst various circuit courts on numerous issues relating to privacy litigation. While the much anticipated *Spokeo* decision clarified that cases alleging privacy violations must necessarily also include "concrete" harm, the Supreme Court left much room for argument on other issues. And while the lower courts continued to dismiss cases alleging security breaches or data misuse, other courts permitted plaintiffs to proceed past the pleading stage.

Regulators also continued to push the boundaries of their respective authorities. In a surprising turn of events in November 2015, an FTC administrative law judge dismissed the FTC's enforcement proceeding against LabMD, finding that the evidence was wanting and that the FTC must show "likely substantial consumer injury" when bringing enforcement actions for "unfair practices."[1] The FTC was undaunted by the higher bar, however, and continued to set new precedence for what might constitute "unfair and deceptive practices." The FCC, the CFPB, and the SEC have now also joined the fray with their own privacy enforcement actions.

Lastly, despite much promise about how the U.S.-E.U. Safe Harbor program would be saved by a "Version 2.0," the E.U. has effectively rejected the most recent rendition of the "Privacy Shield" program agreed to between the U.S. and the European Commission. In addition, the E.U. has taken the position that its newly minted GDPR will apply to data practices worldwide, even if such activities arguably occur only in the U.S. It remains to be seen how far the E.U. is willing to take its efforts, such as whether it will try to impose its version of the "right to be forgotten," and prohibitions against "individual profiling."

II. NEW U.S. LEGISLATION, AMENDMENTS, AND UPDATES

Legislative and regulatory proposals involving energy, telecommunications, self-driving automobiles, and student education were all in play during the spring of 2016:

- In March 2016, the Federal Communications Commission (FCC) issued a notice of proposed rulemaking (a 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 ISP's may share their customers' information with third parties."[2] 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) "expressive, affirmative" opt-ins for "[a]ll other uses and sharing of consumer data." In addition, NPRM 16-39 would impose transparency requirements on notice, "robust security requirements," and breach notification obligations.[3]

- In April 2016, the United States Senate passed an energy bill, the Energy Policy Modernization Act, which would give the Department of Energy (DOE) significant authority to regulate the nation's power grid, supervise cybersecurity research, develop new mitigation strategies, and to step in during a cyber attack.[4] If passed into law, the bill would require the DOE to promulgate regulations requiring the protection of "critical electric infrastructure information." The bill would also require the creation of a "cyber resilience" program "to establish a cybertesting and mitigation program to identify vulnerabilities of energy sector supply chain products to known threats; to oversee third-party cybertesting; and to develop procurement guidelines for energy sector supply chain components."[5] The House of Representatives is expected now to reconcile the bill with a more politically contentious House bill passed in 2015, the North American Energy Security and Infrastructure Act of 2015.[6]

- In April 2016, the National Highway Traffic Safety Administration (NHTSA) reminded the general public of its enforcement authority under the National Traffic and Motor Vehicle Safety Act, including in the area of emerging automotive technologies such as connected and automated cars. The NHTSA, in discussing various factors it will be looking for when evaluating cybersecurity risks, also noted that cybersecurity vulnerabilities may be considered a "safety-related defect compelling a recall." Thus,"[m]anufacturers of emerging technologies and the motor vehicles on which such technology is installed have a continuing obligation to proactively indentify safety concerns and mitigate the risks of harm... Where a manufacturer fails to adequately address a safety concern, NHTSA, when appropriate, will explicitly address that concern through its enforcement authority."[7]

- Although there was no movement on any privacy legislation in Congress, states have continued to pass data privacy legislation.[8] Several states have introduced legislation to limit the collection of non-academic data by restricting the administration of surveys, prohibiting assessments that collect nonacademic data, or refusing to fund state education data systems if the system includes any nonacademic data beyond what is required for administrative purposes.[9]

- States have also been updating and revising their data breach notification laws, since no federal breach law is in sight. For example, Nebraska recently changed their laws to include account credentials as part of the definition of "personal information," joining California, Florida, Nevada, and Wyoming.[10] In addition, some have argued that Tennessee recently removed its encryption safe harbor for data breaches.[11]

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 violation. It vacated the Ninth Circuit opinion, remanding the proceedings for further determination. 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 indicated 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."[12]

On the other hand, the *Spokeo* Court merely 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."[13] Based on the Court's interjection of ambiguity into its holding, data privacy litigation on the issue of "concrete harm" will likely remain highly divisive for the next few years.

A. Data Breach Litigation

1. Challenges Based On Lack of Article III Standing

Continuing with 2015 trends, the circuit courts arguably remain 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, plaintiffs continue to survive motions to dismiss in some courts.

Critically, the Seventh Circuit 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.[14] As it has been more accepting of theories of liability not accepted in other circuits,[15] the Seventh Circuit has become one of the hotbeds of data breach litigation following *Remijas*.

Most post-*Remijas* courts in other circuits have continued to grant motions to dismiss on the basis of lack of Article III standing.[16] And even in the Ninth Circuit, which many view as being just as plaintiff-friendly as the Seventh Circuit, there continues to be great variance. While some Ninth Circuit courts have been more willing to entertain speculative theories of injury-in-fact, others refuse.[17]

Currently, it appears that courts will refuse to apply *Remijas* where plaintiffs fail to allege resulting identity fraud or theft, especially after months have passed since the data incident.[18]

2. Challenges Against Class Certification

Notably, class certification has not been granted in any consumer brought data breach cases.[19] Instead, Ninth Circuit courts continue to set precedence by striking broad class allegations where class counsel has trouble assembling class representatives who can allege out-of-pocket loss. For example, in granting Zappos' motion to strike, the District Court of Nevada held:

> In a prior order, the Court informed Plaintiffs that it "would not certify a class as broadly defined as Plaintiffs propose specifically because a majority of the putative class cannot claim any measurable damages"…Plaintiffs have failed to heed the Court's warning. The proposed class would include any person whose PII was compromised during the Zappos data breach, whether or not the person was the victim of actual fraud following the breach. The proposed class is far too broad, which prevents Plaintiffs from meeting the requirements of commonality and typicality.[20]

Cases such as *In re Zappos* demonstrate that even if plaintiffs survive a motion to dismiss, they may nonetheless have their class allegations stricken or fail to obtain class certification. Most of the theories of damages that plaintiffs have presented thus far suffer from issues of typicality, commonality, and ascertainability that will only be further exposed at the class-certification stage.

3. New Frontiers?

Plaintiffs have recently filled court dockets with product defect cases based on software vulnerabilities, alleging that businesses and their products made the consumers susceptible to cyber attacks.[21] 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. For example, while data breach cases

often struggle with "benefit of the bargain" as a theory of damages, and whether plaintiffs will be able to prove actual identity theft or fraud, restitution is less of a problem in product defect cases.

But the Ninth Circuit recently 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.[22] 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. The ruling will likely have important implications for data breach litigation, where plaintiffs typically argue that the defendant failed to follow their own promises of cybersecurity, thereby allegedly committing fraud or breaching some "implied contract."

B. Data Misuse Litigation

There is arguably greater disparity amongst the circuits regarding cases that allege data misuse. 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 assault organizations by using creative legal theories of liability. Some have even managed to obtain partial class certification.

1. Cases Alleging Misuse of User Likeness

The growth of online social networks in the past decade has created interesting legal issues where the networks intersected with ecommerce. For example, in January 2016, the Ninth Circuit Court of Appeals upheld the lower court's final approval of a $20 million settlement between Facebook and some of its users, who alleged that Facebook used its "like" feature to have users promote advertisements, thereby allegedly misappropriating the user's likeness.[23] Objecting parties have since petitioned the U.S. Supreme Court for review of the Ninth Circuit's opinion.[24]

As new technologies have been introduced into social networks, plaintiffs have also tried to leverage existing statutes that never contemplated such technologies. For example, Snapchat was sued in May 2016 for alleged violations of the Illinois Biometric Information Privacy Act (BIPA), for its use of picture modification technologies in its "snaps" and "stories."[25] Plaintiffs allege that Snapchat impermissibly collected, stored, and used biometric data without the user's knowledge or consent in direct violation of the BIPA. This case follows other BIPA suits against Shutterfly and Facebook, in Illinois and California, respectively.[26]

2. Cases Alleging Impermissible Scanning of User Messages

Facebook users have also accused the company of violating their privacy rights by illegally scanning and retaining records of the URL links sent between users in direct messages. The plaintiffs were granted partial class certification in May 2016. Plaintiffs alleged that after Facebook scanned URLs as part of a "URL preview," it created a record of the user who sent the URL, and kept a record of all global users who sent the same URL. The "shared objects" amongst the users were then used to generate "likes" on whatever the URL was linked to, third-party user recommendations for the Facebook site and applications generally, and targeted advertising for specific users.[27] The plaintiffs claimed that such practices violated the federal Electronic Communications Privacy Act (ECPA) and the California Invasion of Privacy Act (CIPA).[28]

Facebook explained that such scanning had legitimate business purposes, including anti-malware protection and industry-standard filtering for child pornography. In addition, Facebook argued that the URL data was anonymized and used only in aggregate form. The court ultimately disagreed with Facebook, on both its motion to dismiss and opposition to class certification.[29]

The court distinguished class certification between those seeking only injunctive and declaratory relief under Fed. Rules of Civ. Proc. Rule 23(b)(2) and those seeking monetary damages under Fed. Rules of Civ. Proc. Rule 23(b)(3). Class certification was granted only as to the proposed class seeking injunctive and declaratory relief under Rule 23(b)(2). The Court denied certification of the proposed Rule 23(b)(3) class, because that required plaintiffs to show that the damages are measurable on a class-wide basis, failing to demonstrate "predominance" and "superiority." And here, monetary damages would have required individualized inquiry.[30]

Notably, in response to Facebook's contention that there was "implied consent," the court differentiated *In re Google Gmail Litigation*,[31] and why there may have been implied consent in that case. The court pointed out that for the targeted advertisements in the *Gmail* case, when users clicked the ads and followed through, the ads contained disclosures indicating that they were being served "based on emails from your inbox." And in one of Google's website disclosures, Google provided that "(Google) also scans keywords in users' email which are then used to match and serve ads."[32]

3. Cases Alleging Impermissible Collection of User Connections

In Spring 2016, various mobile application companies, including co-defendants Twitter and Yelp, continued to

fight allegations that they impermissibly uploaded and disseminated plaintiffs' PII, including those from their private mobile address books.[33] In one instance involving the iOS ecosystem, for example, plaintiffs alleged that the defendant application companies did not have the right to upload and disseminate information from their private address books, because this required a circumvention of the security Apple had touted on its devices. The court previously denied defendants' motion to dismiss in March 2015.[34]

This fight follows LinkedIn's agreement to a $13 million settlement in June 2015 to resolve a purported class action for alleged impermissible "contact list harvesting." Plaintiffs had alleged that the social network application impermissibly harvested user contact lists to send out invitations to join the social network.[35] LinkedIn agreed as part of the settlement to provide more detailed disclosures.[36]

4. Cases Alleging Impermissible Tracking of User Activity

Facebook has also been under class action fire in *Facebook Internet Tracking Litigation* for allegedly continuing to track users after they logged off. Facebook then allegedly cross-referenced the webpages with Facebook "like" or "share" buttons against logged-off users, using cookies installed on the users' machines and applications.[37] In October 2015, a California court dismissed the non-statutory claims for failure to show Article III standing, but allowed plaintiffs to amend statutory claims, which had failed scrutiny only under Rule 12(b)(6). To date, the battle is still ongoing, with Facebook seeking to dismiss the amended complaint.[38]

This case should be contrasted with the Third Circuit case, *Google Tracking Litigation*.[39] After dismissing most of the causes of action against Google for its use of cookies, the Third Circuit permitted plaintiffs' California invasion of privacy tort causes of action to survive the motion to dismiss.[40] The Court argued that where Google knew that certain users employed browsers with "cookie-blockers," Google should have known that users "clearly communicated denial of consent for installation of cookies," notwithstanding whatever terms they may have agreed to or whatever settings they may have set.

Although some would say that the two cases can be distinguished based on their facts, the plaintiffs in *Facebook Internet Tracking Litigation* also alleged that Facebook had circumvented P3P "do not track" signals readable by Microsoft's Internet Explorer browser. The court dismissed the privacy claims nonetheless.[41]

The cases alleging impermissible active tracking should be contrasted with cases alleging that defendants continued to retain and utilize user information after users terminated their accounts and services. Former Time Warner Cable users had their class action tossed for lack of Article III standing, where the users alleged that Time Warner continued to retain and use their PII after the users terminated services. This allegedly violated the cable company's obligations under the Cable Communications Privacy Act (CCPA). Although the users tried to side-step more rigorous tests by seeking only injunctive relief, the court granted the motion to dismiss nonetheless, noting that the users failed to separately show "concrete" harm as required by *Spokeo*. The court noted that there were no allegations of identity theft, sale of the information to third parties, or data inaccuracies.[42] The court indicated that while the retention may be a violation under the CCPA, a mere technical violation – particularly on a first-party basis – was insufficient pursuant to *Spokeo*.[43]

5. Cases Alleging Violation of Privacy Statements

One of the most carefully watched cases is *Svenson v. Google, Inc.*, in which the plaintiffs survived a motion to dismiss in April 2015, keeping intact their causes of action based on contract and California's Unfair Competition Law (UCL). Plaintiffs alleged that Google violated its own privacy statements to Google Wallet users by sharing more information on the users with third party vendors during transactions with the vendors than Google had represented in its privacy statements. Plaintiffs managed to survive the motion to dismiss for lack of Article III standing by alleging that: (1) Google received a portion from the third party vendors for each transaction as part of the "benefit of the bargain," and (2) Plaintiffs suffered diminution of value to their PII because "[t]here is a robust market for the type of information [at issue]."[44]

Plaintiffs recently moved for class certification.[45] An order on the motion for class is expected in the third quarter of 2016. It is currently unclear whether Google will file a motion to dismiss under the new guidance from the Supreme Court in *Spokeo*, as Time Warner Cable had done, *supra*. Regardless, the outcome of the case may have significant implications for ecommerce.[46]

6. Cases Alleging VPPA Violations

The Northern District of Georgia recently granted CNN's motion to dismiss in *Perry v. Cable News Network*, a consumer class action in which the plaintiffs alleged that CNN committed a violation of the Video Privacy Protection Act[47] (VPPA) for its alleged tracking of application users using Media Access Control (MAC) addresses.[48] In finding that MAC addresses are not "personally identifiable information," this case follows a line of similar VPPA cases.[49]

On the other hand, the First Circuit refused to revisit the appeal in *Yershov v. Gannett Satellite Information Network*, where the appellate court held that using Gannett's mobile application made plaintiff a covered "subscriber" under the

VPPA. Plaintiff filed suit in 2014, alleging that Gannett violated the VPPA by tracking and analyzing videos he watched on a USA Today mobile application, although Plaintiff did not pay for the application. While the district court dismissed the case after finding that "mere use" of an application did not make plaintiff a covered subscriber, the appellate court disagreed.[50]

The *Yershov* court is in the minority on the issue of what would make someone a "subscriber" for the purposes of the VPPA, with the majority of courts requiring "something more" such as payment for service.[51] The *Yershov* court also disagreed with the *Perry* line of cases on the issue of what would constitute "personally identifiable information," finding that GPS coordinates tracked by the application was sufficient to constitute PII.[52]

Many in the industry responded with dismay in response to *Yershov*, but were somewhat assuaged with the Third Circuit's opinion in *In re: Nickelodeon Consumer Privacy Litigation*, where the appellate court mostly endorsed the majority view on what constitutes PII. Plaintiffs alleged that Google and Viacom shared PII as part of affiliate marketing for the website Nick.com. The appellate court found that even if defendants tracked and then shared IP and MAC addresses, they were not disseminating PII under the VPPA.[53] In addition, the court noted that the VPPA only permits suit against the disclosing entity, but not the receiving entity.[54]

Notably, plaintiffs have already began suing "smart TV" manufacturers and their software partners for their collection of data through the voice recognition input components of the televisions. These cases, mostly involving Vizio for now, include VPPA allegations.[55]

IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

A. The Federal Trade Commission

In November 2015, an FTC administrative law judge dismissed the FTC's enforcement proceeding against LabMD, finding that the FTC must show "likely substantial consumer injury" when bringing enforcement actions for "unfair" practices" under Section 5 of the Federal Trade Commission Act (the FTC Act).[56] The FTC was undaunted by what most commentators viewed as a higher threshold, and continued to set new precedence for Section 5 enforcement:

- *In re Gigats.com*: In the FTC's first enforcement action against an education lead generator, Gigats.com agreed to settle charges against it 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.[57]

- *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.[58] 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 customers, that the "update" did not remove prior versions of Java SE. This case, along with *In re Henry Schein Practice Solutions*, *supra*, demonstrate that the FTC is continuing to provide guidance to the software security market of best practices through settlements.

- *In re "Silverpush" Code*: 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.[59]

- *In re Very Incognito Technologies, Inc., d.b.a. 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 E.U. The CBPR facilitates the transfer of PII between APEC and E.U. 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 E.U. authorities that it intends to diligently enforce the various E.U.-sanctioned data transfer programs.[60]

- *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."[61] 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 device's privacy settings. The FTC alleged that InMobi in fact tracked consumers, including children, regardless of whether they opted in or denied permissions in their settings, which also violated the Children's Online Privacy Protection Act (COPPA).[62] As with the FTC's proceedings against Nomi Technologies last year,[63] *In re Mobi* will have important implications for the internet of things (IoT). Cross-device and cross-platform issues have become increasingly problematic, with great variance on the type of consumers involved, the privacy statements made across applications and platforms, and lack of consistency amongst partners and third-party affiliates.

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)."[64] In June 2016, an appellate court affirmed the FCC's classification of broadband as a telecommunications service, thereby applying common carrier regulations to such services.[65]

Continuing to demonstrate its interpretation of Section 222 of the Communications Act of 1934, the FCC announced in March 2016 that it reached an agreement with Verizon for a $1.35 million consent decree, for Verizon'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."[66] This case demonstrates that the FCC intends to police wireless carriers very aggressively, likely even more aggressively than the FTC.

Although the FCC and FTC have at times publicly criticized each other for overstepping their respective jurisdictions, they have also been more aggressively 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.[67] 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.[68]

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 Health Insurance Portability And Accountability Act (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.[69]
- New York Presbyterian Hospital – $2.2 million for allegedly allowing crew members from ABC to film patients without their consent.[70]
- 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.[71]
- Raleigh Orthopedic Clinic –$750,000 for allegedly failing to secure a business associate agreement before handing patient data over to a potential business partner.[72]

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.[73] It remains to be seen how audited business associate relationships will fare, especially since they have only been covered by HIPAA since 2013.[74]

Notably, the FTC has been actively trying to get ahead of the development of health wearables. Not only did the FTC hold a number of workshops on IoT, but it also released a "Mobile Health Apps Interactive Tool" in April 2016.[75]

D. Other Administrative Enforcement Efforts

In addition to the FTC, the FCC, and the OCR/HHS, a number of other regulators are increasing their efforts in the data privacy arena. In May 2016, Paypal settled with the Texas Attorney General 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.[76]

In June 2016, the Security and Exchange Commission (SEC) announced that Morgan Stanley Smith Barney agreed to pay $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."[77]

The Consumer Financial Protection Bureau (CFPB) has also 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.[78]

V. INTERNATIONAL DEVELOPMENTS

The European Parliament formally adopted the General Data Protection Regulations (GDPR) on April 14, 2016.[79] The GDPR is set to take effect in two years, and is admittedly the most comprehensive privacy regulation in the world. At the same time, some wonder whether Europe has become so entangled in regulations that it discourages foreign investments.

A. "Privacy Shield" Will Likely Need Overhaul

As of Spring 2016, the E.U.-U.S. Privacy Shield program is unlikely to remain as previously announced by the FTC. After the FTC's announcement, authorities in both Germany and France immediately began prosecuting U.S.-based international companies for violations.[80]

Numerous E.U. organizations also protested and criticized the Privacy Shield, arguing that it is only a slight improvement over the now expired Safe Harbor, and asking the Article 29 Working Party to recommend renegotiations.[81] On April 13, 2016, the Article 29 Working Party formally recommended that the deal be renegotiated for improvements.[82] Additional developments are expected in July.[83]

B. Model Clauses Are Likewise Challenged

Organizations in the United States should be aware that it is not just the Privacy Shield program that is under scrutiny, but model clauses as well. 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 reportedly recommended referral of the case to the Court of Justice of the European Union.[84]

VI. CONCLUSION

As we move into the next quarter, we will begin to see the impact of *Spokeo* in class action privacy litigation. And *Spokeo* itself has yet to be fully adjudicated, as it remains to be seen how the Ninth Circuit will decide the remanded case, and whether it will ultimately find plaintiff's harm "concrete and particularized."

Regulatory agencies, including the FCC, FTC, CFPB, OCR/HHS and SEC, are expected to continue to aggressively increase their enforcement efforts in the privacy arena. We expect greater collaboration amongst the agencies, although the bounds of each agency's jurisdiction have yet to be fully explored and decided.

Further, as the E.U. and the U.S. continue to grapple over the "Privacy Shield," the E.U. will begin to apply its newly-minted GDPR to data practices worldwide. It remains to be seen, however, just how far the E.U. will take its efforts, and whether and what impact the GDPR might have on reaching an agreement on the Privacy Shield. Spanish data protection authorities have already begun arguing that Google's servers in California are subject to its authority.[85]

Similarly, the E.U. Advocate General recently issued an opinion that dynamic IP-addresses are PII.[86] Hopefully, such overly expansive definitions will not be adopted formally, lest technology investments only be further stifled in Europe.

ENDNOTES

1 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).

2 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).

3 Press Release, *FCC Proposes to Give Broadband Consumers Increased Choice Transparency and Security For Their Personal Data* (FCC, Mar. 31, 2016).

4 Davenport, *Senate Passes Legislation Tailored to a Modern Energy Landscape* (New York Times, Apr. 20, 2016).

5 Note that Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) currently have standards and requirements in place for electric power and power grids. NERC's current rules and regulations on Critical Infrastructure Protection (CIP) standards can be located at: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Not only does FERC work with NERC on reliability standards, but FERC is actively working with the National Institute of Standards and Technology (NIST) to incorporate information technology standards into the smart grid as well. See FERC's website at: http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.

6 S.2012 – North American Energy Security And Infrastructure Act of 2016, available at: https://www.congress.gov/bill/114th-congress/senate-bill/2012/text#toc-H9F1807490C324DB9818E07BA6E034610.

7 Fed. Reg. Vol. 81, No. 63, p. 18938-18939 (Apr. 1, 2016).

8 Breitenback, *States Scramble to Protect Student Data And Privacy* (PBS News Hour, Jun. 9, 2016).

9 *Student Privacy Legislative Update – June 23, 2016* (IAPP).

10 Hoyme, *Nebraska Amends Data Breach Notification Law* (JDSupra.com, May 4, 2016).

11 McClure, *Tennessee Amends Data Breach Notification Law – Removes Encryption Exemption (or Does It?)* (Wyatt Tarrant & Combs LLP, Apr. 4, 2016) (noting that the definition of "personal information" at T.C.A. §47-18-2107(3) still provides "when either the name or the data elements *are not encrypted*").

12 *Spokeo, Inc. v. Robins,* 578 U.S. ___, at *7-10 (May 16, 2016).

13 *Id.*, at *8-10.

14 *Remijas v. Neiman Marcus Group*, 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 China Bistro*, 819 F.3d 963, 2016 U.S. App. LEXIS 6766, *4-8 (7th Cir. 2016) (accord, citing to same reasoning in *Remijas*).

15 See e.g., *Irwin v. Jimmy John's Franchise*, 2016 U.S. Dist. LEXIS 48162, *7-9 (N.D. Il. March 29, 2016) (dismissing most causes of action, but permitting some causes of action to survive, including one based on "implied contract"); see also *Allen v. Schnuck Markets, Inc.*, 2015 U.S. Dist. LEXIS 113892 (S.D. Ill. Aug. 27, 2015). (denying motion to dismiss, including claims based on implied contracts); contrast with *Longenecker-Wells v. Benecard Services, Inc.*, *17-20 (M.D. Penn. Sept. 22, 2015) (granting motion to dismiss for failure to state a viable claim, including a cause of action based on implied contract arising from employment, finding the allegations "implausible" as "the defendants might anticipate that they are likely to experience data breaches, regardless of what preventative measures have been taken").

16 See *Whalen v. Michael Stores, Inc.*, 2015 U.S. Dist. LEXIS 172152, *14-15 (E.D. N.Y. Dec. 28, 2015) (refusing to apply *Remijas*, and noting that plaintiffs only alleged that the putative class representative was affected, but even then, she did not suffer out-of-pocket losses); accord *In re SuperValu, Inc.*, 2016 U.S. Dist. LEXIS 2592 (D. Minn. Jan. 7, 2016), *11-19 (citing *Whalen*, amongst

ENDNOTES *continued ...*

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"…); *Khan v. Children Nat'l Health Sys.*, 2016 U.S. Dist. LEXIS 66404, *12-16 (D. Mary. May 19, 2016) (granting motion to dismiss, and distinguishing *Remijas*); see *Chambliss v. CareFirst, Inc.*, 2016 U.S. Dist. LEXIS 70096, *11-13 (D. Mary, May 27, 2016) (granting motion to dismiss, and again distinguishing *Remijas*).

17 Compare *In re Anthem Data Breach Litig.* 2016 U.S. Dist. LEXIS 18135 (N.D. Cal. Feb. 14, 2016) and 2016 U.S. Dist. LEXIS 70594 (N.D. Cal. May 27, 2016) (denying motion to dismiss on various theories of liability not recognized by other courts, such as the "inherent value of PII"), and *Patton v. Infosearch.com LLC.* 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 PII).

18 See e.g., *Whalen*, 2015 U.S. Dist. LEXIS 172152, *13-15; *In re SuperValu*, 2016 U.S. Dist. LEXIS 2592, *13-15; *In re Zappos.com, Inc. Custom Data Security Litigation*, 2016 U.S. Dist. LEXIS 60453, *26-28 (D. Nev. May 6, 2016); *Khan*, 2016 U.S. Dist. LEXIS 66404, *15-17; *Chambliss*, 2016 U.S. Dist. LEXIS 70096, *9-11.

19 Gerner et al., *Illinois Breach Decisions Show It's Not Just About Standing* (Law360, Apr. 21, 2016) [noting for example, *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 293 F.R.D. 21(D. Maine, Mar. 20, 2013) (denying class certification)].

20 *In re Zappos.com, Inc. Custom Data Security Litigation*, 2016 U.S. Dist. LEXIS 60453, *26-28; see also *Baum v. Keystone Mercy Health Plan And Amerihealth Mercy Health Plan*, 2016 Pa.Super.Unpub. 1358 (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).

21 See e.g., Trader, *Drivers in Fiat Car Hacking Suit Say Their Injuries Are Real* (Law360, March 22, 2016) (on hackable car case, *Flynn v. FCA US LLC*, S.D. Ill. Case No. 15-00855); see also Salvatore, *ADT Says Alarm Hackability Suit Fails For Lack of Examples* (Law360, Jun. 6, 2016) (on hackability of home security services, *Edenborough v. ADT LLC,* N.D. Cal. Case No. 16-02233).

22 *Haskins v. Symantec Corp.*, 2016 U.S.App. LEXIS 11105 (Jun. 20, 2016).

23 2016 U.S. App. LEXIS 518 (9th Cir.). In the underlying case, *Fraley v. Facebook*, N.D. Cal. Dist. Ct. Case No. 11-CV-01726, the court held that there was Article III standing because California statutorily guaranteed publicity rights pursuant to Cal. Civ. Code Section 3344. 830 F.Supp.2d 785, 799-801 (N.D. Cal. 2011). See also *Perkins v. LinkedIn Corp.*, 53 F.Supp.3d 1190, 1208-1209 (N.D. Cal. 2014), citing to *Fraley* in case alleging LinkedIn impermissibly "harvested" user contacts to send out invitations "endorsing" LinkedIn for more sign-ups. Importantly, all of these cases preceded the *Spokeo* case.

24 Daniels, *Facebook's $20M User Privacy Deal Challenged At High Court* (Law360, May 31, 2016).

25 *Martinez v. Snapchat, Inc.*, Sup. Ct. of Cal., Los Angeles, Case No. BC-621391.

26 Grande, *SnapChat's Facial Data Gathering Flouts Ill. Law, Suit Says* (Law360, May 25, 2016).

27 Brandom, *Lawsuit Claims Facebook Illegally Scanned Private Messages* (TheVerge.com, May 19, 2016).

28 *Campbell v. Facebook, Inc.*, 2016 U.S. Dist. LEXIS 66267 (N.D. Cal. May 18, 2016).

29 Trader, *Facebook Users Get Partial Class Cert. In Scanning Case* (Law360, May 19, 2016)

30 *Campbell*, 2016 U.S. Dist. LEXIS 66267, *33-35, citing to *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 623, and *Comcast Corp. v. Behrend*, 133 S.Ct. 1426, 1423 (2013).

31 2014 U.S. Dist. LEXIS 36957 (N.D. Cal. Mar. 18, 2014).

32 *Campbell*, 2016 U.S. Dist. LEXIS 66267, *37-42.

33 Trader, *App Users Push Back At Yelp's Bid to Escape Privacy Suit* (Law360, June 6, 2016).

ENDNOTES *continued ...*

34 *Opperman v. Path*, 84 F.Supp.3d 962 (2015).

35 *Perkins v. LinkedIn Corp.*, N.D. Cal. Dist. Ct. Case No. 13-CV-04303.

36 Godoy, *LinkedIn Pays $13M to Settle Email Harvesting Class Action* (Law360, Jun. 12, 2015).

37 *In re Facebook Internet Tracking Litigation*, N.D. Cal. Dist. Ct. Case No. 12-MD-02314.

38 Sieniuc, *Facebook Defends Bid to Toss $15B Tracking MDL* (Law360, Jun. 13, 2016).

39 806 F.3d 125 (3rd Cir. Nov. 10, 2015); affirmed as precedence post-*Spokeo* in *In re: Nickelodeon Consumer Privacy Litigation*, D.N.J. Case No. 15-1441 (Jun. 27, 2016), *72-73 (noting where children are involved, plaintiffs alleging that companies have violated their own privacy statements may have alleged sufficient intrusion upon seclusion to have established Article III standing, even under a post-*Spokeo* analysis).

40 See *In re Google, Inc. Cookie In Placement Consumer Privacy Litigation*, 806 F.3d 125 (3rd Cir. Nov. 10, 2015) [request for rehearing on motion to dismiss denied on December 11, 2015]. The case was settled in June 2016, after plaintiffs petitioned to the Supreme Court the 3rd Circuit's decision. Lowrey, *Google Inks Deal With Web Users In Browser-Tracking MDL* (Law360, Jun. 21, 2016).

41 *In re Facebook Internet Tracking Litigation*, 2015 U.S. Dist. LEXIS 145142, *20-21 (N.D. Cal. Oct. 23, 2015), N.D. Cal. Dist. Ct. Case No. 12-MD-02314, p. 5:5-9.

42 *Gubala v. Time Warner Cable, Inc.*, 2016 U.S. Dist. LEXIS 79820, *12-15 (E.D. Wis. Jun.. 17, 2016).

43 *Id.*, *13-14. Interestingly, another district court arguably reached the opposite conclusion on how *Spokeo* should be applied – at least as to third party use – in a case alleging that Hearst Communications violated the Michigan Video Rental Privacy Act (VRPA) by selling customer data without their consent, although Hearst argued that *Spokeo* should apply because plaintiffs suffered no concrete damages. Salvatore, *Hearst Can't Escape Privacy Suit Over Customer Data* (Law360, Jun. 17, 2016) (reporting on *Edwards v. Hearst Communications, Inc.*, Case No. 15-09279.

44 *Svenson v. Google, Inc.*, 2015 U.S. Dist. LEXIS 43902, *5-6 (Apr. 1, 2015); but see *Haskins v. Symantec Corp.*, 2016 U.S.App. LEXIS 11105 (June 20, 2016) (finding that UCL claims for software vulnerabilities required reliance).

45 Lowrey, *Google Android Users Urge Judge to Certify Class of Millions* (Law360, Jun. 6, 2016).

46 But see *In re Facebook Privacy Litig.*, N.D. Cal. Case No. 10-02389 (Jun. 29, 2016) (denying class certification in redacted order, in case alleging Facebook violated its own privacy statement by sharing plaintiffs' information). Given its likely impact on cases like *Svenson*, we expect clarification on the basis in the next few weeks.

47 18 USC §2710 *et al.*

48 *Perry v. Cable News Network, Inc.*, N.D. Ga. Case No. 1:14-cv-02926-ELR, at *2 (Apr. 20, 2016).

49 *Eichenberger v. ESPN Inc.*, 2015 U.S. Dist. LEXIS 157106 (W.D. Wash. May 5, 2015); *Robinson v. Disney Online*, 2015 U.S. Dist. LEXIS 142486 (S.D.N.Y. Oct. 20, 2015); *Locklear v. Dow Jones & Co.*, 101 F. Supp. 3d 1312 (N.D. Ga. 2015), *abrogated on other grounds*, 803 F.3d 1251 (11th Cir. 2015); *Ellis v. Cartoon Network. Inc.*, 2014 U.S. Dist. LEXIS 143078 (N.D. Ga. Oct. 8, 2014), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015); *In re Nickelodeon Consumer Privacy Litig.,* 2014 U.S. Dist. LEXIS 91286 (D.N.J. July 2, 2014); *In re Hulu Privacy Litig.*, 2014 U.S. Dist. LEXIS 59479 (N.D. Cal. Apr. 28, 2014).

50 *Yershov v. Gannett Satellite Inf. Network*, 2016 U.S.App. LEXIS 7791, *10-15 (1st. Cir. Apr. 29, 2016) (but recognizing difference with 11th Circuit, in *Ellis v. Cartoon Network*. supra).

51 See *Ellis v. Cartoon Network. Inc.*, 803 F.3d 1251 (11th Cir. 2015)[finding plaintiff was not a "subscriber"]); *Austin-Spearman v. AMC Network Entm't LLC*, 98 F. Supp. 3d 662 (S.D.N.Y. 2015) (accord with *Ellis*); *In re Hulu Privacy Litig.*, 2012 U.S.Dist. LEXIS 112916 (N.D. Cal. Aug. 10, 2012) (same).

ENDNOTES *continued ...*

52 *Yershov*, 2016 U.S.App. LEXIS 7791, *6-9.

53 *In re: Nickelodeon Consumer Privacy Litigation*, D.N.J. Case No. 15-1441, *60-62, Order on June 27, 2016; but see courts' discussion in *id.*, at fn. 174 [disagreeing with precedence such as *Hulu* in dicta and noting that "even a numeric identifier might qualify as personally identifiable information, at least in certain circumstances"].

54 *Id.*, at *41-42.

55 See *Reed v. Cognitive Media Networks et. al.*, Case No. 15-05217 (N.D. Cal. Nov. 13, 2015) (suing Vizio and its software partner); *Hodges v. Vizio*, Case No. 15-02090 (C.D. Cal. Dec. 16 2015); *Mason v. Vizio Holdings*, Case No. 15-11288 (N.D. Ill. December 15, 2015); and *Ogle v. Vizio*, Case No. 15-00754 (E.D. Ark. Dec. 10, 2015).

56 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).

57 Press Release, *FTC Charges Education Lead Generator With Tricking Job Seekers By Claiming to Represent Hiring Employers* (FTC April 28, 2016).

58 Press Release, *FTC Approves Final Order In Oracle Java Security Case* (FTC, Mar. 29, 2016).

59 Press Release, *FTC Issues Warning Letters to App Developers Using "Silverpush" Code* (FTC, Mar. 17, 2016).

60 Press Release, *Hand-Help Vaporizer Company Settles FTC Charges It Deceived Consumers About Participation In International Privacy Program* (FTC, May 4, 2016).

61 Press Release, *FTC Approves Final Order In Henry Schein Practice Solutions Case* (FTC, May 23, 2016).

62 Press Release, *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission* (FTC, Jun. 22, 2016).

63 Press Release, *FTC Approves Final Order In Nomi Technologies Case* (FTC, Sept. 3, 2015)

64 *In the Matter of Protecting And Promoting the Open Internet,* FTC GN Docket No. 14-28, Mar. 12, 2015 Report and Order on Remand, Declaratory Ruling, and Order.

65 Davis, *Court Empowers FCC to Address Broadband Privacy, Data Caps* (The Daily Online Examiner, Jun. 14, 2016) [on *US Telecom Ass'n v. FCC*, D.C. Cir. Case No. 15-1063, Order on June 14, 2016).

66 *In the Matter of Cellco Partnership, d.b.a. Verizon Wireless*, FTC File No. EB-TCD-14-00017601, Mar. 7, 2016 Order.

67 Frankel, *Comcast, Cablevision and AT&T Violating Privacy Through Addressable Advertising, Groups Say* (Fiercecable.com Jun. 9, 2016).

68 Statt, *The FCC And FTC Are Investigating How Companies Release Mobile Security Patches* (The Verge, May 9, 2016).

69 Press Release, *Improper Disclosure of Research Participants' Protected Health Information Results In $3.9 Million HIPAA Settlement* (HHS, Mar. 17, 2016).

70 Kennedy, *NY Hospital Will Pay $2.2M For Violating HIPAA On TV* (Law360, Apr. 21, 2016).

71 Press Release, *$1.55 Million Settlement Underscores The Importance of Executing HIPAA Business Associate Agreements* (HHS, Mar. 16, 2016).

72 Lagasse, *An Orthopedic Clinic Pays $750,000 Over HIPAA Violation Surrounding Improper Patient Data Sharing* (Healthcareitnews.com, Mar. 15, 2016).

ENDNOTES *continued ...*

73 *OCR Launches Phase 2 of HIPAA Audit Program*, available at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html

74 Overley, *Feds Launch Long-Awaited HIPAA Audits* (Law360, Mar. 21, 2016).

75 Located at: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

76 Roberts. *Venmo Likely Investigated Over User Privacy Violations* (Fortune.com, May 24, 2016).

77 Godoy, *SEC Fines Morgan Stanley $1M For Data Security Failures* (Law360, Jun. 8, 2016).

78 *In the Matter of: Dwolla, Inc.*, CFPB File No. 2016-CFPB-0007, Consent Order dated March 2, 2016.

79 Bracy, *MEPS Finalize GDPR, DPD* (IAPP Arp. 14, 2016).

80 Piltz, *Hamburg Data Protection Watchdog Fines International Companies For Illegal Data Transfers* (Delegedata.de, Jun. 6, 2016).

81 *IAPP Asia-Pacific Dashboard Digest: Privacy Groups Want Renegotiation of Privacy Shield* (IAPP, Mar. 17, 2016).

82 Bracy, *WP29 Says Privacy Shield Needs Improvements* (IAPP Apr. 13, 2016).

83 Kelleher, *For Data Transfers, Uncertainty Is The Only Certainty* (IAPP, Jun. 9, 2016).

84 Bracy, *Model Clauses In Jeopardy With Irish DPA Referral to CJEU* (IAPP, May 25, 2016).

85 *For Data Transfers, Uncertainty Is the Only Certainty, supra*.

86 Kuschewsky, *E.U. Advocate General Considers Dynamic IP Addresses to Be Personal Data* (Covington & Burling LLP, May 13, 2016, reporting on *Breyer v. Germany*, E.U. Ct. of Justice, Case C-582/14.

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.