DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE

FEBRUARY 2016

By

Mark C. Mao, **Ronald Raether**, **Ashley Taylor**,
Sheila Pham, **Sofia Jeong**, **Reade Jacob**, **Ryan Lewis**,
Julie Hoffmeister, and **Jessica Lohr**

TROUTMAN SANDERS

troutmansanders.com

I. INTRODUCTION [1]

A. An Overview of Privacy Law In The United States

Privacy law in the United States is generally viewed as following a "sectoral model." Unlike the European Union (EU) and Canada, the US does not have comprehensive national legislation covering all industries. Specific privacy statutes govern only some sectors; otherwise, only certain general activities are regulated. Under such a regime, spotting issues can be tricky.

As a result, when analyzing privacy issues in the US, it is best to first consider whether the issue occurs in the context of a covered sector. If not, one should then consider whether the issue involves a covered activity. Even after this step, the analysis is not complete. It is necessary to consider state laws regulating certain types of information, such as social security numbers and biometric information.

Sector-specific privacy statutes relate primarily to (a) health services, (b) financial services, (c) education, (d) telecommunications, and (e) utilities. Each of these statutory schemes generally provides consumers with rights to notice, access, and correction of their personally identifiable information (PII). The statutes, and the rules promulgated by the agencies enforcing them, also typically require that covered entities implement reasonable security measures to safeguard the PII.

In the area of health services, the most influential statute is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended and supplemented by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). These primarily apply to "covered entities" and their "business associates."

Federal regulation of the financial services sector is focused on the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), the Gramm-Leach-Bliley Act (GLBA), the Dodd-Frank Wall Street Reform and Consumer Protections Act (Dodd-Frank), and various anti-money-laundering laws. As with medical privacy, the entities to which these laws apply can be rather specific.

In the education arena, emphasis is on the Family Educational Rights and Privacy Act of 1974 (FERPA), as supplemented by the Protection of Pupil Rights Amendment (PPRA). These laws have the broadest application to schools that receive federal funding. Notably, Congress is currently debating different versions of bills for use of data from secondary and university educational institutions, and nearly 200 bills are being considered in the state legislatures.[2]

Telecommunication entities such as "(telecommunication) carriers," cable television, and "video tape service providers" are also subject to federal legislation. Notably, authorities have recently widened the scope of entities subject to regulation. For example, the Telecommunications Act of 1996 had long been interpreted to exclude broadband internet services from the definition of "telecommunications service." But the scope is now subject to intense debate due to a reverse in course by the Federal Communication Commission (FCC), after it held that a mobile broadband provider could be a regulated "carrier," pursuant to Section 222 of the Act.[3] As a result, a broader group of entities must be sensitive to the Act's limitations on the right of carriers to use "customer proprietary network information."

Similarly, the Video Privacy Protection Act of 1988 (VPPA) has become the topic of controversy due to judicial findings that streaming services such as Netflix – technologies that were not available at the time of passage of the act – may qualify as "video tape service providers."[4] Much like the Cable Television Privacy Act of 1984, which governs cable providers, VPPA prohibits "video tape service providers" from disclosing customer personal information unless an enumerated exception applies, or unless providers have obtained consent in the required form.

Privacy laws for utility power grids are a more recent development. As of the date of this publication, Congress is deliberating legislation on the establishment of open standards for power grids that enhance connectivity and interoperability of power grids, while integrating Fair Information Practice Principals (FIPPs).[5] The federal proposals under consideration trail similar efforts by the various states, as approximately a dozen states now have legislation governing power grids with privacy provisions.[6]

For these regulated industries, 2015 was littered primarily with regulatory orders and enforcement actions, in addition to developments in civil litigation. Although existing statutes remained in place, regulators sought to increase their powers in existing areas and reach into emerging technologies.

As for privacy laws covering specific activities, such activities generally relate to (a) marketing, (b) credit reporting, (c) transmission of electronic information, and (d) criminal activities and investigation. Marketing laws have broad applications, as they prohibit certain types of marketing and can apply generally to any organization engaged in the covered activities. Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of

2003 (CAN-SPAM) to address the use of email for marketing purposes. The Federal Communication Commission (FCC) and the Federal Trade Commission (FTC) also regulate telemarketing activities such as "robocalls" and "texting" pursuant to the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud Abuse Prevention Act (TCFAPA).

Until recently, the Fair Credit Reporting Act of 1970 (FCRA) was generally confined to situations requiring background checks used for credit, housing, and employment applications. Thus, FCRA was viewed as part of the sectoral laws governing financial institutions. But with the advent of new data technologies, the FTC and courts have increasingly held that organizations selling services based on new technologies may potentially be "consumer reporting agencies" and likewise, businesses employing such services may be using covered "consumer reports." The FCRA has numerous requirements on notice, access, and correction.

Privacy-focused federal regulations also apply to certain facets of electronic information transmission. The Electronic Communications Privacy Act of 1986 (ECPA) generally prohibits the interception of electronic communications. The Stored Communications Act (SCA) was enacted as part of the ECPA in 1986 to regulate the unauthorized acquisition, alteration, and blocking of electronic communications while in electronic storage.

Lastly, in light of the Snowden revelations, the USA Freedom Act was signed in mid-2015 to require greater transparency and accountability in government searches and seizures. The Act ended the bulk collection programs conducted by the National Security Agency (NSA), previously permitted pursuant to the US Patriot Act. Procedurally, authorities are now required to provide greater specificity and limits regarding their investigative requests, and investigative courts established pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA) may need to seek independent advisors for certain requests. Private companies subject to investigative requests are now provided greater opportunity to publicly report information about the number of FISA orders they receive.

In light of the terrorist attacks of Paris, Congress passed the Cybersecurity Information Sharing Act (CISA) in late December 2015, which will permit organizations to share information about cybersecurity threats with lessened fear of prosecution, even if it implicates trade secrets. However, CISA passed amidst a countervailing movement against "Big Brother," pushed particularly by technologists that argue "info-sharing" is synonymous with intentionally creating backdoors for hackers.[7]

B. Trends In 2015 Continue Into 2016

As will be discussed herein, regulators continue to be the main policymakers of privacy law in the United States. As the most active policymaker, the FTC suffered some significant setbacks in 2015, but looks to aggressively push into new areas and technologies in 2016. Other agencies, such as the FCC and SEC, are emerging as allies.

Outside of the regulatory context, however, those who claim to be "privacy advocates" have enjoyed only mixed success. While some courts have accepted new arguments to deny motions to dismiss in data breach litigation, claimants continue to have difficulty proving damages and establishing standing. Similarly, although claimants are finding some success in impermissible "tracking" cases, damages continue to be a significant issue, as will class certification.

Other trends of 2015 are likely to continue in 2016. Despite rhetoric, legislators appear to recognize the importance of data analytics in the growth of American technologies and ecommerce in the past two decades. And as emerging technologies such as automation, augmented reality, and the "internet of things" (IoT) grow in importance, the availability of data analytics will only be increasingly more important.

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

Most of the federal legislative activities in 2015 have been in the area of the government's right to search and request information. Despite early attempts to create comprehensive federal data security and breach legislation,[8] such efforts will likely remain unfinished until after the new President comes into office in 2017.

On a state level, privacy advocates advanced numerous proposals affecting educational privacy. In addition, states such as California continued to advance privacy laws regulating issues arising in emerging technologies.

A. The USA Freedom Act

In mid-2015, President Obama signed into effect the USA Freedom Act,[9] which modified the US Patriot Act. The US Patriot Act had previously modified the Foreign Intelligence Surveillance Act of 1978 (FISA),[10] which had created special courts that could issue "discovery orders" based on probable cause of a crime involving a "foreign power" or "an agent of a foreign power." Discovery orders included wiretaps, pen registers/traps, trace orders, and electronic discovery.

The USA Freedom Act sought to necessitate greater transparency and accountability in the discovery order process. The Act ended the recent bulk collection conducted by the National Security Agency (NSA), subject to a short allowance for the transition. Authorities are now required to provide greater specificity and limits regarding their investigative requests:

- Title I requires that FISA court orders approving the production of "tangible things" must include "each specific selection term used as a basis for such production." FISA courts can no longer authorize the collection of tangible things by the government without the use of a specific selection term.
- Title I requires that government applications for the ongoing production of call detail records must show "reasonable grounds" that the records "are relevant," and "a reasonable, articulable suspicion" that the "specific selection term" is associated with a foreign power or terrorist activities.
- Title II requires that government applications for orders approving pen registers and trap and trace devices include a "specific selection term" as in Title I.
- Title III places limits on how the government can use "unlawfully obtained information."
- Title V reforms existing legislation to require government agencies to use specific selection terms as the basis for issuance of national security letters.

Lastly, FISA courts need to seek independent advisors in certain situations, and there is now more public access to the opinions of the judges of these courts. Likewise, private companies subject to requests are provided greater opportunity to publicly report information about the number of FISA orders they receive.

B. The Cybersecurity Information Sharing Act of 2015

CISA is Title I of the Cybersecurity Act,[11] which was signed into law by President Obama as part of a larger omnibus bill passed at the end of 2015. The intent of the bill was to allow private organizations to share and collaborate on cybersecurity threats to prevent attacks and terrorism.

Information-sharing is centralized in the Department of Homeland Security. Although there are broad safe harbors to protect organizations from liability, such protections require organizations to share information "in accordance" with CISA. Where the sharing is qualified for CISA protections, not only is there no civil liability, but regulatory liability could also be limited.

However, private entities must review the information to be shared and remove any information that the entity "knows at the time of sharing" to be personal or personally identifiable information (PII) not directly related to a cybersecurity threat. Privileges and other protections would not be waived as a result of the sharing of information.

On the other hand, there is no duty to share, and CISA does not create a duty to warn or act. CISA does not prevent the government from using an organization's non-participation as part of a future lawsuit for failure to maintain or secure. It also does not expressly provide liability protections for a decision not to use the information to improve cybersecurity defenses.

Another caveat is that the government's use of the shared information is not necessarily limited to cybersecurity purposes. For example, the information may be disclosed, retained, and used to: (1) respond to, prevent, or mitigate a specific threat of

death, or serious bodily or economic harm, including a terrorist act; (2) respond to, investigate, prosecute, prevent, or mitigate a serious threat to a minor, any offense arising out of the same; and (3) for certain offenses relating to fraud, identity theft, espionage, censorship, or the protection of trade secrets.

Perhaps most importantly, CISA authorizes private entities to use defensive measures for cybersecurity purposes on their own information systems and those of other consenting entities. In addition, CISA explicitly shields private entities from any liability for monitoring activities conducted in a manner consistent with CISA's requirements. Both requirements can affect how organizations structure their privacy policies and consumer-facing statements.

Lesser known are CISA provisions that can affect organizational implementation of what is commonly known as the HIPAA "Security Rule." Section 405 of Title IV directs the U.S. Department of Health and Human Services' secretary to establish and regularly update a set of voluntary cybersecurity "best practices." Although these voluntary practices must be consistent with the Security Rule, they may also end up being more specific than and inconsistent with current industry practices.

C. Other Significant Legislative Developments

1. Driverless & "Smart" Cars

Nevada was the first state to authorize self-driving cars in 2011, and since then five other states have joined. Sixteen states introduced legislation relating to autonomous vehicles in 2015, although most proposals either need to be revived or are still awaiting further deliberation.[12]

In January 2016, the Department of Transportation (DOT) entered into an agreement with 17 major automakers to enhance driver safety, including sharing information to thwart cyber-attacks on wired vehicles.[13] The agreement included the sharing of best practices, lessons learned, and research, in order to identify emerging threats, in areas such as hacking. The agreement also included an announcement from the DOT that the Obama Administration plans to award approximately $4 million in grants to fund demonstration projects that would assist in the development of self-driving cars. According to the agreement, the National Highway Traffic Safety Administration (NHTSA) will propose industry principles by July 2016.

2. Power Grids

To date, approximately a dozen states have statutes or proposals to protect power grids against disruption. The regulations seek not only to protect infrastructure from terrorist attacks, but to also protect against hackers and criminals.[14] California's Cal. Civ. Section 1798.98, for example, prohibits utilities from sharing consumer electricity and gas usage information without consent, and requires the implementation of reasonable security to safeguard that information.

In May 2015, the US Senate introduced Senate Bill No. 1232 to establish a Smart Grid Interoperability Working Group and to promote "the establishment and adoption of open standards that enhance connectivity and interoperability on the electric grid." The bill included other initiatives as well, such as a directive to identify and promulgate Fair Information Practice Principles (FIPPs) for "the collection, use, disclosure, and retention of individual customer information."[15]

3. Education Privacy

In 2015, 47 states introduced a total of nearly 200 bills addressing student privacy, with 15 states passing student privacy laws.[16] President Obama also called for legislation at the federal level to enhance student data safeguards under the Family Educational Rights and Privacy Act (FERPA).

Before California's Student Online Personal Information Protection Act (SOPIPA) was passed,[17] FERPA put the primary compliance burdens of lawful disclosure on the schools themselves. Generally, student data was to be protected from disclosure unless consent of the parent or eligible student was provided to the school. Where the contractor de-identified the data, the data was arguably not FERPA protected.[18] Thus, under FERPA, most service providers of covered schools simply de-identified data to limit or mitigate liability arising out of their contractual obligations with schools.

Many states' new legislation and proposals are based on California's SOPIPA, which went into effect January 1, 2016. Under SOPIPA, service providers also can be directly liable for failing to meet their compliance obligations and are subject to direct enforcement from the state. SOPIPA also puts in place more explicit security controls. Notably, it is unclear whether de-identified information may be used for the purposes of targeted advertising.[19] SOPIPA specifies permissible uses of de-identified information, but it is vague on impermissible uses.

4. California

Continuing the trend as the model state for privacy legislation, California passed a number of additional privacy laws in

2015. Most notably:

- AB 32 increased the penalty for online harassment and "revenge porn," with a maximum penalty of $10,000 for each "digital image…distributed."[20]
- AB 856 expanded existing law on physical invasion of privacy to include invasion of airspace without permission in order to capture a visual image, sound recording, or other impression of someone engaging in private activities.[21]
- AB 1116 prohibits the operation of a voice recognition feature in a connected television without first prominently informing the user, and also prohibits the general use or sale for advertising purposes of recordings captured by a connected television.[22]
- SB 34 regulates the privacy and usage of data collected by an automated license plate recognition (ALPR) system.[23]
- SB 178 and 741 (the California Electronic Communications Privacy Act (CalECPA)) added procedures for law enforcement to access and obtain data on an electronic device or from an online service provider[24] and before intercepting cellular transmissions.[25] The new sections require that law enforcement obtain a warrant, wiretap order, order for electronic reader records or subpoena issued pursuant to existing state law before compelling or accessing electronic information, except in emergency situations. Although CalECPA requires that the government notify a person whose information is sought by warrant, a court may delay this notice up to 90 days where it finds that the notification may lead to an "adverse result," such as physical danger to an individual or the destruction of evidence.[26]

III. EVOLVING CASE LAW

A. Data Breach Litigation

Since 2006, the courts have been dealing with whether any "real world" injury or actual damages results from a data breach.[27] Up until the Supreme Court's decision in *Clapper v. Amnesty International*[28] in 2012, the Circuit Courts were beginning to provide some guidance as to when a plaintiff might have a cognizable claim. *Clapper* reignited the debate of whether a plaintiff could fabricate standing or pursue a claim over fear of future harm. Decisions in 2015 have brought forward this debate and addressed new theories of harm that were being advanced by plaintiffs. At present, success for plaintiffs on these issues often depends on not only which district court has the case, but also which judge presides over the case.

However, most other types of cases do not end simply because a plaintiff avoids a motion to dismiss. While we are still seeing a number of cases settle, some companies have begun to litigate whether their information security controls were reasonable, with remarkable success for the company. We expect to see more companies positioned to defend their information security practices and successfully defeat class certification.

1. Motions to Dismiss: Standing and Damages

In 2015, the Courts have continued to work through questions of the how the Supreme Court's decision in *Clapper* changed earlier rulings on whether the plaintiff alleged "certainly impending" damages. Most courts continue to hold that such damages are a constitutional requirement under Article III to demonstrate minimal standing to file suit.[29] Many courts continue to reject the position that a plaintiff has standing based on a fear of future identity theft and the purchase of services to mitigate that fear.

Similarly, even if plaintiffs could get past the standing requirement, data breach cases were previously dismissed for their inability to attribute damages to the loss of personally identifiable information (PII). Most courts still require at least a showing of "real and immediate" harm,[30] such as fraudulent charges against the plaintiffs' accounts. However, even where sufficient PII might have been disclosed, which might allow hackers to make fraudulent charges or open accounts, courts are generally requiring that claimants plead actual unauthorized charges to present an initial showing of damages. The passage of appreciable time since the incident strengthens the argument that plaintiff lacks standing due to an inability to plead damages in the form of actual loss. [31]

However, some courts have been receptive to new arguments presented by even if contrary to controlling authority. [32] For example, in the recent consolidated case relating to Anthem's data incident in 2014, the Northern District Court of California argued that under Second Circuit law, compromise of PII itself may be sufficient to confer standing due to "loss of [the] value of PII."[33] The court proceeded to cite to two Ninth Circuit decisions in "support," although one is cited for a proposition contrary to the actual language of the decision.[34] The broad view towards the potential compromise of PII stood in stark contrast to other contemporaneous Ninth Circuit decisions that still required some minimal allegation of fraudulent charges.[35]

Additionally, in at least one state court case, the court found that plaintiffs' general allegations of injury were sufficient to survive a motion to dismiss, despite the lack of any allegation of unauthorized persons having actually viewed, accessed, or misused consumer private information.[36] Courts are looking to the content of the breach notification letters in deciding whether to allow the plaintiff to engage in discovery to understand the facts behind the statements made in those letters.

Another novel theory of damages emerging is a form of "unfair business practices," which include allegations that defendants promised security and privacy and plaintiffs thereby lost out on the "benefits of the bargain." In both *Anthem* and *LinkedIn*, the court permitted the claims to survive under California's Unfair Competition Law (UCL).[37] UCL claims can now be found in almost every complaint arising from a data incident even though most consumers likely never read any terms of use, paid any additional amounts for information security, or made any purchasing decision on the basis of any such "promise." However, whether "benefits of the bargain" and UCL claims will survive class certification challenges remains to be seen, as plaintiffs have tended to rely on fraud-based allegations that are often replete with problems on class commonality and typicality.

2. New Trends & Arguments

With the filing of an increasing number of data breach cases, courts are confronting new issues and trends head on. We are observing three important trends: (1) defendants are more willing to take cases to trial, successfully defending cases on the standard of care; (2) derivative lawsuits based on privacy events are increasingly common; and (3) litigation between businesses resulting from privacy events continues to develop.

a. Defending On The Standard of Care

Defendants are increasingly willing to defend against allegations on the basis of the standard of care to which they contend that they had adhered. For example, the plaintiff in *Lozano v. Regents of the University of California* alleged that her medical records were improperly accessed by the current romantic partner of her ex-boyfriend, who allegedly used the identification and password of a doctor to access her personal health information (PHI).[38] Plaintiff alleged that her PHI was then texted to others, revealing that she had a sexually transmitted disease. She sought $1.25 million in damages, arguing that the UCLA health system failed to reasonably secure her PHI by not requiring a second form of security for access.

The UCLA health system disagreed, arguing that it used security protocols consistent with existing standards and that it should not be held responsible for "inside jobs." On Sept. 3, 2015, a jury found that UCLA was not legally liable for the breach. As one of the first data breach cases to be decided at trial, *Lozano* proved that an organization suffering a data incident does not necessarily breach a standard of care, although reasonable minds may differ on how to implement that standard.[39]

b. Derivative Liability

In 2014, plaintiffs filed derivative lawsuits against the executives of Wyndham Worldwide[40] and Target[41] for their highly publicized privacy incidents.[42] These derivative claims were among the first since the unsuccessful suit against Heartland Payment Systems' management in 2009. In 2015, other shareholders of retailers filed similar suits.[43]

As a result of such lawsuits, companies filing IPOs in 2015 have begun including disclosures of privacy-related incidents and cybersecurity efforts in their public filings. Among the first to so do was Fitbit.[44] Plaintiffs may also bring a derivative lawsuit where a company fails to properly disclose privacy-related incidents in their public filings.[45]

c. Business vs. Business Litigation

Businesses are increasingly filing suit against each other for data breach incidents. After the intrusions suffered by major retailers, organizations have tried to mitigate losses by proposing settlement offers with major card brands, due to potential payment card industry (PCI) liability implications.[46] The issuing banks of the cards objected to the settlement efforts, demanding that they be settled with directly.[47]

In Target's case, Target reached a $67 million agreement with Visa before the plaintiff banks were class-certified. The banks later defeated a proposed settlement of $19 million between Target and MasterCard, by convincing enough banks not to sign the proposed settlement. The opposition eventually led to an increased settlement of $39 million.[48]

Perhaps just as importantly, victims of breach events are now bringing suits against vendors that allegedly failed to properly assist them during privacy events. For example, in December 2015, a casino gaming company filed suit against Trustwave, alleging that while Trustwave was assisting it with one data incident, another incident occurred under Trustwave's care.[49] This case stands in contrast with a prior case, where the court found that the well-prepared vendor had adequate security controls in place and was not liable for the data incident suffered by its client.[50]

B. "Impermissible" Tracking Cases

Claimants have also continued to file privacy lawsuits against organizations for impermissible "tracking" practices. Alleged violations include the unauthorized use of persistent identifiers such as cookies and impermissible tracking across different applications and devices.

While organizations have tried to defend against claims of impermissible tracking by changing the terms and conditions users must agree to as a precondition to using their services, claimants continue to invent new and clever theories of civil liability, particularly by using non-users as putative class members. On the regulatory side, the FTC has been aggressively trying to regulate emerging data technologies with an expansive interpretation of its Article 5 powers under the FTC Act.

1. Expanding The Definition of "PII"

As new technologies reach consumers, claimants have continued to push to expand what may constitute "personally identifiable information." Although Illinois' Biometric Information Privacy Act (BIPA)[51] specifically exempts photographs as "bio-identifiers," claimants have argued that the use of geometrics extracted from photographs for the facial recognition technologies should be covered by BIPA. Cases have been filed against companies such as Shutterfly[52] and Facebook,[53] with much to be decided in 2016.

Notably, Texas also has laws governing biometrics,[54] and similar new laws may be in play for California.[55] The addition would not be surprising in California, as legislation in 2015 added usernames in combination with passwords, health

information, and "information captured by automatic license plate recognition systems" to the statutory definitions of PII.[56]

2. Persistent Identifiers, URL Tracking, And "Content Scanning"

The spotlight thus far has largely focused on data breach cases. Perhaps even more important for American commerce, however, is the development of "impermissible tracking" cases. Much of the U.S. dominance in technology of the last two decades has relied on the creativity of American software, which was supported by innovative data analytics. As the information available has increased however, renewable debates have emerged over privacy concerns as to the collection of that data and the benefits of data analytics.

After dismissing most of the causes of action against Google for its use of cookies pursuant to a motion to dismiss, the Third Circuit permitted plaintiffs' California invasion of privacy tort causes of action to survive.[57] The court contended that Google had promised its users that their privacy would be respected, that they can customize their preferences, and that users can "reset…[the] browser to refuse all cookies." Google disagreed with the Court's characterizations, because the users accepted terms and controlled their own preferences.

The court nonetheless contended that if the users used browsers and other tools which were set to "do-not-track" by default, Google should not track. The court argued that where Google knew that certain users were using 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. The surprising result created additional litigation in the Third Circuit for other ecommerce companies.

Like cookie-tracking, URLs have long been tracked by social media platforms, particularly for the purposes of reposting to or from another platform. In addition, e-commerce organizations have historically tracked incoming and outgoing traffic from other web pages to assess website performance. And in the case of email services, hosting systems often need to scan traffic to prevent incoming spam, malware, and other inappropriate materials.

Claims alleging impermissible URL tracking and email scanning have enjoyed some success against preliminary motions for dismissal, despite defendants' presentation of strong business justifications for their practices. For example, in the case of Yahoo, the email service provider claimed that its servers needed to scan incoming emails to prevent fraud and spam. Its motion to dismiss was denied, with Yahoo eventually agreeing to settle the case in January 2016.[58] In the case of the scanning of URL referer headers, courts have noted that such practices can be problematic when appropriate disclosures are not in place.[59]

Notably, courts reviewing impermissible tracking cases involving persistent identifiers (i.e., cookies) and packet scanning (i.e., URL referer headers) have begun following the reasoning of data breach cases, albeit with the same wide divergence of opinions. In one of the numerous "impermissible tracking" cases against Facebook, the plaintiffs alleged that Facebook was impermissibly tracking users' browsing history using persistent identifiers. The claims against Facebook were dismissed in October 2015 – albeit with leave to amend – due to the lack of "realistic harm or loss."[60]

Other courts, however, have allowed similar claims of impermissible sharing of PII to proceed past motions to dismiss.[61] Like in data breach cases, plaintiffs are enjoying some success in claiming that services that violate their own privacy terms are "unfair" under various unfair competition laws.[62]

At least one court has tried to distinguish impermissible tracking cases that should survive a motion to dismiss from those that should not by pointing out that those surviving cases involved claims of impermissible disclosure to third parties.[63] Since URL tracking is generally more likely to involve some tracking assistance through a third party, URL tracking may present different but significant risks when compared to the use of persistent identifiers.

3. Cross-Device Tracking

Tracking behavior *across devices* seems to have drawn a significant amount of scrutiny, particularly in California. With the burgeoning of the "internet of things" (IoT), businesses are increasing efforts to track consumer behavior across different "smart" devices. Thus, infamous companies such as SilverPush have attracted public outcry with their cross-device tracking using "inaudible signals" emitted by one device that could be recorded by another device.[64]

In January 2016, software maker Carrier IQ, along with Samsung, HTC America, and other mobile phone manufacturers, reported to a California federal judge that they had reached a $9 million deal with 79 million consumers over a lawsuit alleging that the software and cell phone manufacturers were illegally eavesdropping and keeping tabs on user conversations.[65] Similarly, in February 2016, software maker Superfish settled its part of a class action with Lenovo, wherein putative class members alleged that Lenovo laptops were sold with preloaded Superfish applications that served as spyware on the users.[66]

In addition, 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.[67] Notably, California recently passed legislation prohibiting manufacturers from unauthorized enablement of voice-recognition features on smart TV devices.[68]

4. The Video Privacy Protection Act (VPPA) And The Use of Pseudonyms

VPPA cases have been among some of the most interesting tracking cases, largely due to the use of pseudonyms as a hotly litigated issue. Although now under increased scrutiny, pseudonyms have long been viewed as a defense against impermissible tracking and as a way to avoid "damages" if the data were ever compromised or inadvertently disclosed.

VPPA cases typically involve putative class members alleging that they did not consent to having their PII and video preferences disclosed to third parties.[69] Most defendants have prevailed by arguing that the class members are either not a "subscriber,"[70] or are not individually identifiable due to the use of pseudonyms.[71] Only one court has denied a motion to dismiss, holding that PII may be implicated where pseudonyms could be used to identify an individual when combined with other data.[72] For now, VPPA litigation continues to be an example of why the use of pseudonyms may present a viable defense for organizations in privacy litigation.

5. Consumer Profiling

The debate over use of pseudonyms in VPPA cases also carries over to a growing interest in the appropriateness of using "big data analytics" to "profile" users and consumers. Technologists and marketers would argue that data analytics increase market efficiency by directing and targeting traffic to users and consumers in accordance with what they actually want. Privacy "advocates" argue that such practices inevitably lead to unwanted targeted marketing, which is impermissibly intrusive.

As of the date of this publication, proponents and opponents alike are impatiently waiting for the Supreme Court's decision in *Spokeo v. Robins*,[73] after oral argument was heard on Nov. 2, 2015. Spokeo is a data aggregator that advertises that it has collected data from a number of "untraditional" sources, such as social media.

Before filing the case, the FTC had filed a complaint against Spokeo, arguing that it was a "credit report agency" (CRA) issuing "consumer reports," as covered by the Fair Credit Reporting Act (FCRA). On June 12, 2012, the FTC reported that Spokeo had agreed to pay $800,000 to settle charges that it violated the FCRA, by failing to take the required steps to protect consumers on issues such as accuracy, by failing to ensure that credit reports would only be used for permissible purposes, and for deceptive advertising.[74] Many critics saw the FTC's move as a bold and expansive one, as data aggregators employing new data technologies like *Spokeo* were not previously dealt with as a CRA covered by the FCRA. The FTC's analysis was viewed by some as turning the FCRA's logic on its head, by finding that the profile information Spokeo sold was being used for a covered purpose such as employment, thereby creating a "consumer (credit) report" and making Spokeo a CRA.[75]

Although the Supreme Court is considering *Spokeo v. Robins* on a somewhat different issue, it is unlikely that the FTC inadvertently timed the release of its report entitled, "Big Data – a Tool For Inclusion or Exclusion (Jan. 2016)." With the legal community waiting on the Supreme Court's decision, the FTC proceeded to lay down its views on the use of data analytics.

The FTC reminds organizations that it has powers to regulate e-commerce pursuant to the FCRA, various equal opportunity laws, and the Federal Trade Commission Act (FTC Act). The FTC reiterated its position that aggregators and marketers compiling "non-traditional" information gathered from social media to profile users for the purposes of credit, employment, insurance, housing, or other similar decisions about the users' eligibility, may be deemed CRAs, and parties using such information may be deemed as using "consumer reports." Quietly recognizing the limitations of the FCRA, the FTC also reminded businesses of equal opportunity laws and its powers under Section 5 of the FTC Act.

Perhaps even more importantly, the FTC discussed how an organization using *anonymized* consumer data directly in combination with demographic data from an aggregator to make a covered decision regarding consumers (e.g., on creditworthiness) "likely" implicates the FCRA.[76] This was inconsistent with the FTC's own prior finding regarding data anonymization in its 2011 report, "40 Years of Experience with the Fair Credit Reporting Act (July 2011)," wherein it stated, "[i] nformation that does not identify a specific consumer does not constitute a consumer report even if the communication is used in part to determine eligibility." The FTC recognized its reversal of position and stated in a long footnote that its prior statements therein encouraging de-identification were "(not) accurate."[77]

Attempts to pigeonhole data aggregators as CRAs will be imperfect, especially since the data aggregation efforts of new technology will substantially differ from one another. For example, faced with allegations similar to those in *Spokeo*, LinkedIn successfully argued that the claims against it for FCRA violations should be dismissed because, unlike Spokeo, LinkedIn aggregates its data through its users, even if reports pulled from LinkedIn can be used for employment purposes.[78]

Regardless, one of the most interesting questions of 2016 remains how the FTC and civil claimants will deal with targeted advertising companies and ecommerce, as they are accused

of using "consumer reports" for certain purposes traditionally covered by the FCRA, such as for credit applications, and housing. Setting aside the FTC's intent to police technology profiling, data aggregators that have traditionally not been considered CRAs are already under fire. Following the spirit of *Spokeo*, plaintiffs have argued that even data aggregators that are more akin to search engines may be considered CRAs if the resulting information is provided to other organizations specifically for purposes such as determining employment eligibility.[79]

As will be further discussed below, the European Union enacted laws controlling consumer "profiling" as well, and it remains to be seen how the industries that have thus far powered the American technology industry for the past 20 years will fare under the new laws and policies, both internationally and domestically.

IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

Regulators have been no less active than legislators and the plaintiffs' bar. It is important to keep in mind that the number of active regulators in the privacy arena is increasing, across different agencies and in new industries.

A. The Federal Trade Commission

The FTC continues to pursue an aggressive agenda, proactively tackling new privacy issues with emerging technologies. Under Article 5 of the FTC Act, the FTC has power to prohibit "unfair and deceptive practices." As discussed below, although examples of deceptive practices are more readily available, what constitutes an "unfair" practice is less clear and the subject of much debate. It is therefore critical for organizations to track the enforcement efforts of the FTC, so that they can steer clear of unfair practices. In addition, some of the examples of what is prohibited will likely be surprising:

- *In re Sitesearch*: In late 2014, the FTC filed a complaint against Sitesearch Corp., dba LeapLab,[80] alleging that it sold the PII of hundreds of thousands of consumers to scammers who then had their financial accounts compromised. Among the scammers was the respondent in a prior FTC enforcement action, Ideal Financial Solutions. According to the FTC's complaint, the defendants had reason to believe these marketers had no legitimate need for the sensitive information they were selling. Sitesearch eventually defaulted, and in February 2016, the FTC secured nearly $10 million in partially suspended payments to resolve its claims with the group.[81] The FTC's enforcement action suggests that the agency would hold data brokers secondarily liable for the misuse of data by another.

- *In re Morgan Stanley*: The FTC announced in August 2015 that it would not take any enforcement action against Morgan Stanley for an insider cyber breach disclosed in January 2015. Morgan Stanley had improperly configured the access controls for one limited set of reports, but corrected the problem as soon as it became aware of the issue. Morgan Stanley apparently satisfied the FTC, which noted that: "it [Morgan Stanley] had a policy limiting employee access to sensitive customer data without a legitimate business need, it monitored the size and frequency of data transfers by employees, it prohibited employee use of flash drives or other devices to download data, and it blocked access to certain highrisk apps and sites." In its closing letter, the FTC implied that it might not pursue further action if an organization suffers a "human error," but had reasonably appropriate policies in place.[82] As with *Lozano v. Regents of the University of California*, discussed above, the Morgan Stanley case demonstrates that a data incident does not necessarily entail an organization's breach of its standard of care.

- *In re Safe Harbor Compliance*: In August 2015, the FTC charged 13 US companies with misrepresenting that they were compliant with the US-EU Safe Harbor framework, when their certifications had lapsed or when the organization had never applied for the program at all.[83] It is likely that under the US-EU Privacy Shield program, the FTC will continue to be the primary US agency enforcing the certifications.

- *In re Nomi Technologies*: In a controversial move, the FTC entered into a consent decree with Nomi Technologies in September 2015, a mobile device retail tracking technology company, regarding allegations that Nomi deceived consumers about their ability to opt-out of in-store tracking.[84] Nomi provided consumers with an opt-out mechanism on its website. But as Nomi was the service provider and not the retailer, consumers were typically unaware of the in-store tracking when they stepped into the retail store. Nonetheless, the FTC held Nomi liable for allegedly misleading consumer about the available choices for opt-out. *Nomi* demonstrates that organizations should be careful about their assurances to consumers about their privacy, and that even the best of intentions, when misapplied, could create regulatory liability.

- *In re LabMD Appeal*: In a surprising turn of events in November 2015, an FTC administrative law judge dismissed the FTC's enforcement proceeding against LabMD for allegedly failing to properly secure over 4,000 patient records with reasonable security protocols. Like many enforcement actions before *LabMD*, the FTC claimed that such failures were "unfair" under Section 5 of the FTC Act.[85] Assessing the FTC's proffer of evidence, the judge found proof wanting, and held that although the FTC may have "proven the 'possibility' of harm… [it] has not [proven] any 'probability' or likelihood of harm." Instead, "[f]undamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case."[86] Undoubtedly one of the most important privacy developments in 2015, *LabMD* curtailed FTC's authority in an unprecedented manner. The FTC has to now prove *actual* or *likely substantial consumer injury* when bringing enforcement actions against "unfair" practices.[87] Such a requirement is similar to what plaintiffs must plead for data breach litigation.

- *In re Lifelock*: In December 2015, Lifelock settled with the FTC for violating provisions of its prior settlement in 2010 with 35 state attorneys general.[88] The FTC alleged that Lifelock failed to secure PII as agreed, which made deceptive its advertisement of security of information. The settlement for $100 million supposedly goes towards consumer refunds. *Lifelock* is instructive in that FTC enforcements can result in large settlements, where a prior order was violated.

- *In re Oracle (Java SE)*: In December 2015, the FTC reached a settlement with Oracle over charges that it allegedly deceived customers regarding the security of the Java Platform, Standard Edition (Java SE) platform.[89] 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. In addition, Oracle knew that at least 44 types of malware had been developed against Java SE, including ones that exploited older versions. The action was notable as one of the first actions by the FTC against a software manufacturer for alleged failures to provide adequate security updates when promising "secure software."

- *In re Vulcan*: In February of 2016, the FTC settled its charges against Vulcan for unfair and deceptive practices, alleging that Vulcan replaced a popular web browser game with a program that installed applications on consumers' mobile devices without their permission.[90] The game, "Running Fred," ran on the Google Chrome browser as an extension, and Vulcan purchased it and then replaced it with its own extension. The FTC alleged that the Vulcan extension purported to offer users unbiased recommendations of popular Android applications, when in fact the extension would install applications directly, while bypassing the permissions process in the Android operating system. The consumers would thereafter be bombarded with advertisements, with the applications sometimes reinstalling themselves even after they are removed. *Vulcan* reminds us that organizations must adhere to their promises of user privacy.

- *In re ASUS (routers)*: In February of 2016, the FTC settled its claims alleging that ASUS misled consumers about the security of its routers and cloud services, which also constituted unfair business practices.[91] The FTC noted that it brought the action against ASUS because it was expecting wider adaptation of the internet of things, where home routers and cloud services would play critical roles. The FTC indicated that it believed that ASUS' routers were particularly vulnerable to hacking, that its cloud services did not use secure connections or encrypt traffic, and that ASUS' software update tool inaccurately promised the most current updates. *ASUS* demonstrates that the FTC plans to stay well ahead of the security issues that may arise from connected devices.

It is important to note that while the FTC continues to aggressively enforce its privacy policies, the FTC has yet to bring an enforcement practice solely based on "unfair" practices after its loss in *LabMD*. Although the FTC has appealed its loss, it is unclear whether it will ultimately be successful.

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)."[92]

As a result, the FCC is now involved in enforcement actions pursuant to the Telecommunications Act. The FCC settled with AT&T for $25 million in April 2015 for breaches involving customer PII and CPNI.[93] It then settled for $3.5 million in July 2015 with TerraCom, Inc. and YouTel America, Inc., for allegedly putting consumer information at risk.[94] On November 5, 2015, the FCC entered into a $595,000 settlement with Cox Communications to resolve an investigation into a data breach in 2014 involving approximately six million subscribers.[95]

Notably, the FCC issued a warning on February 5, 2016 to telecommunications providers that those who fail to file an annual report certifying compliance with the FCC's customer data privacy rules[96] will likely receive a substantial fine.[97]

C. HIPAA Enforcement

In 2015, there were large data incidents involving major health care industry players, including Premera Blue Cross (11 million individuals alleged), CareFirst BlueCross BlueShield (1.1 million individuals alleged), UCLA Health (4.5 million individuals alleged), Excellus (10 million individuals alleged), and Anthem. One common theme amongst these breaches, beyond their magnitude, is the difficulty in assessing and reporting the breach. For example, both UCLA and Excellus experienced substantial delays because of the analysis required following the breach, and noted that the attackers were "very sophisticated."[98]

There were also several noteworthy enforcement actions and settlements involving the Department of Justice (DOJ), the Department of Health and Human Services (HHS), and the Office of Civil Rights (OCR):

- In September 2015, radiation oncology Cancer Care Group agreed to pay $750,000 to settle potential Health Insurance Portability and Accountability Act (HIPAA) violations stemming from the theft of a laptop that contained unencrypted protected health information (PHI).[99] *Cancer Care Group* was notable for the high settlement figure despite the relatively small size of the medical practice.

- In November 2015, the DOJ announced a settlement of $125 million with drug company Warner Chilcott.[100] Although the case primarily involved health care fraud, part of the criminal and civil liability arose out of the company's alleged impermissible use and disclosure of PHI, by encouraging sales representatives to improperly access patient records and files to increase sales. *Warner Chilcott* demonstrates that as with the impermissible tracking cases, organizations can face regulatory liability for impermissible use of information in addition to data breaches.

- In November 2015, HHS announced a $3.5 million settlement with insurance company Triple-S Management Corporation.[101] The settlement was the culmination of multiple data incidents of varying types over many years involving Triple-S and its subsidiaries.

- In December 2015, HHS announced a $750,000 settlement with the University of Washington Medicine (UWM), for allegations that UWM failed to "implement policies and procedure to prevent, detect, contain, and correct security violations." Following a reported breach, HHS noted that although UWM's security policies indicated that it would have up-to-date and documented assessments and safeguards in compliance with HIPAA's Security Rule, UWM failed to so do. *UWM* demonstrates that after any data incident, regulators will continue to look at whether organizations are following their own written security procedures and must be proactive in meeting regulatory standards.[102]

In April 2015, the Office of the National Coordinator for Health Information Technology (ONC) published the second version of its "Guide to Privacy And Security of Electronic Health Information."[103] The guide purports to further clarify certain issues under HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), which amended and supplemented HIPAA, including:

- How to identify whether a contractor is a "business associate";

- When authorizations are required for disclosure;

- Questions to ask IT developers with regard to security; and

- How to better implement a security program process.

In October 2015, the OCR also launched a platform for mobile application developers to ask questions relating to HIPAA, further indicating its commitment to guide the development of new technologies in health care.[104]

We expect the OCR to be more aggressive in its enforcement efforts in 2016 due to certain criticisms publicly issued by the Office of Inspector General (OIG) in an executive summary in September 2015.[105] In the executive summary, the OIG was critical of whether the OCR was sufficiently overseeing covered entities' compliance with HIPAA's Privacy Rule. The OCR will likely respond accordingly.

D. State Attorneys General

There were a number of noteworthy enforcement actions by state attorneys general (AGs) in 2015 and early 2016. In January 2015, Zappos entered into a settlement with nine states over its 2012 data breach that compromised information concerning nearly 24 million of its customers.[106] Despite the breadth of the incident, Zappos argued that it had relatively tight security controls already in place. As to payment card information, only the last four digits were potentially compromised, and as a result, Zappos paid only a modest settlement to the states of approximately $100,000. The Zappos case demonstrates that security controls such as not storing full credit card numbers can mitigate imposition of significant penalties by regulatory authorities.

In February 2015, the New York AG entered into a settlement agreement with Santander, Capital One, and Citibank, to refrain them from using ChexSystems, which provided a database containing information about individuals with less than perfect banking records.[107] The New York AG alleged that the database was used as a blacklist, which prevented individuals from opening bank accounts even if they had immediately paid back money they owed or if they bounced a single check years before. This case demonstrates that although the use of data analytics is still hotly debated, AGs are increasingly scrutinizing such use by financial services.

As data regarding individuals has become more commoditized, AGs have begun venturing into areas more traditionally enforced by the FTC. The New York AG initiated an investigation against major credit reporting agencies after the FTC released a study alleging that 26 percent of consumers had errors in their credit reports.[108] Subsequently, 31 state AGs, led by the Ohio AG, entered into a separate agreement with the credit reporting agencies under similar terms.[109]

Due to the increase of data incidents, more states are willing to take into consideration the totality of circumstances when organizations experience delays in notifying authorities. Nonetheless, organizations should be aware that not all states are the same. For example, in May 2015, the Vermont AG entered into a settlement with Embassy Suites for failing to notify it about a key-logger incident until approximately six months later. The Vermont AG also entered into a settlement with Auburn University for failing to timely notify it about an incident until almost four months later.[110]

In September 2015, the California AG announced that Comcast agreed to a stipulated final judgment to resolve allegations that the company posted online the names, phone numbers and addresses of tens of thousands of customers who had paid for unlisted voice over internet protocol phone service.[111] Comcast must pay a whopping $25 million in penalties and investigative costs to the California Department of Justice and to the California Public Utilities Commission, and approximately $8 million in additional restitution to customers whose numbers were improperly disclosed.

In February 2016, the California AG released its publication, "California Data Breach Report: 2012-2015," that lists 20 "priority action security measures" that the AG states is "the starting point of a comprehensive program to provide reasonable security."[112] Appendices A and B compare the proposed controls to other established security standards and industry statutes to demonstrate uniformity in the suggested "standard of care." The California AG will undoubtedly apply the recommendations provided in her report as her "baseline" standard of care to data breach investigations, and to the use of new technologies, in the state renown for emerging technology companies.

Lastly, state AGs continue to try to influence use of data in emerging technology. The New York AG recently investigated Uber for its use of an internal location tracking system sometimes referenced as "God View," used to allegedly access the location of journalists.[113] The agreement required Uber to encrypt rider location data, adopt multi-factor authentication before employees can access sensitive rider information, and limit the access to location data.

E. Other Administrative Enforcement Efforts

Other than the FTC, the FCC, and various state AGs, a number of other regulators are increasing their efforts in the data privacy arena. The Security and Exchange Commission (SEC) may regulate cyber security by bringing enforcement actions against registered entities that have violated 17 CFR Section 248.30(a), sometimes known as the "safeguards rule." As with the FCC's power, the SEC's power remains relatively untested. The SEC only settled its first privacy based regulatory action in September 2015 against R.T. Jones Capital Equity Management, wherein the SEC alleged that R.T. Jones failed to adopt any written procedures and failed to protect the PII of its customers.[114] However, the SEC began 2016 by announcing that cybersecurity will be a "top SEC objective."[115]

The Consumer Financial Protection Bureau (CFPB) has sought to regulate privacy practices under Sections 1031 and 1036 of

the Dodd-Frank Wall Street Reform and Consumer Protection Act. In a public letter from the FTC to the CFPB dated February 8, 2016, the FTC reminded the public of the CFPB's powers, while sharing its sentiments on the use of "Big Data" in the financial industry and how it could implicate both the FTC and CFPB's efforts on Regulation B of the Equal Credit Opportunity Act (ECOA).[116] The FTC expressed its concerns about "the lead generation industry…how online lead generation works, why types of lead generation conduct may be unlawful…best practices for entities, and how consumers can avoid unlawful conduct." In addition, the FTC pointed out that "firms can and do sell information, they collect more information, deny more applicants, and mortgage denial rates increase." More aggressive efforts by the FTC, likely with assistance from the CFPB, should be expected with regard to how targeted marketing and data analytics are used.

Regulations and proposals have been more interesting in areas covered by emerging technologies, particularly for automated cars and medical devices. Although Nevada was the first state to pass legislation relating to autonomous vehicles, California continues to lead the way with some of the most comprehensive proposals. The current proposal as of February 2016 will impose requirements that autonomous vehicles must be equipped with self cyber-risk assessment capabilities, and that the vehicle company must issue tracking disclosures and obtain consent from consumers when PII is collected.

On January 22, 2016, the U.S. Food and Drug Administration (FDA) issued draft guidance clarifying its recommendations for addressing post-market cybersecurity vulnerabilities in medical devices.[117] By its terms, the Guidance applies to: "1) medical devices that contain software (including firmware) or programmable logic, and 2) software that is a medical device." The Guidance does not apply to experimental or investigational medical devices.[118]

While the guidance is a draft only and unenforceable, it does represent the FDA's current thinking regarding the medical devices community's responsibilities to monitor, identify, and address cybersecurity threats to medical devices, including for emerging connected medical devices. Three particularly notable facets to the issued guidance stand out:

- First, the FDA emphasizes the importance of information sharing in managing cybersecurity risk to medical devices. The FDA also emphasizes that benefits may accrue if the various parties implicated in the medical device lifecycle share information regarding vulnerabilities and threats. To incentivize such information sharing among entities in the medical device field, the FDA suggests that those entities join Information Sharing Analysis Organizations (ISAOs).[119] In an unprecedented move, the FDA suggested that manufacturers that voluntarily join an ISAO may be exempt from certain FDA reporting requirements. In essence, ISAO member manufacturers will be looked upon favorably in the event of a cyber breach.[120]

- Second, the guidance reinforces the FDA's advocacy of so-called "privacy-by-design" in the manufacture of medical devices for post-market application. As part of its premarket considerations, the FDA urges that manufacturers should "address cybersecurity during the design and development of the medical device."[121] It is evident, however, that preemptive design measures are meant to mitigate post-market developments. "Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound post-market evidence capture in the event of an attack."[122]

- Finally, the draft guidance acknowledges the dynamic nature of medical device cyber threats in the post-market environment, sets priorities for managing those threats, and in doing so may implicitly establish a manufacturer's standard of care. The draft guidance emphasizes prospective monitoring, and notes that "[b]ecause cybersecurity risks to medical devices are continually evolving, it is not possible to completely mitigate risks through premarket controls alone."[123] The FDA further urges manufacturers to characterize cybersecurity vulnerabilities as "acceptable or unacceptable" and "controlled or uncontrolled."[124] Those characterizations essentially acknowledge that post-market cyber threats are not predictable and not completely preventable. Additionally, the draft guidance provides clarity as to a device maker's prospective duties to report updates and patches made in response to a perceived vulnerability. For now, the only remedial actions that will require prompt reporting to the FDA by device makers are arguably those intended to correct vulnerabilities affecting the "essential clinical performance" of a device or that "present a reasonable probability of serious adverse health consequences or death."[125]

V. NOTABLE INTERNATIONAL DEVELOPMENTS

Although there was much development domestically, certain international developments will likely affect privacy law in the US as well. Although US-born multi-national corporations (MSCs) continue to dominate the international scene, MSCs must still adhere to the laws of each nation state within which they do business. As they adopt policies in accordance with local laws, there will be considerable pressure for MSCs to have some consistency in the privacy policies amongst their offices, even for those in the US.

This article will end therefore by assessing major developments in the regions of the U.S.' two largest trading partners: the European Union and the Asia-Pacific region.

A. The "Privacy Shield" For Transatlantic Data Protection Framework

In light of the Snowden revelations, an Austrian privacy activist named Max Schrems brought suit against Facebook for its alleged transfer of personal data to the United States' National Security Agency (NSA), as part of NSA's PRISM program. Schrems'"Europe v. Facebook"group filed suit against Facebook in Ireland with the Irish Data Protection Commissioner. On June 18, 2014, the suit before the Irish High Court was referred to the Court of Justice of the European Union (CJEU). The central question of the referral was the legitimacy of the European Union's granting of the "Safe Harbor" status to the United States when it came to the transfer of personal information.

On September 23, 2015, the CJEU found that with respect to the powers of national supervisory authorities, the European Commission may adopt a decision that a third country ensures an adequate level of protection that is binding on all member states and their organs, including national supervisory authorities.[126] However, a European Commission determination, such as the Commission Decision 5000/250 that first found the Safe Harbor "adequate," does not prevent a national supervisory authority from examining claims lodged by individuals concerning the processing of their PII. In fact, "[w]hile the Advocate General (of the CJEU) acknowledges that the national supervisory authorities are legally bound by the Commission decision (on the Safe Harbor)…such a binding effect cannot require complaints to be rejected summarily."[127] Thus, the CJEU found that the Safe Harbor program was inadequate in so far as it allowed for government interference with individual privacy rights, it failed to give individuals violated a means of redress, and it prevented national supervisory authorities from exercising their powers on behalf of their citizens.[128]

Although the European Union said it had reached an agreement in principal with the United States on a revised Safe Harbor program for trans-Atlantic data flow by the end of January 2016 – deemed the "Privacy Shield" program – debates on the details continue to the date of this publication. Organizations and scholars were quick to notice that *Schrems* also put into question mechanisms such as Binding Corporate Rules (BCRs) and standard contractual clauses (SCCs).[129] The national supervisory authorities know this as well. The national supervisor authority of France announced that Facebook would have only three months to fix their various data transfer issues,[130] while the authority in Hamburg Germany announced that it will soon be ready to hand down fines against three unnamed companies for relying on the Safe Harbor.[131]

The FTC, White House, and Congress are all apparently working hard to negotiate not only the Privacy Shield program details, but also other assurances that need to be in place. For example, on February 24, 2016, President Obama signed into law what was previously named the "Judicial Redress Act," in an effort to given EU citizens the right to sue the US government for alleged privacy violations.[132]

On February 29, the FTC announced more tentative details of the Privacy Shield program, subject to a determination of adequacy from the EU prior to implementation.[133] The documents provided concurrent with the announcement suggests that the Privacy Shield program will likely include the following requirements in its final form:[134]

- Obtain affirmations from organizations that they will follow rules on consent, relevance, proportionality, access, and correction[135];
- Make arbitration available for disputes;
- Additional information to be provided to data subjects, including a declaration of the organization's participation in the Privacy Shield program, a statement of right of access to PII by data subject, and the identification of the arbitration forum for disputes;
- Stronger controls on data transfers to third-party data controllers, including assurances that "the recipient will provide the same level of protection as the (EU) Principles";
- Stronger controls on data transfers to third-party data processors and "agents," including assurances that "the recipient will provide the same level of protection as the (EU) Principles";

- Obtain assurances from organizations that they will remain responsible for misuse, even if its responsibilities were delegated to other controllers, processors, or "agents";
- Commitments by organizations to "respond expeditiously" to EU member complaints "through the Department (FTC)";
- That the FTC "verify self-certification requirements" provided by organizations, including commitments by the organizations to "cooperate with the appropriate EU data protection authorities";
- More extensive verification of, and follow up on, expired certifications and organizations that have been removed; and
- Commitment by the FTC to work more closely with European data protection authorities.

In its release, the FTC repeatedly assures the EU that the FTC will vigorously enforce the requirements of the Privacy Shield program. Just as interestingly, there appears to be a "national security" exemption for U.S. intelligence that remains to be discussed.[136]

B. General Data Protection Regulation (GDPR)

In December 2015, the European Commission, European Parliament, and the European Council agreed to replace the 1995 Data Privacy Directive in its entirety with the General Data Protection Regulation (GDPR).[137] Set to take effect in 2018, the GDPR should further standardize data protection across all EU member states. The following should be noted about the GDPR.

1. Privacy-Friendly Design

- "Privacy by design" as default.[138]
- PII should only be collected for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[139]
- Generally, processing of data will only be allowed with explicit consent, to perform a contract or legal obligation, to protect the vital interests of the data subject, to perform a task in the public interest, or (in very limited circumstances) "for the purposes of legitimate interests pursued by the controller or by a third party."[140] Consent can be revoked at any time and cannot generally be presented as "take it or leave it."[141]

2. Accounts For Emerging Technologies

- Data subjects have the right to object to "automated profiling" that "produces legal effects concerning him or her."[14]Genetic and biometric data are "sensitive personal data," which are subject to stricter rules (i.e., a general prohibition with exceptions).[143]
- Encryption and anonymization are encouraged – as is the use of pseudonyms where possible – as part of good data security practice.[144]

3. Timely Accessibility, Portability, And Erasure

- Data subjects have very broad rights to access and control data collected regarding them from the controller, regardless of whether the data is collected by the controllers or from third parties.[145]
- Controllers have to provide any information they hold about a data subject free of charge within one month of the request.[146]
- Data subjects have the right to control their data through the "right of erasure" and "right of rectification."[147]

4. Tighter Controls On Controller-Processor Relationships

- Increased obligations on data controllers, including more detailed contractual vendor controls.[148]
- Vendors may not subcontract the service without the consent of the controller.[149]

5. New Internal Control Requirements

- Data Protection Officers (DPOs) are often mandated, and DPOs shall enjoy independence and not be terminated for exercising their duties.[150]
- Increased use of privacy impact assessments.[151]

6. More Forceful Breach Requirements And Enforcement

- Notification must be provided for any data breach that creates significant risk for the data subjects within 72 hours of discovery.[152]
- Data protection authorities (DPAs) would be empowered to fine organizations up to 4% of their annual revenue.[153]

As compliance is set to take place in 2018, MSCs would do well to reassess their products, technologies, and compliance for consistency with the GDPR. Compliance with the GDPR is no small undertaking. Insofar as an MSC intends to rely instead on the Privacy Shield program, the organization would do well to remember that it is likely there will be demands by the EU that the Privacy Shield provide for "adequate" protections when compared to the GDPR.

C. The Network Information Security (NIS) Directive

In December 2015, the various EU institutions reached an informal agreement on the general text and concept of the Network Information Security (NIS) Directive.[154] The NIS Directive will require operators of certain "critical infrastructure" sectors to meet certain minimum standards on data security. In addition, the NIS Directive provides specific details on how those operators will need to notify public authorities in the event of a cybersecurity breach.

Thus far, the "critical infrastructure" operators include those in energy, water, transport, health, and banking industries. In addition, certain digital service providers, including cloud services, ecommerce platforms, and search engines, will likely be covered. The current draft speaks of more restrictions on critical infrastructure.

Should the NIS Directive be adopted by the individual EU members, each member will have 21 months to adopt and implement the NIS Directive into law. Members will have an additional six months to apply the framework created in the NIS Directive to identify specific companies that may be covered.

D. The Trans-Pacific Partnership (TPP) Agreement

The Trans-Pacific Partnership (TPP) Agreement (Agreement), signed on February 4, 2016, is a free trade agreement that involves twelve countries: the United States, Japan, Malaysia, Vietnam, Singapore, Brunei, Australia, New Zealand, Canada, Mexico, Chile and Peru.[155] China is not part of the Agreement although it is a major player in the global economy.[156] The original Pacific 4 (P4) trade agreement began with a trade agreement involving just four countries – Brunei, Chile, New Zealand and Singapore – agreeing to cooperate on intellectual property and competition law policies.[157] The P4 expanded to the TPP after about seven years of negotiations and encompasses the original issues in addition to issues of customs, trade remedies, labor, e-commerce and environmental policies.[158]

The main goal of the Agreement is to govern global trade. The Agreement includes "rules that will help Made-in-America exports, grow the American economy, support well-paying American jobs and strengthen the American middle class."[159] The Agreement promises to achieve these goals by providing tax cuts to "Made-in-America" exports, providing strong worker protections, and "promot[ing] e-commerce, protect[ing] digital freedom, and preserv[ing] an open internet."[160] More specifically from a privacy and electronic commerce perspective, the Agreement allows cross-border data flows and prohibits requirements related to data localization.

1. Cross-Border Data Flows

Each TPP member country is required to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business."[161] Since "conduct of the business" is a broad term, the inference is that data flow for any commercial purpose would suffice, meaning that PII can freely flow between corporate entities of TPP members. Additionally, TPP members are encouraged to develop mechanisms that are compatible with other regimes to promote compatibility of legal approaches to protecting personal information.[162] The Agreement allows easier cross-border data flows for TPP member countries and facilitates a growing digital economy. In light of the tentative "Privacy Shield" safe harbor data transfer pact reached between the European Commission and the U.S. Department of Commerce,[163] U.S. companies may have to adopt different approaches in cross-border data flows between the U.S. and Europe, and between the U.S. and TPP member countries.

2. Data Localization No Longer Required

The most relevant portion of the Agreement as applied to cybersecurity and data privacy is the Electronic Commerce section in Chapter 14 of the Agreement. The biggest game changer is that data can now rest and be stored

in data centers located in a country outside of the place of business. Previously, some of the TPP member countries, such as Vietnam, had required companies that want to do business in Vietnam to maintain a copy of their data for inspection by local authorities.[164] The Agreement now prohibits TPP members from requiring companies located in a TPP country to build data centers in the market countries in which they serve.[165] With the requirement of data localization no longer applicable, companies can rely on building fewer data centers and potentially increase data security data at a lower cost. This change reduces administrative costs and facilitates global e-commerce. Under the Agreement, no TPP member country "shall require the transfer of, or access to, source code of software owned by a person or party of another TPP member country as a condition for the important, distribution, sale or use of such software, or of products containing such software, in its territory."[166] Since the Agreement now prohibits requirements that force businesses to disclose valuable intellectual property with foreign governments or potential competitors upon entering the TPP market, it can facilitate a more robust entrance of TPP member businesses into different parts of the world.

VI. CONCLUSION

Moving forward through 2016, emerging technologies are quickly becoming the focus of new legal issues, regulations, and case law. In all likelihood, the focus of developing privacy law will be shaped by the evolution of augmented reality, automated cars, and connected "things."

In addition, the Supreme Court's much anticipated decision in *Spokeo* will be a further indicator of where we are heading, judicially and otherwise. *Spokeo* is critical not only because of the issue of standing, but also because it marks a crossroad between older laws such as the FCRA and a much more connected world. Laws in the US and EU both point to greater control on profiling, but targeted data is a major impetus for the burgeoning of technology in the last two decades. In truth, data is the reason for American technological dominance. And companies will need to continue being vigilant on these emerging legal issues when making decisions relative to functionality, privacy, and information security.

ENDNOTES

1 Nothing in this academic publication should be relied on as legal advice, or construed as creating an attorney-client privilege.

2 Whitener, *State Student Privacy Laws: A Game-Changer For Service Providers* (IAPP Nov. 23, 2015).

3 *In the Matter of Protecting And Promoting the Open Internet,* Federal Trade Commission GN Docket No. 14-28.

4 See e.g., *Mollett v. Netflix, Inc.,* No. 12-17045, 795 F.3d 1062 (9th Cir. July 31, 2015).

5 See Smart Grid Act of 2015, S. 1232.

6 Bergal, *Nearly a Dozen States Working to Protect The Electric Grid* (Stateline, March 4, 2015).

7 See Abelson *et al.*, *Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data And Communications* (MIT Jul. 7, 2015), available at: https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

8 Senate Bill 177 (introduced Jan. 13, 2015).

9 PL 114-23 (June 2, 2015).

10 50 USC Section 1861 *et seq*.

11 2015 SB 754, Title I.

12 *Autonomous/Self-Driving Vehicles Legislation* (NCSL, Jan. 19, 2016).

13 Plungis, *Auto Industry, US Reach Agreement On Cybersecurity, Safety* (Bloomberg, Jan. 15, 2016).

14 Bergal, *Nearly a Dozen States Working to Protect the Electric Grid* (Stateline, Mar. 4, 2015)

15 S. 1232 (introduced May 6, 2015), Summary.

ENDNOTES *continued ...*

16 Whitener, *State Student Privacy Laws: A Game-Changer For Service Providers* (IAPP Nov. 23, 2015).

17 Cal. Bus. & Prof. Section 22584 *et seq.*

18 See 34 CFR 99.31(b).

19 *State Student Privacy Laws: A Game-Changer For Service Providers*, supra.

20 Cal. Pen. Section 502.

21 Cal. Civ. Section 1708.8.

22 Cal. Bus. & Prof. Section 22948.20-22948.25.

23 Cal. Civ. Section 1798.29, 2798.82, and 1798.90.5-1798.90.55.

24 Cal. Pen. 1546 *et seq.*

25 Cal. Gov. Section 53166.

26 Myers, *CalECPA: California's New Privacy Law* (IAPP Oct. 9, 2015).

27 See e.g., *Anderson v. Hannaford Brothers Co.*, 659 F. 3d 151 (1st Cir. 2011); see e.g., *Krottner v. Starbucks*, 628 F.3d 1139 (9th Cir. 2010)

28 133 S.Ct. 1138.

29 See *SuperValu Inc. v. Customer Data Security Breach Litigation*, 2016 U.S. Dist. LEXIS 2592 (D. Minn. Jan. 7, 2016) [no standing in case alleging compromised credit card and debit card information]; *Whalen v. Michael Stores Inc.*, 2015 U.S. Dist. LEXIS 172152 (E.D.N.Y. Dec. 28, 2015) [dismissing claims arising out of data breach for lack of damages arising from retail breach, and distinguishing *Remijas v. Neiman Marcus Group*, *infra*]; *Cahen v. Toyota Motor Co.*, 2015 U.S. Dist. LEXIS 159595 (N.D. Cal. Nov. 25, 2015) [dismissing claims for hacking vulnerabilities and impermissible tracking of drivers)]; *Antman v. Uber Tech.*, 2015 U.S. Dist. LEXIS 141945 (N.D. Cal. Oct. 19, 2015) [dismissing claims arising from hacker downloads of drivers' personal information]; *Fernandez v. Leidos, Inc.*, 2015 U.S. Dist. LEXIS 114858 (E.D. Cal, Aug. 28, 2015) [dismissing customer data breach claims arising from lost backup tapes in a personal vehicle containing personal information including health information]; *In re Zappos.com, Inc.*, 2015 U.S. Dist. LEXIS 71195 (D. Nev. Jun. 1, 2015) [dismissing customer data breach claims arising from hacking incident]; *Green v. eBay Inc.*, 2015 U.S. Dist. LEXIS 58047 (E.D. LA. May 4, 2015) [no standing in case involving cyber attack exposing user passwords, names, and other PII]; *In re Horizon Healthcare Services Inc. Data Breach Litigation*, 2015 U.S. Dist. LEXIS 41839 (D. N.J. Mar. 31, 2015) [dismissing generalized allegations of identity theft following the stealing of two employee laptops]; *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359 (M.D. Pa. 2015) [no standing in case involving hacking of national payroll firm]; *Peters v. St. Joseph Serv. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015) [no standing in case involving infiltration of network of health care provider storing personally identifiable health information]; *Lewert v. P.F. Chang's China Bistro*, 2014 U.S. Dist. LEXIS 171142 (N.D. Ill. Dec. 10, 2014) [no standing in case where plaintiffs claimed that restaurant chain failed to secure their credit card information]; *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279 (N.D. Ala. 2014) [finding no standing despite plaintiff's allegations of unauthorized charges on his debit card because plaintiff did not allege that he actually had to pay for the charges]; *U.S. Hotel & Resort Mgmt., Inc. v. Onity, Inc.*, 2014 U.S. Dist. LEXIS 103608 (D. Minn. Jul. 30, 2014) [recognizing that "[i]n the 'lost data' context . . . a majority of the courts . . . hold that plaintiffs whose confidential data has been exposed, or possibly exposed by theft or a breach of an inadequate computer security system, but who have not yet had their identity stolen or their data otherwise actually abused, lack standing to sue the party who failed to protect their data"]; *In re Science Applications International Corp. Backup Tape Data Theft Litig.* ("*SAIC*"), 45 F. Supp. 3d 14 (D.C. 2014) [no standing in case involving theft of data tapes with information concerning U.S. military and their families]; *Strautins v. Trustwave Holdings Inc.*, 27 F. Supp. 3d 871 (N.D. Ill. 2014) [no standing in case alleging data company's malfeasance led to breach of South Carolina's Department of Revenue]; *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014) [no standing

ENDNOTES *continued ...*

in case involving hacked access to plaintiffs' information provided to insurance company]; *Polanco v. Omnicell Inc.*, 988 F. Supp. 2d 451 (D. N.J. 2013) [no standing in case involving theft of an employee laptop containing unencrypted information]; *In re Barnes & Noble Pin Pad Litig.*, 2013 U.S. Dist. LEXIS 125730 (N.D. Ill. Sept. 3, 2013) [no standing in case involving tampering with personal identification number pads used to process payment information].

30 This test of "real and immediate" harm is generally a Ninth Circuit test, whereas most courts subscribe to the test of "certainly impending" harm laid down by the *Clapper* court.

31 See e.g., *Fernandez v. Leidos*, *supra* [order on Aug. 27, 2015, granting motion to dismiss despite allegations of extensive loss of personal health information, finding that at least four years have passed by]; see also *In re Zappos.com*, *supra* [order on Jun. 1, 2015, granting motion to dismiss, and finding that three and a half years have passed].

32 See *Remijas v. The Neiman Marcus Group*, LLC, 794 F.3d 688 (7th Cir. 2015) [reversing district court's decision in a case alleging compromised credit and debit card information]; see *In re Anthem Inc. Data Breach Litig.*, 2016 U.S. Dist. LEXIS 18135, Case No. 15-02617 (N.D. Cal. Feb. 14, 2016) [permitting various causes of action to survive]; see *Weinberg v. Advanced Data Processing, Inc. et al.*, 2015 U.S. Dist. LEXIS 165077 (S.D. Fl. Nov. 16, 2015) [case alleging failure to safeguard emergency medical service patients' protected health information]; see *Enslin v. Coca-Cola Co.*, 2015 U.S. Dist. LEXIS 133168 (E.D. Penn. Sept. 30, 2015) [finding plaintiff's claims arising from stolen laptops containing personal information sufficient to establish standing]; see *Corona v. Sony Pictures Entertainment Inc.*, 2015 U.S. Dist. LEXIS 85865 (C.D. Cal. Dec. 15, 2014) [case alleging theft of sensitive personally identifying information of former and current Sony employees]; see *In re Target Corp. Customer Security Breach Lit.*, 2015 U.S. Dist. LEXIS 123779 (D.Minn. Dec. 2, 2014) [case alleging loss of millions of credit card records due to malware installed at point of sale]; see *In re Adobe Systems Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) [case arising from a cyber attack that exposed customers' personal information]; see *In re Linkedin User Privacy Litig.*, 2014 U.S. Dist. LEXIS 42696 (N.D. Cal. Mar. 28, 2014) [case arising from hackers posting users' passwords on the internet, with motion to dismiss denied in part on theories of unjust enrichment]; see *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014) [case alleging failure to provide reasonable network security to safeguard plaintiffs' personal and financial information]; see also *Walker v. Boston Medical Center Corp*, 2015 Mass. Super. LEXIS 127 (Super. Ct. Mass. Nov. 19, 2015) [finding general allegation of injury regarding medical information data breach sufficient to overcome motion to dismiss prior to discovery].

33 *In re Anthem Inc. Data Breach Litig.* Order on Feb. 14, 2006 at p. 165-171.

34 In her opinion, Judge Lucy Koh stated that in *Corona,* Judge Gary Klausner held that "loss of value of PII" was sufficient to show cognizable damages. *Anthem* at p. 168 (citing to her own opinion in *Adobe*, and then *Corona*). The statement however, appears contrary to Judge Klausner's ruling, at page 8 of the *Corona* decision: "[t]o the extent Plaintiffs' alleged injury relies on a theory that their PII constitutes property, those allegations also fail, as Plaintiffs have not provided any authority that an individual's personal identifying information has any compensable value in the economy at large." (Citing to *In re Jetblue Airway Corp. Privacy Litig.*, 379 F.Supp.2d 299, 397 (2005).)

35 See e.g., *Antman v. Uber Tech.*, *supra*; *Fernandez v. Leidos, Inc.*, *supra*; *In re Zappos.com, Inc.*, *supra*.

36 See *Walker*, *supra*. The court issued an order on Nov. 19, 2015, finding that plaintiffs' general allegations of likely injury were sufficient to withstand a motion to dismiss. The court found support from its conclusion by drawing inferences from defendant's notice to plaintiffs of the data incident, which suggested that the letter suggested that plaintiffs' medical records were available to the public on the internet for some period of time and that there is a serious risk of disclosure.

37 See e.g., *In re Anthem Inc. Data Breach Litig.*, *supra*; see e.g., *In re Linkedin User Privacy Litigation*, *supra*; but see *Remija v. Neiman Marcus*, 794 F.3d at 694-695 (court skeptical of "overpayment" as damages); but see also *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (in case involving two stolen laptops, court denies "benefit of the bargain" of paid monthly premiums as damages).

38 Los Angeles Sup. Ct. Case No. BC55419

ENDNOTES *continued ...*

39 See also *Krystel v. Sears Holding Corp.*, Los Angeles Sup. Ct. Case No. BC486354 (peeping Tom case where, on Feb. 4, 2016, jury found Sears not liable for the intruder's viewing of over 1,000 women, including by using secret cameras).

40 See *Palkon v. Holmes*, Case No. 14-01234 (D. N.J.) (asserting claims for breach of fiduciary duty and waste of corporate assets against officers and directors of Wyndham Hotels based on three separate data breaches, but court dismissed the claims under the business judgment rule on Oct. 20, 2014).

41 See *In re Target Corporate Shareholder Derivative Litigation*, Case No. 14-00203 (D. Minn.) (currently still pending).

42 LaCroix, *Data Breach-Related Derivative Lawsuit Filed Against Home Depot Directors & Officers* (The D&O Diary, Sep. 9, 2015).

43 *Bennek v. Ackerman et al.*, Case No. 15-2999 (N.D. Ga.) [complaint filed Sep. 2, 2015].

44 Fitbit, Inc.'s Form S-1, filed with the SEC on May 7, 2015, at p. 96, available at: https://www.sec.gov/Archives/edgar/data/1447599/000119312515176980/d875679ds1.htm#rom875679_20.

45 *Schneider v. Mobileiron et al.*, 2015 Cal. Sup. LEXIS 303, Santa Clara Sup. Ct. Case No. 115CV284001 [complaint filed Aug. 5, 2015, alleging that IPO registration statement was "materially misleading" for failing to disclose breach event].

46 See *Lone Star National Bank v. Heartland Payment Systems*, 729 F.3d 421 (5th Cir. 2013) (permitting issuing banks to proceed as a class against Heartland); but see *Pennsylvania State Emps. Credit Union v. Fifth Third Bank,* 398 F.Supp.2d. 317 (M.D. Penn 2005) (reaching opposite result). Notably, some businesses have also tried to sue the card brands, such as in *Genesco v. Visa USA*, 2013 U.S. Dist. LEXIS 101503, Case No. 13-00202 (M.D. Tenn., Jul. 18, 2013) (Genesco suing Visa entities to recover $13.3 million withheld through issuing banks after a data breach that lasted between 2009 and 2010, although Genesco was PCI DSS-compliant).

47 Grande, *Banks Get Access to Outreach In Home Depot Breach Suit* (Law 360, Feb. 8, 2016).

48 Grande, *Target Pays $39M to Settle Card Issuers' Data Breach Claims* (Law 360, Dec. 2, 2015).

49 *Affinity Gaming v. Trustwave Holdings*, Case No. 15-2464 (D. Nev.) [complaint filed Dec. 24, 2015]. In the consumer to business context, third-party contractor Keypoint Government Solutions was also sued by the victims of the Office of Personnel Business Management data breach incident in 2014. See *American Fed. of Gov. Employees et al. v. U.S. Office of Personal Management et al.*, Case No. 15-1015 (D. D.C.).

50 See e.g., *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 613-614 (8th Cir. 2014) [finding bank's security protocols adequate, in a suit brought by escrow company for alleged account takeover].

51 740 ILCS 14/.

52 *Norberg v. Shutterfly, Inc.*, 2015 U.S. Dist. LEXIS 175433, Case No. 15 CV 5351 (N.D. Ill. Dec. 29, 2015)

53 *Gullen v. Facebook.com, Inc.*, 2016 U.S. Dist. LEXIS 6958, Case No. 15 C 7681 (N.D. Ill. Jan. 21, 2016) [dismissing for lack of personal jurisdiction on Jan. 21, 2016]; but see *Norberg*, *supra* n. 11 [refusing to dismiss for lack of personal jurisdiction on Dec. 29, 2015].

54 Tex Bus. & Comm. Section 503.001

55 2015 Cal. AB 83.

56 See 2015 Cal. AB 1541, and SB 34.

57 See *In re Google, Inc. Cookie In Placement Consumer Privacy Litigation*, 806 F.3d 125 (3rd Cir. Nov. 10, 2015) [request for rehearing

ENDNOTES *continued ...*

on motion to dismiss denied on December 11, 2015].

58 See *Holland v. Yahoo!, Inc.*, Case No. 13-4980, ECF No. 1 ¶ 21 (N.D. Cal. Oct. 25, 2013) (order on May 26, 2015) [allowing claims under the Cal. Invasion of Privacy Act and the Stored Comm. Act to survive against Yahoo for its scanning of incoming non-subscriber emails]. Yahoo agreed to settle the case on Jan. 8, 2016, including by changing how it scans emails to and from inboxes. See also *Perkins v. Linked*, Case No. 13-04303 (N.D. Cal.), where the parties announced in June 2015 a $13 million settlement on claims alleging that LinkedIn "hacked" into user accounts to harvest data, including contacts who then received invitations to join LinkedIn. Godoy, *LinkedIn Pays $13M to Settle Email Harvesting Class Action* (Law360, June 12, 2015).

59 See e.g., *In re Google*, 806 F.3d 138-139 [holding that scanning referrer URL headers can constitute scanning content in some cases]; see e.g., *Campbell et al. v. Facebook, Inc.*, 77 F.Supp.3d 836, Case No. 13-05996 (N.D. Cal. Dec. 23, 2014) [denying motion to dismiss claims for violations of the Wiretap Act and invasion of privacy, where claims accused Facebook of mining URLs and other information in user private messages]; and see e.g., *Facebook Privacy Litig. v. Facebook, Inc.*, 572 Fed.Appx. 494 (May 8, 2014).

60 *In re Facebook Internet Tracking Litigation*, 2015 U.S. Dist. LEXIS 145142, Case No. 12-02314, at p. 33-34 (N.D .Cal. Oct. 23, 2015) [dismissing without prejudice, claims against Facebook for its alleged use of cookies while logged in and logged out, due to lack of "realistic economic harm or loss"]; *Austin-Spearman v. AARP*, 2015 U.S. Dist. LEXIS 98069, Case No. 14-1288 (D. DC July 28, 2015); [finding no actual injury stemming from alleged privacy policy violation involving Facebook and Adobe's collection of PII from AARP members]; see also *Carlsen v. Gamestop, Inc.*, 112 F.Supp.3d 855 (D. Minn. 2015) [dismissing claims against Gamestop for allegedly using Facebook to share PII, finding no actual injury]. But see *Facebook Privacy Litig. v. Facebook, Inc.*, 572 Fed.Appx. 494, 496 (May 8, 2014) [reversing lower court dismissal and finding sufficient allegations "that they (appellants) were harmed both by the dissemination of their personal information (to third party advertisers) and by losing the sales value of that information"].

61 See e.g., *In re Facebook Privacy Litigation*, Case No. 10-02389, 2015 U.S. Dist. LEXIS 67937 (N.D. Cal. May 22, 2015) [where a motion for class certification is currently pending on contract and fraud claims, after having dismissed unfair competition law (UCL) claims for no loss of money or property]; see also *Facebook Privacy Litig. v. Facebook, Inc., supra.* But see *Campbell et al. v. Facebook, Inc.*, 77 F.Supp.3d at 846, Case No. 13-05996 (N.D. Cal. Dec. 23, 2014) [dismissing UCL claims due to plaintiffs' lack of "a property interest in their personal information"].

62 See e.g., *Svenson v. Google Inc.*, 2015 U.S. Dist. LEXIS 43902, Case No. 13-04080, (N.D. Cal. April 1, 2015) [denying motion to dismiss under California's UCL claims, under breach of contract theory and "unfair" business practices, because Google Wallet allegedly shared PII impermissibly].

63 See *In re Facebook Internet Tracking Litigation*, 2015 U.S. Dist. LEXIS 145142, Case No. 12-02314 (N.D. Cal. Oct. 23, 2015), at fn. 3, distinguishing its holding from *Facebook Privacy Litig. v. Facebook, Inc.*, 572 Fed.Appx. 494 (May 8, 2014), due to the latter being about Facebook's transmission of information to third party advertisers. But see *In re Anthem Inc. Data Breach Litig.*, *supra*, at p. 168-169, arguing that *Facebook Privacy Litig. v. Facebook, Inc.*, 572 Fed.Appx. 494 is "prevailing Ninth Circuit…precedent."

64 See Schiff, *As Smart TV Service Providers Feud In Court, The Privacy Issue Lurks In The Wings* (Ad Exchanger, Nov. 23, 2015) (discussing patent suits between smart TV targeting companies Free Stream Media and Samba TV).

65 Acker, *Carrier IQ, Samsung Ink $9M Deal to End Privacy Suit* (Law 360, Jan. 25, 2016) [reporting on N.D. Cal. Case No. 12-02330].

66 Acker, *Superfish Settles Spyware Claims For $1M in Lenovo MDL* (law 360, Feb. 12, 2016) (reporting on *Lenovo Adware Litigation*, Case No. 15-02624 (N.D. Cal.))

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

68 2015 CA AB 1116.

ENDNOTES *continued ...*

69 Plaintiffs have also unsuccessfully brought cases alleging intra-organizational sharing of PII covered by the VPPA (e.g., *Rodriguez v. Sony Computer Entertainment America LLC*, Case No. 12-17391 (9th Cir. Sept. 4, 2015)), sharing with vendors to fulfill the video service (e.g., *Sterk v. Redbox Automated Retail LLC*, 672 F.3d 535, 538-539 (7th Cir. 2012), and intra-household sharing of PII (e.g., *Mollett v. Netflix, Inc.*, Case No. 12-17045 (9th Cir. July 31, 2015)).

70 *Ellis v. Cartoon Network, Inc.*, 803 F.3d at 1255-58 (11th Cir. 2015); *Yershov v. Gannett Satellite Info. Network Inc.*, 104 F. Supp. 3d 135 (D. Mass. 2015) [plaintiff who downloaded free smartphone app was not a subscriber]; *Austin-Spearman v. AMC Network Entm't LLC*, 98 F. Supp. 3d 662 (S.D.N.Y. 2015) (watching free video on content provider's website did not establish subscriber relationship).

71 *Eichenberger v. ESPN Inc.*, No. 14-00463, 2015 U.S. Dist. LEXIS 157106 (W.D. Wash. May 5, 2015) ["[P]laintiff's contention that the definition of PII includes information which can be used to identify a person is inconsistent with the text and legislative history of the VPPA"]; *Robinson v. Disney Online*, No. 14-CV-4146 (RA), 2015 U.S. Dist. LEXIS 142486, at *1 (S.D.N.Y. Oct. 20, 2015) ("PII is information which itself identifies a particular person as having accessed specific video materials."); *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) ["[A] Roku serial number, without more, is not akin to identifying a particular person, and therefore, is not PII." (internal quotation marks omitted)]; *Ellis v. Cartoon Network. Inc.*, No. 1:14-CV-484-TWT, 2014 U.S. Dist. LEXIS 143078 (N.D. Ga. Oct. 8, 2014), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015) [Android device ID not PII because "[f]rom the information disclosed by the Defendant alone, Bango could not identify the Plaintiff or any other members of the putative class"]; *In re Nickelodeon Consumer Privacy Litig.,* MDL No. 2443 (SRC), 2014 U.S. Dist. LEXIS 91286, at *10 (D.N.J. July 2, 2014) ["[PII is] information which must, without more, itself link an actual person to actual video materials"]; *In re Hulu Privacy Litig.*, 2014 U.S. Dist. LEXIS 59479, *12 (N.D. Cal. Apr. 28, 2014) [disclosing Hulu user ID to analytics firm comScore is not disclosure of PII].

72 *Yershov v. Gannett Satellite Info. Network, Inc.,* 104 F. Supp. 3d 135 (D. Mass. May 15, 2015)

73 Supreme Court Docket No. 13-1339.

74 FTC online press release, June 12, 2012.

75 Ross et al., *Case Study: US v. Spokeo* (Law360 Jul. 11, 2012).

76 At p. 16-17.

77 *Id.* at Footnote 85.

78 *Sweet v. LinkedIn Corp.*, No. 14-04531, 2015 U.S. Dist. LEXIS 49767 (N.D. Cal. Apr. 14, 2015).

79 Acker, *Corelogic Can't Slip FCRA Claims In Background Check Suit* (Law360 Feb. 18, 2016) (reporting on order in *Henderson v. Corelogic Nat'l Background Data*, Case No. 12-00097 (E.D. Vir. Feb. 18, 2016); but see *Fiscella v. Intelius*, 2010 U.S. Dist. LEXIS 57918 (granting motion to dismiss against FCRA claims to Intelius, which enables online searches of public records).

80 *FTC v. Sitesearch Corp.*, Case No. 14-02750 (D. Ariz. 2014).

81 Grande, *Data Brokers Settle FTC Claims Over Data Sold to Scammers* (Law360, Feb. 18, 2016).

82 See Fair, *Letter to Morgan Stanley Offers Security Insights About Insiders* (FTC Aug. 10, 2015).

83 Press Release, *Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed to Comply With International Safe Harbor Framework* (FTC Aug. 17, 2015).

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

ENDNOTES *continued ...*

85 "Unfair" practices are those that: (1) cause or are likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves, and (3) not outweighed by countervailing benefits to consumers or competition.

86 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).

87 Unfortunately, Wyndham hotels would have benefitted from the *LabMD* decision as it was subject to the same type of FTC enforcement action for "unfair" privacy practices. But the defense for Wyndham had already signed the consent decree by the time the administrative law judge issued his decision in *LabMD*. See *FTC v. Wyndham Worldwide Corp.*, Case No. 13-01887 (D. N.J.) (see Stipulated Order For Injunction, filed on Dec. 9, 2015).

88 Fair, *FTC's $100 Million Settlement With Lifelock: May(en) Force Be With You* (FTC Dec. 17, 2015).

89 Press Release, *Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates* (FTC Dec. 21, 2015).

90 Press Release, *Tech Company Settles FTC Charges It Unfairly Installed Apps on Android Mobile Devices Without Users' Permission* (FTC Feb. 5, 2016).

91 Press Release, *ASUS Settles FTC Charges That Insecure Home Routers And "Cloud" Services Put Consumer Privacy At Risk* (FTC Feb. 23, 2016).

92 *In the Matter of Protecting And Promoting the Open Internet,* Federal Trade Commission GN Docket No. 14-28.

93 *In the Matter of AT&T Services, Inc.,* FCC Case No. 15-399 (FTC April 8, 2015).

94 *In the Matter of TerraCom, Inc. and YourTel America, Inc.*, FCC Case No. 14-173 (FTC Jul. 9, 2015).

95 *In the Matter of Cox Communications*, FCC Case No. DA 15-1241 (Nov. 5, 2015).

96 FCC Enforcement Advisory, *Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy*, Enforcement Advisory No. 2015-03 (FCC May 20, 2015).

97 Grande, *FCC Warns of Crackdown on Privacy Certification Failures* (FTC Feb. 5, 2016).

98 Bourque, *HIPAA And Health Care Data Privacy – 2015 In Review* (Mintz Levin Dec. 11, 2015), available at: https://www.healthlawpolicymatters.com/2015/12/11/hipaa-and-health-care-data-privacy-2015-year-in-review/

99 Press Release, *$750,000 HIPAA Settlement Emphasizes The Importance of Risk Analysis And Device And Media Control Policies* (Sept. 2, 2015).

100 Press Release, *Warner Chilcott Agrees to Plead Guilty to Felony Health Care Fraud Scheme And Pay $125 Million to Resolve Criminal Liability And False Claims Act Allegations* (DOJ Oct. 29, 2015).

101 Press Release, *Triple-S Management Corp. Settles HHS Charges By Agreeing to $3.5 Million HIPAA Settlement* (HHS Nov. 30, 2015).

102 Press Release, *$750,000 HIPAA Settlement Underscores The Need For Organization-Wide Risk Analysis* (HHS Dec. 14, 2015).

103 *Guide to Privacy And Security of Electronic Health Information* (ONC April 2015) available at https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

104 See http://hipaaqsportal.hhs.gov/.

ENDNOTES *continued ...*

105 OCR Should Strengthen Its Oversight of Covered Entities' Compliance With The HIPAA Privacy Standards (OIG September 2015).

106 Press Release, *AG Coakley Reaches Settlement With Zappos Over Data Breach* (Attorney Gen. of Mass., Jan. 7, 2015).

107 Press Release, *AG Schneiderman Announces Commitment By Citibank to Eliminate Barriers to Low-Income Americans to Obtain Checking And Savings Accounts* (NY Attorney Gen. Feb. 20, 2015).

108 Press Release, *N.Y. Office of the Attorney General, AG Schneiderman Announces Groundbreaking Consumer Protection Settlement with the Three National Credit Reporting Agencies* (NY Attorney Gen. Mar. 9, 2015).

109 Jim McCabe et al., *Déjà vu: State AG Consumer Reporting Settlement Follows Landmark New York Agreement*, Morrison Foerster Client Alert (May 26, 2015).

110 Press Release, *Attorney General Settles Security Breaches With Embassy Suites San Francisco Airport And Auburn University* (Va. Attorney Gen. May 21, 2015).

111 Press Release, *Attorney General Kamala D. Harris Reaches $33 Million Settlement With Comcast Over Privacy Violations* (Cal. Dept. of Justice, Sept. 17, 2015).

112 California Data Breach Report: 2012-2015 (Kamala D. Harris, AG Cal. Dept. of Justice Feb. 2016), p.31.

113 Press Release, *N.Y. State Office of the Attorney General, AG Schneiderman Announces Settlement with Uber to Enhance Rider Privacy* (NY Attorney Gen. Jan. 6, 2015).

114 SEC Press Release 2015-202.

115 Trader, *Cybersecurity Compliance a Top SEC Priority In 2016* (Law 360 Jan. 13, 2016).

116 FTC letter to Patrice Alexander Ficklin of the Consumer Financial Protection Bureau, dated Feb. 8, 2016, available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-enforcement-activities-under-equal-employment-opportunity-act-regulation-b/160210cfpb_ecoa_report.pdf.

117 Draft Guidance, *Postmarket Management of Cybersecurity in Medical Devices*, p. 4, January 22, 2016, U.S. Department of Health and Human Services, Food and Drug Administration, available at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022

118 Guidance, p. 7.

119 As the Draft Guidance explains, ISAOs are the product of "Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (EO13691), released on February 13, 2015."

120 *See* Draft Guidance at p. 20 ("If the company took this action to mitigate the risk within 30 days of learning of the vulnerability and is a participating member of an ISAO, FDA does not intend to enforce compliance with the reporting requirement under 21 CFR part 806.").

121 Draft Guidance at p. 11.

122 Draft Guidance at p. 24.

123 Draft Guidance at 11.

ENDNOTES *continued ...*

124 Draft Guidance at 13.

125 Overley, Jeff, "FDA Details Cybersecurity Steps for Approved Med. Devices" (Law360, Jan. 15, 2016)

126 Press Release No. 106.15, Advocate General's Opinion in Case No. C-362/14 (Court of Justice of the European Union Sept. 23, 2015), available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf.

127 *Id.* at p. 2; the Advocate General's opinion was adopted by the CJEU, see *Maximilian Schrems v. Data Prot. Comm'n*, 2015 E.C.R. I-1-35, CJEU Case No. C-362/14, available at: https://cdt.org/files/2015/10/schrems.pdf.

128 Press Release No. 106.15 at p. 2-3.

129 See e.g., Bracy, *EU DPAs Respond to Privacy Shield; BCRs Are a Go, for Now* (IAPP Feb. 3, 2016); but see Wugmeister, *Digital Privacy: Europeans Threaten to Halt Data to US* (Newsweek Feb. 2, 2016) (US-based law firms arguing that national supervisory authorities actually have more limited powers).

130 Grande, *Facebook Gets 3 Months to Fix France's Data Transfer Qualms* (Law360 Feb. 8, 2016).

131 Meyer, *Here Comes The Post-Safe Harbor EU Privacy Crackdown* (Fortune Feb. 25, 2016).

132 Freking, *Obama Signs Bill Extending Privacy Protections to Allies* (AP News Feb. 24, 2016); but see Bender, *The Judicial Redress Act: a Path to Nowhere* (IAPP Dec. 17, 2015) (criticizing the Judicial Redress Act for failing to provide any redress to the problems with US-government surveillance that was raised by *Schrems*).

133 Press Release, *Statement of FTC Chairwoman Edith Ramirez on EU-US Privacy Shield Framework* (FTC Feb. 29, 2016); see also Sayer, *Five Things You Need to Know About the EU-US Privacy Shield Agreement* (PC World Feb. 29, 2016) (stating draft program is still subject to approval).

134 Package to the European Commission, Commissioner of Justice, from the US Dept. of Commerce, dated Feb. 23, 2016, which includes a package with tentative details on the Privacy Shield program, subject to an adequacy decision, at p. 5-11, available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf?utm_source=govdelivery

135 Instead of "correction," the words used for the summary initial details are actually "recourse mechanisms." *Id.* at p. 5. It remains to be seen whether "recourse mechanisms" will be read to include the now infamous EU "right to be forgotten." But see *id.* at p. 34, Section 8(a)(i)(3) (on "hav[ing] the data corrected, amended, or deleted…" Because this publication is being released before any further clarification has been released, "correction" was selected as the best description of the new tentative requirement.

136 *Id.* at p. 10.

137 A copy of the December 15, 2015 draft is available at http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

138 *Id.* at Article 23.

139 *Id.* at Article 5(1)(b); Article 6; see also Article 14.

140 *Id.* at Article 6(1).

141 *Id.* at Article 7(1), (3)-(4).

142 *Id.* at Articles 19-20.

ENDNOTES *continued ...*

143 *Id.* at Article 9.

144 *Id*. at Article 30(1)(a).

145 *Id.* at Articles 14-15.

146 *Id.* at Article 12(1)-(4); see also Articles 14-15.

147 *Id.* at Article 14(1)-(3); Articles 16-17b.

148 *Id.* at Article 22; Article 26(1).

149 *Id.* at Article 26(1a)-(2a).

150 *Id.* at Articles 35 and 38(3).

151 *Id.* at Article 33.

152 *Id.* at Articles 31-32.

153 *Id.* at Article 79(3aa).

154 Press Release, *MEPs Close Deal With Council on First Ever EU Rules on Cybersecurity* (European Union Dec. 7, 2015), available at http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity.

155 BBC, *TPP: What is it and why does it matter?* available at: http://www.bbc.com/news/business-32498715.

156 China is in separate negotiations with the US, as both are involved with the U.S.-China Business Council (USBC) to complete a bilateral investment treaty. The USBC's Board of Directors issued top priorities for the two countries with a heavy focus on more collaboration on investment, cybersecurity, and intellectual property protection. Lawson, *Group Calls For US-China Work on IP, Cybersecurity in 2016* (Law360 Jan. 20, 2016).

157 *Id*.

158 Wikipedia, *Trans-Pacific Partnership*, available at: https://en.wikipedia.org/wiki/Trans-Pacific_Partnership.

159 Executive Office of the President, Office of the United States Trade Representative, *the Trans-Pacific Partnership*, available at: https://ustr.gov/tpp/#what-is-tpp.

160 *Id*.

161 The Trans Pacific Partnership, art. 14.8(5), Feb. 4, 2016.

162 *Id*.

163 Grande, *US, EU Agree To New Trans-Atlantic Data Transfer Rules* (Law360 Feb. 2, 2016). (Note that the actual details of this new Privacy Shield safe harbor program have yet to be announced.)

164 Brown, *Trans-Pacific Partnership Would Promote Cross-Border Data Transfers and Restrict Data Localization* (Data Privacy Monitor Nov. 10, 2015), available at: http://www.dataprivacymonitor.com/international-privacy-law/trans-pacific-partnership-would-promote-cross-border-data-transfers-and-restrict-data-localization/. Decree 72, or the "Management, Provision, Use of Internet Services and Information Content Online," was signed by Prime Minister Nguyen Tan Dung on July 15, 2013 prohibited

ENDNOTES *continued ...*

even basic flow of information such as sharing of news stories on various social networks. Therefore, the TPP Agreement is a game changer for countries with stringent internet law policies such as Vietnam.

165 The Trans Pacific Partnership, art. 10, Feb. 4, 2016.

166 The Trans Pacific Partnership, art. 14.17(1), Feb. 4, 2016.

CONTACTS

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

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

Ashley L. Taylor Jr.
Richmond / Washington, D.C.
804.697.1286; 202.274.2944
ashley.taylor@
troutmansanders.com