GIBSON DUNN

January 28, 2016

# CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW: 2016

To Our Clients and Friends:

We wish everyone an auspicious Data Privacy Day. Observed annually on January 28, Data Privacy Day constitutes an international effort to raise awareness and promote privacy and data protection best practices. Data Privacy Day commemorates the signing of Convention 108--the first legally binding international treaty dealing with privacy and data protection--on January 28, 1981. In January 2014, the United States Congress adopted S. Res. 337, a nonbinding resolution supporting the designation of January 28 as "National Data Privacy Day" in the United States. Currently, approximately 30 countries in North America and Europe "celebrate" Data Privacy Day.

An annual commemoration of the need to raise awareness about data privacy risks and best practices is fitting, as 2015 saw a number of developments in the cybersecurity and data privacy arena. Large-scale data breaches impacting millions of consumers continued to plague cyberspace. Increased pressure from consumer protection groups resulted in a number of new and proposed laws that will alter company data collection and sharing practices, and has also led the FTC and other U.S. regulators to step up their oversight and enforcement activities with respect to cybersecurity and data privacy practices. Last year also saw international regulators continue to take bold action on data privacy issues--most notably, the European Court of Justice invalidated the EU-U.S. Safe Harbor regime, leaving many U.S. companies scrambling to ensure that their transatlantic data flows can continue in the new year.

In this fourth edition of Gibson Dunn's Cybersecurity and Data Privacy Outlook and Review, the firm's Privacy, Cybersecurity and Consumer Protection group describes key data privacy and security events from 2015, as well as anticipated trends for the near future. The topics covered are: (i) civil litigation; (ii) U.S. government regulation of privacy and data security; (iii) legislative developments; (iv) international developments; and (v) U.S. government data collection.

---

**Table of Contents**

---

## I. Civil Litigation

### A. Standing in Data Breach Litigation

As the frequency and scope of data breaches continue to increase, companies handling consumer and employee data face an ever-increasing risk of litigation. While establishing Article III standing--particularly the element of injury-in-fact--is a substantial obstacle for data breach plaintiffs, the fact-specific nature of the inquiry continues to allow a handful of cases to survive a standing challenge (at least six such suits survived past the pleading stage in 2015). This year, key issues for standing continued to include whether the plaintiff alleged any actual instances of identity theft or fraud and whether personal information was specifically targeted by hackers.

The Supreme Court's 2013 decision in *Clapper* continued to provide the basic test for establishing the injury-in-fact element of Article III standing, namely that "threatened injury must be *certainly impending* to constitute injury in fact." *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (2013) (citing *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). Indeed, the majority of courts deciding data breach cases this year have held that absent allegations of actual identity theft or other fraud, increased risk of harm alone is insufficient to confer Article III standing. Recent cases continue this trend. *See, e.g.*, *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015) (finding no standing where plaintiffs did not allege that they actually suffered any form of identity theft as a result of the defendant's data breach); *In re Horizon Healthcare Services Inc. Data Breach Litigation*, No. 13-7418, 2015 WL 1472483 at *6 (D.N.J. Mar. 31, 2015), *appeal docketed*, No. 15-2309 (3d Cir. Jun. 1, 2015) (finding no standing where plaintiffs did not allege "*any* post-breach misuse of compromised data"); *Green v. eBay Inc.*, No. 14-1688, 2015 WL 2066531, *5 (E.D. La. May 4, 2015) (citing *Clapper* and finding threat of future harm stemming from disclosure of names, passwords, birthdates, e-mail and physical addresses "far too hypothetical or speculative"); *Peters v. St. Joseph Servs. Corp.*,

74 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (finding alleged future harm "speculative" where disclosed information included social security numbers, addresses, medical records and bank account information, and where illicit credit card purchase was declined); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958-59 (D. Nev. 2015) (distinguishing cases within the Ninth Circuit that conferred standing based on increased risk of harm alone, and holding that increased risk of future harm in this case was insufficient to confer standing given no evidence of personal data misuse in three year period).

However, following the outcome in *In re Target Corporation Customer Data Security Breach Litigation*,[1] where the court found a cognizable injury based on claims that Target's data breach had resulted in customers incurring unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees, plaintiffs have found some success in establishing standing where they similarly allege that exposure of their personal information has already resulted in tangible injury and the injury is traceable to the breach. In *Corona v. Sony Pictures Entertainment, Inc.*, for instance, the court held that allegations that plaintiffs' stolen information had been posted on file-sharing sites and used to send threatening e-mails to former Sony employees and their families were sufficient to confer standing. No. 14-CV-09600 RGK, 2015 WL 3916744, at *3 (C.D. Cal. June 15, 2015). On November 24, the court granted class certification for purposes of settlement and approved a settlement agreement of at least $2 million and up to $4.5 million. In *Enslin v. The Coca-Cola Company*, the court found standing sufficient to survive a motion to dismiss where the plaintiff had "already suffered palpable harm, including the alleged theft of funds from his bank accounts on two occasions, unauthorized use of four credit cards, and the unauthorized issuance of new credit cards in [his] name." No. 2:14-cv-06476, 2015 WL 5729241 at *6 (E.D. Pa. Sept. 30, 2015). "Although seven years passed between [the employee's] employment and the misuse of his information, the chain linking the loss of [his] SSN, credit cards, and banking information, and the subsequent identity attacks [he] suffered, [was] plausible," as his employer had direct control over the laptops containing his personal information and had contractually agreed to protect it. *Id.* at *8-9.[2]

The Seventh and Ninth Circuits, with few exceptions, have thus far been more inclined than others to hold that an increased risk of future harm alone is sufficient to establish injury in fact. This year, the Seventh Circuit reversed a lower court's dismissal for lack of standing where hackers stole 350,000 Neiman Marcus customers' credit card numbers. *Remijas v. Neiman Marcus Group, LLC*, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014), *reversed*, 794 F.3d 688 (7th Cir. 2015). The court distinguished *Clapper*, stating that plaintiffs had established an "objectively reasonable likelihood" of identity theft and credit card fraud, and that substantial risk of harm created Article III standing. *Id.* at 693. The court found that the risk that plaintiffs' personal data would be misused by hackers was "immediate and very real," reasoning: "Why else would hackers break into a store's database and steal consumers' private information?" *Id.* (internal quotations omitted). The court also held that plaintiffs' allegations of actual injury (illicit credit card charges and phone scams) after the breach and resulting purchase of credit monitoring and identity theft protection services qualified as concrete injuries. The sheer volume of the breach and resulting harm to consumers--some 350,000 cards had been compromised and 9200 customers had already incurred fraudulent charges-- likely played a non-trivial role in the court's finding of a cognizable injury. Somewhat surprisingly, however, the court also used Neiman Marcus's offer of free identity theft protection against the company as evidence of risk of

harm. *Id.* at 694.[3] Neiman Marcus sought *en banc* review, which was denied in mid-September. Now on remand, the lower court has ordered supplemental briefing on the motion to dismiss in light of the Seventh Circuit's decision.

The standard for establishing Article III standing is particularly critical in the context of federal and state statutes that create private rights of action. A number of courts have found that alleging the violation of a private right of action created by statute does not require separate proof of Article III injury in fact. This spring, the U.S. Supreme Court will decide *Spokeo, Inc. v. Robins*, which puts this standing question squarely at issue. Robins sued Spokeo, an information aggregator that gathers and sells reports of public data about individuals, for violations of the Fair Credit Reporting Act, alleging that he suffered prolonged unemployment because Spokeo presented false information about him. The Ninth Circuit reversed the district court's dismissal for lack of standing, concluding that Robins' alleged injury was indeed sufficient to confer standing. *Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014). In April 2015, the U.S. Supreme Court granted certiorari specifically on the issue of whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm by authorizing a private right of action based solely on the violation of a federal statute. *Spokeo, Inc. v. Robins*, 135 S. Ct. 1892 (2015). The Court held oral argument in November 2015. As many privacy-related statutes contain private rights of action for monetary penalties, the decision is likely to have significant consequences for privacy and data breach suits.

### B. E-mail Scanning

A number of key developments occurred in 2015 in ongoing class action lawsuits alleging that major Silicon Valley technology companies violated state and federal laws by scanning user e-mails and messages for targeting advertising and user-profiling purposes. Companies operating electronic communications services should continue to monitor these suits, as they allege privacy violations based on what many consider to be standard industry practices, analyze the disclosures that satisfy consent to information collection and use,[4] and are potentially massive in scope, with the proposed classes including all or many users of such services.

One such suit was filed against Yahoo! in late 2013, alleging that Yahoo! disclosed users' e-mails to third parties without consent. In 2014, Judge Lucy Koh allowed plaintiffs' claims under the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631, and Section 2702(a)(1) of the Stored Communications Act to survive a motion to dismiss. *In re Yahoo! Mail Litig.*, 7 F. Supp. 3d 1016, 1034, 1037 (N.D. Cal. 2014). Plaintiffs filed a motion for class certification in February 2015, seeking to certify a Rule 23(b)(2) "injunctive" class only--likely designed to avoid Judge Koh's holding in the substantially similar case of *In re Google Inc. Gmail Litigation*, No. 13-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)), wherein Judge Koh denied class certification because consent presented individual issues that would predominate over common issues. Unlike in *Gmail*, however, the proposed class in *Yahoo!* consisted of non-Yahoo! e-mail users who had sent e-mails to or received e-mails from Yahoo! e-mail users. In its opposition to class certification, Yahoo! argued that even if non-Yahoo! e-mail users did not read or agree to Yahoo!'s Terms of Service, individual inquiries would be required to determine whether users impliedly consented due to the extensive disclosures and press coverage that disclosed Yahoo's practices to the public. In certifying the class, Judge Koh

distinguished between Rule 23(b)(2) and 23(b)(3), holding that while some class members may have consented to Yahoo!'s conduct, that did not negate the proposed class's challenge to Yahoo!'s "uniform policy of intercepting, scanning and using contents of e-mails sent to and from Yahoo! Mail subscribers by non-Yahoo Mail subscribers." *In re Yahoo! Mail Litig.*, 308 F.R.D. 577, 598–601 (N.D. Cal. 2015). Yahoo! filed a petition for permission to appeal the class certification decision under Rule 23(f) in June, which was denied by the Ninth Circuit in August. *See In re Yahoo! Mail Litig.*, No.15-80101 (9th Cir.), ECF Nos. 1, 5.

Yahoo! filed a motion for summary judgment in September 2015, arguing, among other things, that the CIPA claims fail because Yahoo! only accesses e-mails through automated scanning on its own servers--*after* the e-mails reached the inboxes of the intended recipients--and accordingly does not "intercept" any communications while "in transit," as is required under CIPA. *See* Mot. at 20–24, *Holland et al v. Yahoo! Inc.*, No. 5:13-cv-04980-LHK (N.D. Cal), ECF No. 135. What it means to be "in transit" was addressed in another recent decision in the recently settled case of *In re Carrier IQ, Inc., Consumer Privacy Litigation*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015). In *In re Carrier IQ*, plaintiffs alleged that Carrier IQ developed, and various mobile phone manufacturers implemented, software that collected sensitive data from users' phones in violation of the Electronic Communications Privacy Act ("ECPA") and various state privacy statutes. Though Judge Edward M. Chen dismissed plaintiffs' primary ECPA claim, he found that the plaintiffs sufficiently alleged that Carrier IQ's software "intercepts" communications and concluded that communications could potentially be intercepted while in "transitory" electronic storage, a conclusion arguably contrary to that reached in other courts in the Ninth Circuit, which found that data cannot be "intercepted" while in electronic storage. *Compare id*. at 1076–82, *with Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878–79 & n.6 (9th Cir. 2002); *NovelPoster v. Javitch Canfield Grp.*, No. 13-cv-05186, 2014 WL 3845148, at *10–11 (N.D. Cal. Aug. 4, 2014); *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1152–53 (C.D. Cal. 2007).

The outcomes in *Yahoo!* and other cases on these issues would have affected another putative class action filed in September 2015 against Twitter, alleging that the company violates ECPA and CIPA by scanning users' private direct messages without consent and altering links in the messages to route traffic through Twitter's own server. *See* Complaint, *Raney v. Twitter, Inc.*, No. 3:15-CV-04191, (N.D. Cal. Sept. 14, 2015), ECF No. 1. Less than a month after filing suit, the plaintiffs filed a motion for class certification under both Rule 23(b)(2) and 23(b)(3), arguing that Twitter's liability turned on common questions about Twitter's privacy policies. Twitter filed a motion to dismiss plaintiffs' complaint on the grounds that processing communications on a service provider's servers is not an "interception" under ECPA, and that Twitter's practice falls under the "ordinary course of business" exception. *Id*. at ECF Nos. 29, 33. However, the plaintiff voluntarily dismissed the case on January 14, 2016, prior to either motion being heard or decided. *Id*. at ECF No. 51.

Another putative class action to watch--nearly identical to the Twitter lawsuit--was filed against Google in September 2015. *See* Complaint, *Matera v. Google, Inc.*, No. 5:15-cv-04062-LHK (N.D. Cal. Sept. 4, 2015), ECF No. 1. Plaintiff alleged that Google's purported practice of collecting information on non-users violates the California Invasion of Privacy Act and ECPA. Because those allegations are related to those in the previous *In re Google Inc. Gmail Litigation*, Judge Koh was

assigned the case. However, unlike in *In re Google Inc. Gmail Litigation*, in which users sought only damages, the named plaintiff in *Matera* seeks both damages and injunctive relief. Google moved to dismiss or stay the case in October 2015, arguing that its terms of service now explicitly require users to consent to its e-mail scanning practices and provide that such information can be used for marketing purposes. Google also asked Judge Koh to either revisit her previous ruling regarding whether Google's e-mail scanning practices fall within ECPA's "ordinary course of business" exception or certify the question for a mid-litigation appeal to the Ninth Circuit, and argued that the suit should be stayed until the Supreme Court rules on the *Spokeo* case discussed above (*see* "Standing in Data Breach Litigation" section). *Id*. at ECF Nos. 20, 21. In his opposition to the motion, the named plaintiff argued that Google's terms of service do not cover Google's conduct, and that even if users had consented to Google's conduct, he still has standing to seek injunctive relief because Google reserves the right to modify the terms at any time and previously concealed its practices. He also argued that Judge Koh need not revisit her previous ruling, and that the suit should not be stayed until *Spokeo* is decided. *Id*. at ECF Nos. 29, 30. The motion to dismiss is currently pending.

### C. Telephone Consumer Protection Act

In 2015, the number of lawsuits alleging violations of the Telephone Consumer Protection Act ("TCPA") (42 U.S.C. §§ 227 *et seq*.) continued to increase. The appeal to the plaintiffs' bar stems from the TCPA's authorization of $500 to $1,500 in statutory damages *per violation*, which can be aggregated for class claims. Several large settlements made headlines last year, including a settlement with HSBC for $40 million, the third largest TCPA settlement to date, as well as others in the $8-12 million range.[5] Given the risk of a huge payout, it is important for any business using telephone or text message communications to monitor the evolving interpretations of the TCPA in the courts and by the Federal Communications Commission ("FCC").

One of the more notable TCPA developments in 2015 was the FCC's omnibus order in July that resolved 21 submissions seeking clarification on the TCPA. Two out of five FCC commissioners dissented, and a number of entities cited the commissioners' dissents in immediate appeals of the order. The appeals, which were consolidated and are currently pending in the D.C. Circuit, directly challenge the FCC's authority and the legality of the order.

Petitioners challenged the order's expansion of the definition of an automatic telephone dialing system, or an "autodialer," to include its *potential* functionalities. Petitioners contend that, to be an autodialer, a device must have the *current* capacity to dial automatically, emphasizing that most courts that have recently grappled with the issue have agreed.[6] Petitioners also challenged the FCC's position that autodialers include *predictive* dialers, which could be modified to satisfy the "autodialer" definition. Petitioners claim instead that autodialers must be able to *automatically* generate and dial random or sequential numbers under the statute.[7] Petitioners also contested the order's finding that a "called party" under the TCPA refers only to the *current* subscriber or user of the dialed telephone number, not the call's intended recipient. Though the order grants businesses a single-call safe harbor for misdirected calls, thousands of telephone numbers are reassigned on a daily basis, and there is uncertainty about the continuing viability of the defense of a "good faith" belief that proper consent was obtained.[8]

Finally, petitioners challenged the order's interpretation of when and how called parties may revoke their "prior, express consent." Telemarketers have been required since October 2013 to obtain express written consent prior to placing artificial or prerecorded telemarketing calls to a residential phone line or wireless number, sending text messages, or calling a wireless number using an automatic telephone system. *See In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, FCC 12-21, ¶ 4 (February 15, 2012). The FCC's July order provides that a consumer may revoke such consent "at any time, through any reasonable means."[9] *Id.* ¶ 2. Petitioners, however, argue that the standard in the FCC's order is arbitrary and capricious and that the order improperly prevents callers and recipients from contractually agreeing to reasonable means of revoking consent.[10] Responsive briefing is due in early 2016, and the decision on appeal is very likely to clarify the enforceability of several key portions of the order, as well as the scope of the TCPA.

Additionally, in 2015 courts continued to analyze federal common law principles of agency in the context of TCPA suits, confirming that sellers using third-party telemarketers can be vicariously liable for a third party's violations of the TCPA in certain circumstances. *See, e.g.*, *Imhoff Inv., L.L.C. v. Alfoccino, Inc.*, 792 F.3d 627, 634-35 (6th Cir. 2015); *Palm Beach Golf Ctr.-Boca, Inc. v. John G. Sarris, D.D.S., P.A.*, 781 F.3d 1245, 1255 (11th Cir. 2015) (TCPA provides for direct liability for an entity on whose behalf goods or services were promoted by unsolicited fax advertisements even though the unsolicited fax was sent by a third party). However, one 2015 decision demonstrates a plaintiff's ability to recover under a theory of vicarious liability is not limitless. In May 2015, a California district court awarded summary judgment because the defendant had neither actual nor apparent authority over the marketing of its security equipment after it had been sold to distributors. *See Makaron v. GE Security Manufacturing Inc.*, No. CV-14-1274, 2015 WL 3526253, at *10 (C.D. Cal. May 18, 2015). The case confirms that businesses, especially those that operate through authorized dealer networks, may avoid TCPA liability by carefully controlling the manner in which they authorize resellers and licensees to use their products, including, at a minimum, requiring a written contract that requires a dealer to comply with applicable laws and regulations.

Additionally, the long-awaited Supreme Court decision in *Campbell-Ewald Co. v. Gomez* came in January 2016, with the Court resolving a deep Circuit split by holding that companies cannot cut off class action claims by merely making an offer of full relief to individual plaintiffs--a practice common in TCPA litigation, as statutory damages can be easily calculated. But the decision expressly left for another day the question of what happens when a defendant not merely makes an offer, but also deposits the amount of the settlement offer with the Court to pay the plaintiff. The decision thus may well leave defendants with an effective option to moot class claims by making--and paying--a settlement offer that provides complete relief, and we anticipate this issue will work its way through the courts in 2016. Companies should also closely monitor an upcoming Supreme Court decision related to the TCPA. The Court's decision in the *Spokeo* case discussed above (*see* "Standing in Data Breach Litigation" section) may also affect the volume and outcomes of TCPA suits, as many TCPA plaintiffs may not be able to articulate actual injury from receiving an unwanted call, given the proliferation of unlimited text and calling plans.

### D. Video Privacy Protection Act

In 2015, the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, continued to play an important role in the data privacy litigation space. The VPPA provides a minimum $2,500 per-person in statutory damages (as well as attorneys' fees) when "video tape service providers" "knowingly" disclose "personally identifiable information concerning any consumer" to third parties, with certain limited exceptions. *Id.*

The VPPA defines a "video tape service provider," in part, as any person "engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." *Id.* Under the statute, a "consumer" can be "any renter, purchaser or subscriber of goods or services from a video tape service provider," while PII includes "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." *Id.*

The law--including its rather hefty per-violation damages provision--was passed in 1988 in response to a local DC newspaper's attempt to embarrass Judge Robert Bork during his Supreme Court nomination hearings by publishing his video store rental records; this did not particularly embarrass Judge Bork, but scared Congress enough to draft and pass the VPPA.[11]

Increased volume of VPPA claims this year resulted in substantial additional analysis of the Act in federal courts across the country. The arguably seminal VPPA case, *In re Hulu Privacy Litigation*, finally drew to a close this year. In March, Hulu obtained summary judgment in the ongoing class action for its alleged VPPA violations on the basis that plaintiffs failed to show that Hulu had knowledge that a social network allegedly would link identification information with video content information. 86 F. Supp. 3d 1090 (N.D. Cal. Mar. 31, 2015). The Court asserted that a violation would require disclosure of (1) the identity of the individual; (2) the identity of the video material; and (3) a connection between the individual and the video material. *Id.* at 1097. Because the individual identifier (the user's social network ID) and the video material identifier (the referral URL from the Hulu video page) were allegedly sent from Hulu to the social network in separate data streams, the Court held that the plaintiffs could not show that Hulu knew that the social network connected the two data elements, and thus could not state an actionable VPPA claim. *Id.*

In the wake of *Hulu*'s resolution, however, other courts continue to grapple with the various arguments raised during the *Hulu* litigation. For instance, a few recent decisions have continued a pattern of narrowing the definition of "personally identifiable information" under the VPPA. In *In re Nickelodeon*, the court dismissed the case, concluding that, because there was no concrete evidence that Google could (or had tried to) use the information Viacom sent it to ascertain personal identities, plaintiffs could not maintain their VPPA claim. MDL No. 2443, 2015 WL148334, at *3-4 (D.N.J. Jan. 20, 2015). In *Eichenberger v. ESPN*, the district court dismissed plaintiff's second amended complaint with prejudice, holding that plaintiff's renewed claim that ESPN disclosed data to Adobe Analytics, which may have taken steps to discover his identity using information gathered from other sources, was insufficient to state a claim under the VPPA. No. 2:14-cv-00463, 2015 WL 7252985, at *6 (W.D. Wash. May 7, 2015). Likewise, more recently, a court dismissed a VPPA class action alleging that

Disney unlawfully disclosed users' personally identifiable information--namely, serial numbers of the Roku devices used to access Disney video content as well as the users' viewing history--to a third-party analytics company. *Robinson v. Disney*, No. 1:14-cv-04146, 2015 WL 6161284, at *7 (S.D.N.Y. Oct. 20, 2015). Both courts concluded that the disclosed "personally identifiable information" must consist of non-anonymous information that specifically identifies an individual and his or her viewing history. Both also determined that a third-party analytics company's ability to identify the consumer by linking the anonymous information to other information independently obtained was not sufficient to hold the video provider liable under the VPPA.

In another case involving a matter of first impression in the Ninth Circuit, plaintiffs alleged that Netflix violated the VPPA by allowing a subscriber's friends to view that subscriber's personally identifiable information after the subscriber accessed her Netflix account on her own television through her password-protected account. *Mollett v. Netflix*, 795 F.3d 1062, 1063-64 (9th Cir. 2015). The Ninth Circuit held that the disclosure of the PII is only "to the consumer," and is therefore outside the purview of the VPPA. *Id.* at *1066. The court held that it is the consumer's choice to disclose the information on his or her television, noting "[t]he lawfulness of th[e] disclosure cannot depend on circumstances outside of Netflix's control." *Id.*

The Eleventh Circuit recently honed in on the definition of "subscriber," as the term is used in the VPPA: "consumer means any renter, purchaser, or *subscriber* of goods or services from a video tape service provider." *Ellis v. Cartoon Network*, 803 F.3d 1251, 1253 (11th Cir. 2015) (emphasis added). While ultimately affirming the dismissal of claims against Cartoon Network, the appeals court rejected the district court's finding that the plaintiff qualified as a subscriber, holding instead that "downloading an app for free and using it to view content at no cost is not enough to make a user of the app a 'subscriber' under the VPPA." *Id.* at *1257. It noted that there was no "ongoing commitment or relationship between the user and the entity," because the plaintiff had not established a Cartoon Network account or profile, provided any personal information to Cartoon Network, paid for the app or signed up for any periodic "services or transmissions" or access to exclusive content.[12] *Id.* Another unpublished decision earlier in the year similarly concluded that a plaintiff's relationship with AMC failed to rise to the level of a "subscriber" based on the common understanding of the word "subscription," which requires an exchange of "money and/or personal information in order to receive a future and recurrent benefit." *Austin-Spearman v. AMC Network Ent., LLC*, 98 F. Supp. 3d 662, 669 (S.D.N.Y. Apr. 7, 2015).[13]

Another circuit court decision this year evaluated the scope of the VPPA's "ordinary course of business" exemption. In *Rodriguez v. Sony Computer Ent. Am., LLC*, the plaintiff alleged that two Sony entities violated the Act by retaining his personally identifiable information and disclosing his personal information from one entity to the other. 801 F.3d 1045, 1048 (9th Cir. 2015). The court held that the alleged disclosures between the Sony entities were exempt under the "ordinary course of business" exemption. *Id.* at 1054. The court further held that the VPPA does not provide a private right of action to enforce its information retention requirements on video service providers. *Id.* at 1053.

Finally, putative class action plaintiffs also recently filed a VPPA claim against a smart television maker for allegedly installing tracking devices in its TVs to collect information about what people watch and relay that information to advertisers and other firms. *See Reed v. Cognitive Media Networks Inc. et al.*, No. 3:15-cv-05217 (N.D. Cal. Nov. 13, 2015). As of this writing, there have been no substantive orders in the case.

### E. California's Song-Beverly Credit Card Act and Point-of-Service Data Collection

In 2015, courts continued to weigh in on the scope of California's Song-Beverly Credit Card Act of 1971 ("Song-Beverly"), Cal. Civ. Code §§ 1747 *et seq.*, which prohibits merchants from requesting or requiring a customer's personal identification information as a condition of accepting a credit card payment. Since the California Supreme Court's landmark 2013 decision in the *Krescent* case, 56 Cal. 4th 128, 133 (2013), which held that Song-Beverly "does not apply to online purchases in which the product is downloaded electronically," courts have continued to place online fraud prevention practices beyond Song-Beverly's reach. For example, citing *Krescent*, in *Ambers v. Beverages & More, Inc.*, 236 Cal. App. 4th 508 (2015), the court declined to extend Song-Beverly's restrictions to online purchases of alcohol that would later be picked up by the customer at a retail store, thereby allowing retailers to demand the photo identification and credit card at the time of pick-up. *Id.* at 516. These cases represent significant wins for online retailers because, limited statutory exceptions notwithstanding, the prohibitory language of Song-Beverly sweeps broadly, and those found in violation face civil penalties of up to $250 for the first violation and up to $1,000 for subsequent violations. Cal. Civ. Code § 1747.08(e).

Courts recently have given clear guidance to brick-and-mortar retailers that have tested the limits of Song-Beverly, allowing such retailers to request personal information from customers so long as doing so is not an express or implied condition of the transaction.[14] Most significantly, in *Harrold v. Levi Strauss & Co.*, 236 Cal. App. 4th 1259 (2015), a California appellate court established a long-awaited bright-line test in affirming the lower court's denial of class certification: a retailer does not violate Song-Beverly by requesting e-mail addresses after credit card transactions are concluded because customers cannot reasonably believe that providing such information is a "condition of acceptance of the credit card." *Id.* at 1265. This decision came two weeks after the Ninth Circuit's decision in *Davis v. Devanlay Retail Grp., Inc.*, 785 F.3d 359, 365–66 (9th Cir. 2015), in which the court certified to the California Supreme Court the very question addressed in *Harrold*. The California Supreme Court ultimately declined to respond to the certified question, pointing to *Harrold*, and situating it as controlling precedent. *Davis v. Devanlay Retail Grp.*, No. 13-15063 (9th Cir.), ECF No. 41.

In 2015, courts also continued to find "special purpose" exceptions to Song-Beverly where the risk of fraud or other policy priorities outweigh the privacy intrusion to customers. Cases like *Lewis v. Safeway, Inc.*, 235 Cal. App. 4th 385 (2015), continue to apply the most common exception where a retailer is obligated by other statutes to confirm and/or record customers' personal information and where it would be absurd to expect the Song-Beverly privacy protections to apply in full force. *Id.* at 395 (dismissing a case against liquor purveyors whose obligations under the Alcoholic Beverage Control Act brought clerk's conduct within exceptions to Song-Beverly); *see also Lewis v. Jinon Corp.*,

232 Cal. App. 4th 1369, 1377 (2015) (requesting a consumer's birthday in connection with a purchase of alcohol fell within "special purpose" exception to Song-Beverly).

### F. Shareholder Derivative Suits Involving Data Breaches

The last few years have seen a significant increase in the number of consumer class actions stemming from data breach and security incidents,[15] and various state and federal regulatory agencies have also turned their attention to cybersecurity issues.[16] Some, though not many, of these corporate data breaches have also resulted in the initiation of shareholder derivative litigation. Nevertheless, a recent string of sizeable settlements of shareholder derivative litigation[17] and ever-expanding media coverage of high-profile data security incidents[18] may well spark renewed interest in shareholder derivative litigation where breaches result in adverse market responses. Three notable shareholder derivative suits this year provide companies with insight into what a modern cybersecurity shareholder derivative suit may look like--and these suits are critical case studies, as many companies have not yet focused their boards on cybersecurity issues. Indeed, while corporations are increasingly choosing to maintain their most valuable assets (trade secrets, confidential customer information, proprietary intellectual property, etc.) in digital formats on Internet-connected networks, a recent survey of more than 1,000 information technology leaders suggested that only 22% had briefed their board of directors on cybersecurity issues within the last 12 months.[19]

In *Palkon v. Holmes*, one of the only cases to have addressed the standard for board responsibility in the context of data breach, the court adopted the strict test articulated in the landmark decision *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).[20] Board members and officers owe various state law fiduciary duties to their corporate entity, and in *Caremark*, the Delaware Chancery Court held that directors may face personal liability in a shareholder derivative context when they violate those duties by failing to "appropriately monitor and supervise" corporate activities.[21] Emphasizing that a company's board of directors should be expected to appropriately implement and adequately maintain information and reporting systems, the *Caremark* Court held that a clear failure to discharge that duty--such as by ignoring obvious red flags, or by evincing a conscious disregard for governance responsibilities--constitutes an actionable failure "to act in circumstances in which due attention [might] have prevented [some] loss."[22] Later decisions have clarified that *Caremark* also applies to corporate officers, and over the last two decades the *Caremark* analysis has become the touchstone for evaluating director and officer conduct in shareholder derivative litigation. Subsequent decisions have also clarified that companies *may not* indemnify directors or officers for liability stemming from *Caremark* violations.[23]

*Palkon v. Holmes* began in February 2014 when plaintiffs filed derivative shareholder suits in the District of New Jersey against ten directors and officers of Wyndham Hotels, asserting claims for breach of fiduciary duty, waste of corporate assets, and unjust enrichment, predicated on three separate data breaches that took place between April 2008 and January 2010 and impacted more than 600,000 customers.[24] They alleged that the directors failed to prevent and to properly disclose, investigate, and remediate the breaches in question. However, the case was quickly dismissed. In October 2014, the district court found that the board's unanimous refusal to pursue the derivative suit constituted a legitimate exercise of the business judgment rule. The court based this finding on a number of

considerations, including the fact that the board received quarterly updates about data security, met to discuss the data breaches and the company's data security policies on numerous occasions, considered security enhancements to prevent future attacks, and appointed an independent audit committee to thoroughly investigate the breaches in response to the initial shareholder demand.[25] In addition, the court noted that the company had actually installed cybersecurity measures before the first data breach transpired.[26]

More recently, in September 2015, a plaintiff filed a derivative shareholder suit, *Bennek v. Ackerman*, against twelve Home Depot directors and officers in the Northern District of Georgia, asserting claims for breach of fiduciary duty and waste of corporate assets predicated on a September 2014 data breach that impacted more than 56 million customers. The complaint alleges that the defendants knew the company's systems were "desperately out of date," were "complacent" about known "vulnerabilities," failed to put into place cybersecurity protective measures "required" by the credit card industry, and failed to ensure that the company effectively monitored the systems that it did have in place to detect and prevent unauthorized access to customer data.[27] Interestingly, the plaintiff has alleged that the defendants were reasonably put on notice of the risks of a data breach by high-profile incidents against *other* companies, including the 2013 Target data breach.[28] In October 2015, Home Depot filed a motion to dismiss, citing *Caremark* as the proper standard for assessing the adequacy of plaintiff's allegations that Home Depot's directors and officers had breached their fiduciary duties by failing to exercise adequate oversight.[29] Noting that claims for breach of duty predicated on a failure of oversight theory are "the most difficult [claims in] corporate law upon which a plaintiff might hope to win a judgment" (quoting and citing *Caremark* for that proposition), Home Depot argued that plaintiff had failed to satisfy both the first prong of a *Caremark* claim (sufficiently pleading a "failure to implement any reporting systems or controls") and the second prong (pleading specific facts sufficient to establish "that the individual defendants had acted in bad faith by consciously failing to monitor or oversee" existing systems or controls).[30] The motion is presently pending.

Although the derivative litigation against Target was filed in 2014, before both *Palkon* and *Bennek*, it has seen the least progress in the courts. Plaintiffs filed four separate shareholder derivative lawsuits against thirteen Target directors and officers, alleging they had ignored their cybersecurity risk management responsibilities.[31] The claims included breach of fiduciary duty, waste of corporate assets, gross mismanagement, and abuse of control predicated on defendants' pre- and post-breach conduct, including alleged failures to take appropriate steps to prevent, investigate, disclose, and ultimately remediate the breach. These suits forced Target to convene a special independent litigation committee to conduct an extensive, multi-year investigation into whether it is in the corporation's best interest to pursue the litigation--an investigation which has included 68 interviews, over 48,000 documents, and over 90 meetings. The consolidated cases are currently pending in the U.S. District Court of Minnesota, which stayed the proceedings until February 2016 to allow for this investigation.

### G. Cybersecurity Insurance Coverage

As more high-profile cybersecurity breaches have occurred, businesses have continued to look for ways to not only improve infrastructure, response plans, and litigation strategy, but also to protect themselves against the cost of cyber events. No sector is immune, and it is estimated that over the next

two years, the probability that an organization will experience a breach involving at least 10,000 records is nearly one in four.[32] In the face of the growing costs and likelihood of cyber events, businesses are turning to insurance providers for protection.

While most generally available commercial policies do not cover many cyber risks,[33] many carriers have more recently started providing standalone offerings to businesses to help cover the costs of cyber events. However, the cyber insurance market is still nascent. The lack of actuarial data regarding cyber breaches makes for significant variations in premiums. And the growing costs and increased probability of cyber events that drive businesses to seek additional insurance may in fact render cyber insurance cost-prohibitive for some companies.

In this nascent market, litigation over the scope of cyber insurance coverage continues. For example, following a data breach, Cottage Health System was sued under California's Confidentiality of Medical Information Act for allegedly failing to properly encrypt medical records.[34] Cottage settled the case for $4.1 million and Columbia Casualty Company, its insurance carrier, agreed to fund the settlement, subject to a reservation of rights under the insurance agreement. However, the cyber insurance policy had required Cottage to "continuously implement the procedures and risk controls identified in [Cottage's] application" for the policy, and had required a "Risk Control Self-Assessment" of Cottage's cyber security. Columbia ultimately sued Cottage in the Central District of California in May 2015, seeking declaratory relief and reimbursement of defense and settlement payments.[35] Columbia alleged that Cottage's Self-Assessment contained false representations, and that Cottage had not followed the "Minimum Required Practices" outlined in the insurance policy.[36] The court ultimately dismissed the action, finding that the parties had not utilized the policy's required alternative dispute resolution process before resorting to litigation.[37] However, this case nevertheless demonstrates the approach some carriers will take in investigating when a business seeks to collect on a cyber insurance policy and the importance of meeting the requirements of the policy to ensure coverage.

The consistent stream of new entrants in the cyber insurance market means that there is little standardization in policy offerings, so businesses must work with carriers to draft policies that best suit their needs. However, even once a company acquires a policy, it must continue to evaluate data privacy and security risks and to assess coverage for such risks. Particular attention should be paid to what is excluded from coverage, such as acts of terrorism (especially with state-sponsored hacking on the rise) and exclusions based on location of data storage and type of data.

Though precisely tailoring a cyber insurance policy to meet business needs can be difficult, industry analysts and government agencies alike agree that cyber insurance is a useful tool for businesses to consider. In September 2015, Deputy Treasury Secretary Sarah Raskin called for greater involvement of the insurance industry in helping protect against cyber threats.[38] And regulators are increasingly adding cyber insurance as a key factor in evaluating a company's cyber preparedness. For example, the New York Department of Financial Services instituted a new Cyber Security Examination Process in 2015 that includes an insurance component when "expand[ing] its information technology . . . examination procedures to focus more attention on cyber security" when evaluating financial institutions.[39] The Securities and Exchange Commission (SEC) has also started to focus on cyber security in its examination procedures.[40] Examiners are now charged with "gather[ing] information

on cybersecurity-related controls," including information related to cyber insurance. This includes whether the firm had cybersecurity insurance coverage, the types of incidents the insurance covered, whether any insurance claims related to cyber events were filed, and the amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage.[41]

## II. U.S. Government Regulation of Privacy and Data Security

### A. Cybersecurity Guidance

In 2015, the Federal Trade Commission (the "FTC") flexed its muscles with several notable enforcement actions, and its authority as the primary regulator over the cybersecurity space was affirmed by the Third Circuit. The cybersecurity guidance landscape also continues to grow and expand, as several other regulatory bodies, including the SEC, issued cybersecurity guidance, creating some concern about the interplay of divergent guidance, but also reinforcing the extent to which cybersecurity issues are posing risks and potentially creating new responsibilities across industries.

#### 1. Challenges to the FTC's Authority

In an FTC action against Wyndham Worldwide Corporation leading to a challenge of the FTC's authority, the Third Circuit clarified and reinforced the FTC's authority to regulate corporate data privacy and security practices under Section 5 of the FTC Act, which prohibits "unfair" and "deceptive" business practices.[42] The lawsuit was the result of three hacks into Wyndham Worldwide's computer system (occurring between 2008 and 2010), causing its customers to face more than $10.6 million in fraudulent payment card charges.[43] The FTC claimed that Wyndham violated the unfairness prong of Section 5 by "fail[ing] to employ reasonable and appropriate measures to protect personal information against unauthorized access."[44] Wyndham challenged the FTC's authority to bring a cybersecurity enforcement action under Section 5 of the FTC Act. Among other arguments, Wyndham claimed that Congress's enactment of various laws that touch on the FTC's role in regulating cybersecurity--including a recent amendment to the Fair Credit Reporting Act (directing the FTC and other agencies to develop regulations for the proper disposal of consumer data), the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act--shows that Congress did not intend the FTC to have broad regulatory authority over corporate cybersecurity practices under the FTC Act.[45] The Third Circuit Court disagreed and suggested that the recent laws were meant to work in concert with the FTC Act to govern cybersecurity practices.[46]

Following affirmance of the FTC's authority, Wyndham and the FTC reached a settlement in December 2015. Under the terms of the settlement agreement, Wyndham must establish a comprehensive information security program designed to protect cardholder data, which will include establishing barriers like firewalls between Wyndham servers and servers belonging to its franchisees.[47] Wyndham must also conduct annual information security audits and undertake other efforts designed to safeguard consumers' information.[48] The benchmark for Wyndham's audits will be the Payment Card Industry Data Security Standard ("PCI DSS"), which applies to entities involved in the payment processing industry.[49] In the event of another data breach that affects more than 10,000 credit or debit card numbers, Wyndham will be required to obtain a written assessment of the

breach and provide it to the FTC within ten (10) days.[50] The company's obligations under the agreement will last 20 years.[51] The Wyndham settlement is particularly noteworthy in the cybersecurity field because its requirements are more specific than prior consent decrees.[52]

Like Wyndham, LabMD also challenged the FTC's authority to regulate cybersecurity practices, both in an administrative action before the FTC and in federal court. However, in 2015, the Eleventh Circuit held that LabMD could not challenge the FTC proceeding in federal court until its administrative remedies have been exhausted.[53] The proceedings are the result of a 2013 enforcement action brought against the now-defunct cancer-screening laboratory, which suffered two data breaches, in 2008 and 2012.[54] In November 2015, an administrative law judge dismissed the FTC's enforcement action.[55] If it stands, the decision would significantly raise the bar for FTC cybersecurity enforcement actions because, under the terms of the order, the FTC must demonstrate that there is more than a mere "possibility" that consumers will be harmed by company practices; it must show that there is a "probability" or likelihood of harm.[56] The ALJ determined that the FTC did not meet the burden of demonstrating more than a "possibility" that LabMD's consumers' sensitive information was ever accessed by anyone.[57] The FTC appealed the ALJ's decision to the full Commission, and the appeal is still pending.[58] Some commentators believe that the appeal will be successful due to what former FTC Commissioner Joshua Wright calls "an unhealthy and biased institutional process" of judicial review: "[I]n 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the administrative law judge ruled found no liability, the Commission reversed."[59]

### 2. FTC Enforcement and Guidance

The FTC continued its efforts to safeguard the privacy and security of consumer data in a number of notable enforcement actions this year. Like Congress and several states, the FTC took action in the realm of children's Internet privacy. In November 2015, the FTC added a new "selfie" method for companies covered by COPPA to obtain parental consent to a company's practice of collecting children's personal information.[60] This method allows a parent to provide consent to the collection of his or her children's data by providing a copy of a government-issued ID that a trained operator can check against a database.[61] Since the "selfie" method requires companies to hire or outsource all of the photos it receives to agents trained to verify whether the photo on a parent's identification card matches the photo submitted by the parent, this new method of obtaining consent could prove costly.

One of the largest consent decrees this year was the $100 million consent decree entered into between the FTC and LifeLock on December 17, 2015.[62] The FTC brought action against LifeLock for allegedly failing to abide by the terms of a 2010 settlement agreement whereby LifeLock was barred from misrepresenting the effectiveness or scope of its identity theft prevention services and obligated LifeLock to adopt certain data security practices.[63]

In addition to the Wyndham and LifeLock consent decrees, the FTC entered into a number of other noteworthy consent decrees in 2015. In March, it finalized a settlement with TRUSTe, a seller of data privacy services, for allegedly misleading consumers by stating that it annually recertifies companies displaying its "privacy seal."[64] Under the order, TRUSTe must pay $200,000 and must not

misrepresent its certification process.[65] Also this year, Internet tracking company Nomi entered into a consent decree with the FTC due to its alleged failure to adequately disclose tracking opt-out mechanisms.[66] Under the terms of the consent agreement, "Nomi will be prohibited from misrepresenting consumers' options for controlling whether information is collected, used, disclosed or shared about them or their computers or other devices, as well as the extent to which consumers will be notified about [the company's] information practices."[67] The Third Circuit's holding in *Wyndham* makes knowledge of the content of these consent decrees important in and of itself. In *Wyndham*, earlier consent decrees were held to be sufficient to place a company "on notice" of practices that the FTC considers unfair and deceptive.[68] This is especially important given that the vast majority of FTC enforcement actions are resolved through consent decrees.[69]

In June, the FTC launched the "Start with Security" business education initiative. The initiative includes guidance for businesses drawing on lessons learned from the over 50 data security cases previously brought by the FTC.[70] The guidance outlines ten steps to implement in order to achieve effective data security. The steps are high-level, consisting of general advice such as "control access to data sensibly"; "require secure passwords and authentication"; "secure remote access to your network"; and "make sure your service providers implement reasonable security measures."[71]

### 3. Other Regulator's Enforcement and Guidance

The SEC launched high-profile investigations this year, demonstrating that the FTC is not the only agency aggressively pursuing a cybersecurity agenda. Indeed, in fall 2015, SEC Commissioner Kara Stein told the *Financial Times* that the agency should "play a much more active role in trying to help companies better protect themselves against an increasing number of cyber security issues in a world in which we are all increasingly connected."[72]

In February, the SEC's Office of Compliance Inspections and Examinations ("OCIE") published a summary of the results of its examination of the cybersecurity preparedness of more than 50 registered broker-dealers and investment advisers.[73] The results showed that over 80% of investment advisers had adopted written cybersecurity policies and roughly the same proportion had conducted periodic firm-wide risk assessments.[74] However, less than 25% incorporated cybersecurity requirements into third-party contracts, and less than 15% maintained policies and procedures about information security training for third-party entities authorized to access their networks.[75] In September, the SEC issued a risk alert to provide additional information on the areas of focus for the OCIE's next round of cybersecurity exams.[76] The next round of examinations will focus on governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response planning.[77]

Also in 2015, the SEC required investment adviser R.T. Jones Capital Equities Management to pay a $75,000 penalty as a settlement for the firm's failure to establish cybersecurity policies and practices.[78] In June 2013, R.T. Jones discovered that a breach of its server exposed the personal information of 100,000 customers. The SEC investigated the breach and concluded that R.T. Jones stored sensitive customer information on a third-party server and did not "conduct regular risk assessments, implement a firewall, adopt encryption or even create a plan to respond to cybersecurity

incidents."[79] According to the SEC, such lax cybersecurity practices violated the Securities Act of 1933, which prohibits the "failure to adopt written policies and procedures reasonably designed to protect customer records and information."[80] Notably, R.T. Jones was found in violation of the 1933 Act, even though there was no evidence that its customers were financially harmed by the data breach.[81] In its decision, the SEC emphasized the importance of enforcing these rules, even in cases where there is no apparent financial harm to clients.[82]

Other federal agencies, including the Financial Industry Regulatory Authority, the Department of Justice, the Federal Communications Commission, and the Office of Management and Budget also issued industry cybersecurity guidance in 2015.[83] Generally, this guidance suggests that companies should implement cybersecurity best practices, including developing an incident response plan, exercising due diligence with third-party vendors, and training employees to understand and manage cyber risks.

State Attorneys General also continued to take an active role in the cybersecurity arena. Days after Lenovo announced that preloaded software on computers it sold allegedly allowed hackers to steal users' personal information, the Connecticut Attorney General announced that he was launching an investigation into the practice.[84] Also, following California's lead, several states have produced cybersecurity guidance for companies doing business in their states.[85]

### B. Legislative Developments

#### 1. Federal

Last year, Congress considered a number of cybersecurity and privacy bills concentrated on three main themes: information sharing, consumer protection, and government access to personal information. Although Congress is likely to pass, and the President to sign, a cybersecurity information sharing law in the near future, there has been less progress (despite considerable discussion) toward passing a national data breach notification law. However, several of the National Security Agency programs exposed by Edward Snowden were scaled back by the passage of the USA FREEDOM Act, which replaced the USA PATRIOT Act.

##### *a) Cybersecurity Information Sharing*

In June, the government unveiled that Chinese hackers had stolen highly sensitive data from 20 million government employees housed in the computer systems for the Office of Personnel Management.[86] In response to this attack and other cyber incidents, Congress developed several laws aimed at providing an incentive for cyberattack information-sharing between the private and public sector. The Senate passed the Cybersecurity Information Sharing Act ("CISA") in September. CISA attempts to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats" between private companies and the government.[87] CISA would create a portal administered by the Department of Homeland Security where companies and the government could alert one another to dangerous hacking activity as attacks happen. To accomplish this goal, CISA encourages cooperation by providing participating companies immunity from suit for

monitoring and sharing relevant information (with exceptions for willful misconduct or gross negligence).[88]

Despite broad government support, privacy advocates and many companies oppose the bill. Critics, including tech leaders,[89] voiced concern that the bill's language authorizing the sharing of cyber threat indicators is too broad and will give the government too much access to private customer information.[90] Despite this opposition, President Obama signed CISA into law in December 2015.[91]

***b) Consumer Protection***

Congress introduced at least seven bills attempting to address cybersecurity breaches.[92] The goal for most of the legislation is to create a national standard that dictates company responses after discovering a data breach. One example is the proposed Data Security and Breach Notification Act. The bill aims to establish strong, uniform national data security and breach notification standards, which would expressly preempt any related state breach notification laws, in order to ensure uniformity.[93] The Notification Act would require companies that discover a data breach to notify consumers if there is a "reasonable risk" that the breach would result in consumers' economic harm, and to notify the FTC, Secret Service, or FBI in the event of a breach impacting more than 10,000 people.[94] Certain members of Congress and privacy activists have criticized the proposed Notification Act for two main reasons: First, the bill would preempt state laws that they contend do a better job protecting consumers' privacy. Second, notification requirements are triggered only if the company decides there is a risk of financial harm, which, in critics' view, gives companies too much discretion and would lead to incidents being underreported. The Committee on Energy and Commerce reported this bill to the full chamber in April, but there has been no movement since.

Shortly after the publication of a magazine article demonstrating how hackers could take remote control of a car,[95] Senators Ed Markey and Richard Blumenthal introduced the Security and Privacy in Your Car Act of 2015 ("SPY Car Act"), S. 1806. The SPY Car Act seeks to prevent cyber intrusions to Internet-connected cars by requiring: (1) anti-hacking measures for all "entry points to electronic systems," (2) manufacturers to separate critical software systems that affect the driver's control of the car from non-critical software systems, (3) that all driving data collected be "reasonably secured," and (4) that vehicles be able to "immediately detect, report, and stop attempts to intercept driving data or control the vehicle."[96] The Act has not advanced in Congress since being introduced in July, but lawmakers from the House of Representatives have since introduced the SPY Car Study Act to require the National Highway Safety Transportation Commission to conduct a yearlong study to recommend a framework for regulating automotive software.[97]

Other notable proposed legislation aimed at protecting consumer data included legislation regulating company use of geolocation data[98] and legislation that would strengthen the Children's Online Privacy Protection Act (COPPA) by, among other things, providing protection to children through age 15 (up from 13), and creating an "eraser button" allowing children to delete personal information online, similar to the 2015 California Digital Eraser law.[99]

### *c) Law Enforcement Access to Personal Information*

President Obama signed the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("USA FREEDOM Act") into law on June 2, 2015. The FREEDOM Act extends parts of the USA PATRIOT ACT and reauthorizes many of the NSA's surveillance activities while making several important changes. Three changes are of particular note. First, the FREEDOM Act effectively ended the NSA's bulk metadata collection program, although the government is still permitted to make targeted requests for information. Second, the Act limits the use of national security letters sent to technology companies demanding data. Third, the Act permits companies to challenge gag orders contained in national security letters and to make certain disclosures about government information orders and requests.[100]

Another key piece of legislation is the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act"), S. 512, which would amend ECPA to authorize the use of search warrants abroad only where the government seeks to obtain the contents of electronic communications of a United States citizen, not a foreign national.[101] Data belonging to foreign nationals would be obtained only if there is a treaty that requires the foreign government to provide assistance to the United States in criminal matters. Currently, law enforcement only needs to issue a subpoena--not a warrant as the law requires for other records that are abroad--to obtain records abroad that are more than 180 days old.[102] The LEADS Act has strong support from the tech industry, especially the cloud computing industry, because the Act could place limits on any non-U.S.-based investigation, driven by concerns that the U.S. government might access their citizens' and users' data stored in the cloud.

The E-mail Privacy Act, H.R. 699, is another proposed ECPA amendment with wide-ranging support. The bill would amend ECPA to require police to obtain a warrant before "a provider of electronic communication service or remote computing service" disclosed electronic messages such as e-mails and messages.[103] Despite strong support from industry leaders and elected officials in both parties, the bill has been delayed in the Judiciary Committee, largely because Committee Chairman Bob Goodlatte, the head of enforcement at the SEC, and others want to ensure the legislation does not hinder police work and civil investigations.[104]

## 2. State

In 2015, California continued to set new trends for privacy legislation. California adopted a new electronic privacy law, as well as new laws governing the growing "Internet of Things." In addition, 2015 saw many states updating their data breach notification laws, continuing efforts to protect student data, and newly focusing on regulating drones.

Governor Jerry Brown signed the California Electronic Communications Privacy Act into law on October 8, 2015.[105] The Act requires law enforcement in California to obtain a warrant before accessing any digital records, including e-mails, text messages, and information stored on smartphones.[106] There are exceptions, however. The government can access electronic communications when it has a good faith belief that an emergency requires access to the information,[107] and government agencies can still issue subpoenas for much of this information

where it is not sought for the purpose of investigating or prosecuting a criminal offense. The law requires the government to notify a person whose information is obtained by warrant when the warrant is executed.[108] A court may delay this notice procedure 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.[109] The law took effect on January 1, 2016.

California may also be paving the way for a new trend in consumer data protection laws in its regulation of smart televisions, likely a harbinger of increased regulation of the Internet of Things. In October, Governor Brown signed Assembly Bill 1166 into law, which requires manufacturers of Internet-connected, or "smart," televisions to notify customers of any voice recognition feature during initial installation. The law also prohibits manufacturers from selling or using any recordings collected through a voice recognition feature for advertising.[110]

Although Congress continued its efforts to pass a national data breach notification law, the status quo remains a patchwork of state data breach notification laws. At the start of this year, 47 states and the District of Columbia had enacted legislation requiring public or private entities to notify individuals after a security breach of personally identifiable information.[111] Although no new states added notification laws, there were a number of amendments to existing data breach notification laws. Most notably, Governor Brown signed three bills amending key sections of California's notification statute. First, personal information is now considered "encrypted" if it is "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."[112] Second, notifications must use specific language.[113] The Senate Bill includes a model notification form. Third, "personal information" now includes information captured by automated license plate recognition systems. Indeed, 2015 also saw several other states expanding the definition of "personal information" in their data breach notification laws.[114]

Several states also took steps to enact laws protecting student information. Following California's lead with 2014's Student Online Personal Information Protection Act, other states passed laws preventing online services used for K-12 schools from using or disclosing a student's information. New Hampshire now requires website and application operators targeting K-12 students and their families to create and maintain "reasonable" security procedures to protect personally identifiable information about a student.[115] The law also prohibits operators from using covered information for targeted advertising. Oregon now provides similar protections and restrictions on the use of students' information. Operators generally may not disclose student information to third parties, but may use "de-identified student information" to improve or market their products.[116]

This year many states also passed laws regulating drones. Perhaps reflecting reactions to several high-profile stories about drones,[117] the laws tended to regulate personal, recreational drone use.[118] For example, the Florida Senate proposed a bill that would prohibit using a drone to take pictures of privately owned property, or anyone on such property, without consent, if a reasonable expectation of privacy exists.[119] By contrast, Texas House Bill 2167 lists lawful ways drone operators can take photos. For example, surveyors and engineers can use drones "provided that no individual is identifiable in the image" captured.[120] California Governor Jerry Brown bucked this

legislative trend and vetoed three bills that would have prohibited civilians from flying drones over wildfires, schools, prisons, and jails. His veto statement explained that each of these acts were already criminal under other laws and cautioned against creating a more complex criminal code without commensurate benefit.[121]

## III. International Regulation of Privacy and Data Security

There have been a number of significant developments in the international regulation of data privacy and cybersecurity, most notably in the European Union, where the critical EU-US Safe Harbor program permitting international data transfers out of the EU was invalidated. Other major developments included the recent approval of the new EU General Data Protection Regulation, agreement on a new EU Cybersecurity Directive, continued application of the Right to Be Forgotten, and a number of notable developments in Russia, the Asia-Pacific region, and other countries.

### A. EU-US Safe Harbor and Data Transfer

On October 6, 2015, the European Court of Justice ("ECJ") addressed the fundamental right to the protection of personal data, as enshrined in the Charter of the Fundamental Rights of the European Union, and invalidated the EU-US Safe Harbor framework for the transatlantic transfer of data. Given the importance of this decision for so many companies, we have provided additional background and context in this review.

The privacy framework of the European Union rests in part on the Charter of the Fundamental Rights of the European Union (the "Charter").[122] Article 7 of the Charter provides for a fundamental right to respect for private and family life, and Article 8 provides for a fundamental right to protection of personal data.[123] As a component of EU privacy and human rights law, the European Union also adopted Directive 95/46/EC ("EU Data Protection Directive") in 1995 governing the protection of individuals with regard to the processing of their personal data within the EU.[124] Article 28(1) of the EU Data Protection Directive requires Member States to set up one or more public authorities responsible for independent monitoring of compliance with EU rules on the protection of individuals and processing of personal data. Article 25(1) of the EU Data Protection Directive also specifies a principle that transfers of personal data from the Member States to third countries may take place only if the third country ensures an "adequate level of protection."[125]

To facilitate international commerce and compliance with the EU data protection laws on the transfer of personal data between EU Member States and the U.S., the U.S. Department of Commerce issued the Safe Harbor Privacy Principles ("Safe Harbor") in 2000.[126] The Safe Harbor was intended for use by U.S. organizations receiving personal data from the EU and included a number of principles on protection of personal data to which the U.S. companies could subscribe voluntarily. Companies pledged adherence to the Safe Harbor principles through a process of self-certification. Importantly, in its Commission Decision 2000/520/EC of 26 July 2000 ("Commission Decision 2000/520"), the European Commission declared that the Safe Harbor regime, as implemented in accordance with the Department of Commerce guidance, was considered to ensure "an adequate level of protection" for

personal data transferred from the European Community to organizations in the U.S., as required by Article 25 of the EU Data Protection Directive.[127]

In the aftermath of the Snowden revelations of extensive collection of personal data by U.S. intelligence services, the Safe Harbor became increasingly questioned, with EU policymakers, including the EU Commission[128] and the European Parliament,[129] calling for an overhaul of the system. EU and U.S. authorities began negotiations for Safe Harbor reforms in 2013. In the past year, there has also been increasing enforcement oversight of the Safe Harbor from the FTC.[130]

### 1. ECJ *Schrems* Decision

On June 25, 2013, Maximilian Schrems, an Austrian national residing in Austria, made a complaint asking the Irish Data Protection Commissioner to prohibit a social network from transferring his personal data to the U.S., contending that U.S. law and practice did not ensure adequate protection of his personal data against surveillance activities of U.S. public authorities.[131] The Commissioner rejected the complaint as unfounded, concluding that he was not required to investigate the matters raised, in part because of Commission Decision 2000/520 finding that the Safe Harbor was considered to ensure an adequate level of protection for personal data transferred from the EU to the U.S. Mr. Schrems brought an action before the High Court of Ireland, challenging the Commissioner's decision not to investigate his complaint. The High Court of Ireland stayed the proceedings and requested a preliminary ruling from the ECJ.

On September 23, 2015, the Advocate General of the ECJ, Yves Bot, issued an advisory opinion, finding the Safe Harbor regime invalid.[132] The Advocate General reasoned that when systemic deficiencies were found in a third country to which personal data of EU citizens is transferred, the EU Member States must be able to take measures to safeguard the rights protected by the EU Charter of Fundamental Rights. He found that national supervisory authorities have the power to intervene and to suspend the data transfers they consider deficient, despite the general assessment made by the European Commission. Less than two weeks later, the ECJ issued its decision holding the European Commission's Safe Harbor adequacy determination invalid.[133]

The Court made two determinations. First, with respect to the powers of national supervisory authorities, the Court stated that the European Commission may adopt a decision that a third country ensures an adequate level of protection under Article 25 of the Directive and that decision is binding on all Member States and their organs, including national supervisory authorities. The Court stated that the Court alone has jurisdiction to declare an EU act, such as a Commission decision, invalid. However, a Commission determination, such as the Commission Decision 5000/250, does not prevent a national supervisory authority of a Member State from examining claims lodged by individuals concerning the processing of their personal data. According to the Court, national supervisory authorities must be able to examine with due diligence whether a transfer of a person's data to a third country complies with the EU Data Protection Directive requirement of "adequate level of protection."[134]

Second, with respect to the validity of the Commission Decision 5000/250 itself, the Court noted that U.S. public agencies can access personal data on the basis of a national security exception to the Safe Harbor and that the persons concerned had no judicial or administrative recourse to oppose such access. The Court deemed this to compromise the fundamental rights to private life and to judicial protection under the Charter. On that basis, the ECJ ruled the Safe Harbor to be invalid.[135]

### 2. Status of Safe Harbor Negotiations

Following the ECJ decision in *Schrems*, Frans Timmermans, First Vice President of the European Commission, stated that he sees the *Schrems* decision "as a confirmation of the European Commission's approach for the renegotiation of the Safe Harbour."[136] Commissioner Vera Jourova agreed, stating that the European Commission's work with the American authorities to revise the Safe Harbor can now be built on in light of the *Schrems* decision, stating "it is important that transatlantic data flows can continue, as they are the backbone of our economy."[137]

On November 6, 2015, the European Commission issued a press release, stating that it had stepped up its negotiations with the U.S. and that its objective is to conclude the negotiations within three months.[138] In the meantime, the Commission issued guidance on transatlantic data transfers, analyzing the consequences of the judgment and setting out alternative bases for transfers of personal data to the U.S.:[139]

- **Contractual Solutions**: The Commission has approved standard contractual clauses that apply to transfers between data controllers and processors.[140] The model clauses include advice on the responsibilities of data exporters and importers, security measures, notification to the data subject in case of transfer of sensitive data, notification to the data exporter if third countries' law enforcement requests access or of any unauthorized or accidental access, and remedial measures and compensation rules in case of damage arising from breach by either party.

- **Binding Corporate Rules for Intra-Group Transfers**: Where a multinational company would like to transfer personal data from the EU to corporate affiliates located outside the EU, it can adopt corporate rules addressed further below. *See section on Article 29 Working Party*.

- **Derogations**: Data can still be transferred where there is informed individual consent to the proposed transfer, important public interest grounds justifying the transfer as necessary, or where necessary for protection of vital interests of the data subject.

The Commission also emphasized that, unlike Commission adequacy decisions, which concern the general assessment of a third country's system and may cover all transfers to that country, the scope of the guidelines above is limited, and applies only to specific data flows. It is the data exporters and importers that bear the responsibility of ensuring that the transfers comply with the EU Data Protection Directive. The European data protection authorities have embraced the ECJ ruling.[141]

FTC Commissioner Julie Brill noted that the *Schrems* decision "clearly came as a shock to many policy makers and companies in the United States," and she said that invalidation of the Safe Harbor, including the self-certification program, will make FTC enforcement of companies' transatlantic

communications more difficult in the absence of company representations.[142] She also said that data transfers relying on the alternatives to Safe Harbor will not offer the same level of transparency previously ensured through the certification process. Brill also hoped that the negotiations would come to a "speedy and successful conclusion."[143]

### B. Other EU Developments

#### 1. EU General Data Protection Regulation Reform

On December 15, 2015, the European Commission, the European Parliament, and the European Council agreed to an EU data protection reform to boost the EU Digital Single Market. The bill should be adopted in early 2016 and come into force in 2018. The EU General Data Protection Regulation ("GDPR") will succeed the operative 1995 Data Privacy Directive, which was the first legal framework for personal data protection across multiple countries. The GDPR will replace the 1995 Data Privacy Directive in its entirety and will standardize data protection across all EU member states.

Core substantive elements of the agreed regulation include the following:

- **Extraterritorial Scope**: The regulation will cover not only data controllers established in the EU, but will also apply to businesses that target EU consumers in the European Economic Area, even if the businesses are not established in the EU and do not process data using servers in the EU.

- **Right to be Forgotten**: The GDPR will implement a "right to be forgotten" (officially called the "right to erasure") whereby personal data must be deleted when an individual no longer wants his or her data to be processed by a company and there are no legitimate reasons for retaining the data. The Council clarified that this right is not absolute and will always be subject to the legitimate interests of the public, including the freedom of expression, and historical and scientific research. This part of the GDPR may impose significant burdens on affected companies, as the creation of selective data destruction procedures often may impose significant costs.

- **Breach Notification**: The GDPR will require notification of security breaches within a specified period of time when the breach is likely to cause a degree of risk to an individual whose data has been compromised. The time period for notification is within 72 hours of awareness of a data breach.

- **Privacy-friendly Techniques**: Privacy by design is the idea that a product or service should be conceived from the outset to ensure a certain level of privacy for an individual's data. Privacy by default is the idea that a product's or service's default settings should help ensure privacy of individual data. The regulation will establish privacy by design and privacy by default as essential principles. By default, businesses should only process personal data to the extent necessary for their intended purposes and should not store it for longer than is necessary for those purposes. These principles will require data controllers to design data

protection safeguards into their products and services from the inception of the product development process. Privacy-friendly default settings also will be standard.

- **Data Portability**: The regulation will establish a right to data portability, which is intended to make it easier for individuals to transfer personal data from one service provider to another. This should enhance competition between providers.

- **Governance**: Data controllers and processors may be required to designate a Data Protection Officer ("DPO") in certain circumstances. Small and medium-sized enterprises ("SMEs") will be exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity.

These requirements will be supplemented by a much more rigid regime of fines for violations. Data Protection Authorities will be able to fine companies that do not comply with EU rules up to 4% of their global annual turnover. As a result of the extra-territorial application of the law, companies located outside the EU should take this into account.

### 2. EU Cyber Security Directive

In December 2015, EU institutions reached an informal agreement on the text of the EU Network and Information Security Directive, commonly referred to as the Cybersecurity Directive. Among other measures, the Cybersecurity Directive will require operators in certain sectors to meet minimum standards on network security and their ability to withstand cyber-attacks. Further, the legislation will require those operators to notify public authorities in the event of a cybersecurity breach.

The scope of the Cybersecurity Directive was widely debated within the EU. So-called critical operators in the energy, water, transport, health, and banking industries were always going to be covered, but it remained unclear whether digital service providers would also be covered. EU lawmakers eventually reached a compromise on the issue. Some digital service providers, including cloud services, e-commerce platforms, and search engines, will be covered, but supervision will reportedly be lighter than that applied to the critical operators. This compromise, reached after months of negotiation on the issue, is intended to reflect the higher degree of potential disruption to society posed by attacks on the critical operators.

Upon formal approval of the Cybersecurity Directive by EU Member States, each government will have 21 months to transpose it into national law. Member States will then have an additional six months to apply the framework created in the Directive to identify specific companies covered by national rules. Notably, the European Parliament's press release specifically identifies Amazon, eBay, and Google as companies that will likely be covered.[144]

### 3. National Data Privacy Law

In October 2015, the European Court of Justice analyzed the question of which national data protection law applies to a business operating across EU Member State borders, and the scope of the powers of the national Data Protection Authority ("DPA") in such scenarios. The Court, in line with the trend of

recent decisions, established a low threshold for the extent of activity that is sufficient to make a business subject to a Member State's data privacy law. The Court also held that if a foreign data privacy law applies, the local DPA lacks jurisdiction to impose penalties outside its own territory and may not impose penalties inside its territory based on alleged violations of the applicable foreign data privacy law.

In *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, the Hungarian DPA found Weltimmo, a Slovakian property-advertising company, in violation of the Hungarian data privacy law and imposed a fine, which Weltimmo disputed in Hungarian courts. The Hungarian courts then referred two questions to the European Court of Justice, asking whether the Hungarian data privacy law applied to Weltimmo, and whether the Hungarian DPA had validly exercised its powers.

Interpreting Article 4(1) of the EU Data Protection Directive, the Court held that the data protection law of an EU Member State applies to data processing activities "where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State."[145] Notably, the Court went on to emphasize that "establishment" is a "flexible concept," which "extends to any real and effective activity--even a minimal one--exercised through stable arrangements." Based on this flexible approach, the Court ruled that Weltimmo likely was established in Hungary and, therefore, bound by its data protection law and subject to its court.

Addressing the second question, the Court found that when a *foreign* data privacy law applies, the local DPA has very little power to impose punishments. Therefore, while DPAs have significant powers to apply their own laws to establishments in their territory, they have little power to apply any law (domestic or foreign) to entities whose activities in the state fall below a certain threshold.

### 4. Article 29 Working Party

The Article 29 Working Party is an independent advisory body on the protection of individuals with regard to the processing of personal data and on the free movement of such data in the EU. The body consists of representatives of national data privacy enforcement agencies, the EU Commission, and other EU institutions. The Working Party issues recommendations, opinions, and working documents, which are frequently relied upon as interpretive guidance by national courts and the EU Commission.

In November 2014, the Article 29 Working Party set forth a centralized process for the review of identical contractual clauses used by a company across multiple Member States (WP 226).[146] The European Commission has made it possible for companies to use standard contractual clauses that provide adequate safeguards during international data transfers. These clauses are one way to legitimize data transfers outside the EU where, for example, the third country has not been recognized as having an adequate level of data protection. While companies cannot amend or change the standard contractual clauses, they can use them in a wider contract with additional clauses.[147] Oftentimes, identical contractual clauses are used across different Member States and consequently, multiple data protection authorities are tasked with analyzing the same contract to assess its compliance with the standard contractual clauses. The new review process aims to reduce inconsistent conclusions

regarding the compliance of identical contractual clauses. The working document outlines the new procedure and the estimated timeline for approval.

Also in November 2014, the Article 29 Working Party issued a statement (WP 227) providing several points on balancing the protection of personal data and privacy with technological innovation and the need for security.[148] The Article 29 Working Party emphasized that data protection is a fundamental right and may not be treated as an economic asset. It also concluded that massive and indiscriminate surveillance is not ethically acceptable whether by third country authorities or by parties acting in the EU, even if data transfers are otherwise authorized.

In December 2014, the Article 29 Working Party adopted a working document (WP 228)[149] containing the legal analysis behind its April 2014 opinion on surveillance of electronic communications for intelligence and security purposes (WP 215).[150] Both the opinion and working document were in response to the mid-2013 discovery of surveillance programs originating from the United States and other countries, referred to as "the Snowden revelations." The Article 29 Working Party provided the current legal framework applicable to surveillance activities for the purpose of national security. This framework consists of a broad spectrum of legislation including United Nations legal instruments, such as the UN Universal Declaration of Human Rights, Council of Europe legal instruments, and European Union Law. The analysis focuses primarily on the legal restrictions on Member States with regards to their own surveillance activities and the transfer of individual data pursuant to the request of a third country public authority. The Article 29 Working Party emphasized that under current legislation and case law of the EU, there is no legal justification for the mass collection or transfer of personal data by either public or private entities for the purpose of surveillance.

In May 2015, the Working Party revised and adopted an explanatory document (WP 204 rev.01) on the Binding Corporate Rules ("BCRs") for data processors.[151] BCRs are a corporate code of conduct based on European data protection standards that ensure adequate safeguards during international transfers of personal data between companies that are part of the same corporation. A multinational company must draft and submit BCRs for approval in order to benefit from their protection. The explanatory document provides guidelines on what is expected in BCRs specifically for data processors that transfer data to subprocessors in the same organization. The revised explanatory document provides additional guidance for processers that receive data requests from third-party law enforcement authorities. The BCRs require that processors assess each request on a case-by-case basis and put the request on hold for a reasonable time in order to notify the data controller, the DPA competent for the controller, and the lead DPA for the processor BCR. These notifications must be made prior to any disclosures. If delay or notification is prohibited by the third-party law enforcement authorities, the BCRs require that the processor use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible.

In September 2015, the Article 29 Working Party issued an opinion (WP 232) analyzing the Data Protection Code of Conduct for Cloud Service Providers, which was drafted by a working group composed of representatives of the industry ("C-SIG").[152] The Code provides industry guidelines for cloud computing providers with regards to data protection and privacy rules in Europe. The Article

29 Working Party chose not to formally approve the current draft of the Code; however, it provides a number of recommendations for C-SIG to consider incorporating into the final version of the Code. One significant comment is that the Code should make clear that while adherence to codes of conduct is encouraged, it will not ensure any protection from DPAs' enforcement powers. In addition, the Article 29 Working Party remarked that the draft Code does not sufficiently elaborate on the specific legal obligations of each and every party involved. By clearly allocating the different roles between the provider and customer, data subjects will be better able to exercise their rights.

Most recently, in October 2015, the Article 29 Working Party issued a statement on the case, *Maximillian Schrems v. Data Protection Commissioner* (C-362-14).[153] While the Article 29 Working Party is still analyzing the impact of the ECJ judgment on other transfer tools, it stated that transfers taking place on the basis of the Safe Harbor decision (2000/520/EC) after the ECJ judgment are unlawful. However, DPAs still consider standard contractual clauses and BCRs legitimate legal tools for ensuring adequate safeguards during data transfers. The Working Party called on the Member States and European institutions to find an appropriate solution, such as a new Safe Harbor agreement, that would enable data transfers to the United States and respect fundamental rights. It noted, however, that if by the end of January 2016, no appropriate solution is found with United States authorities, the EU data protection authorities are committed to taking all necessary actions, including enforcement actions.

### C. EU Member Country Developments

#### 1. United Kingdom

The scope of liability for misuse of personal information in the United Kingdom has been placed in flux following an appellate court judgment entered against Google in March 2015. That case, *Google v. Vidal-Hall*, arose from allegations that Google illegally tracked the online activity of UK citizens while they used Apple's Safari browser and then applied that information to generate ads.[154] The plaintiffs alleged that Google's aggregation of their "browser-generated information" amounted to an improper collection of personal data under the British Data Protection Act and that they are entitled to damages for "distress," or non-pecuniary harm.[155] Before *Vidal-Hall*, the law was well-settled that a plaintiff seeking damages under the British Data Protection Act had to allege some form of economic harm.

The English and Welsh Court of Appeal issued two rulings that expand liability for data-protection violations in the UK. Without reaching the merits of the plaintiffs' claims, the court first acknowledged that misuse of private information constitutes a tort, although it aimed to clarify that this "does not create a new cause of action" but "simply gives the correct legal label to one that already exists."[156] By characterizing the plaintiffs' action as "made in tort," the court permitted the plaintiffs to serve their complaint on Google, domiciled in California, under the relevant jurisdictional provisions.[157] Second, the court determined that Section 13(2) of the British Data Protection Act, which bars plaintiffs from recovering moral damages for nonpecuniary loss, is incompatible with European Union laws on data privacy (specifically, Directive 95/46/EC), as well as the EU Charter of Fundamental Rights, both of which the court understood to protect privacy rather than economic

rights. Thus, the court ruled that Section 13(2) can no longer be applied to limit the availability of damages.[158]

In July, the Supreme Court of the United Kingdom granted Google the right to appeal only the lower court's ruling regarding the availability of moral damages, thus implicitly affirming its conclusion that the plaintiffs had a valid cause of action in tort.[159] Unless and until the lower court's ruling is reversed, plaintiffs in the UK can seek damages for violations of the British Data Protection Act even if they allege only emotional harm.

### 2. France

The European Court of Justice's 2014 ruling that European Union citizens enjoy a "right to be forgotten" has begun to produce the discord and confusion that many data privacy experts in the United States expected when the ruling was first announced. Granting the petition of a Spanish citizen who sought the removal of certain links from Google's search engine, the Court of Justice held that search engines must allow EU citizens to request the erasure of results that contain damaging personal or public information about them. Ultimately, the Court articulated a balancing test that accounts for, on the one hand, the individual's right to privacy, and on the other, the public's right to freely access information.

Unsurprisingly, this ruling has proven difficult to implement, for the simple reason that a link erased on Google.fr is still readily available through Google.com. In June 2015, France's central regulator of data privacy (*La Commission Nationale de l'Informatique et des Libertés*, or "CNIL") gave Google formal notice that it expected the company to comply with right-to-be-forgotten requests on a global scale and erase links not only from its European search engines, but from all versions of its search engine available in all countries.[160] Google responded that it would not comply and, through its Global Privacy Counsel, stated that "as a matter of principle, we respectfully disagree with the idea that a national data protection authority can assert global authority to control the content that people can access around the world."[161]

Google then filed an informal appeal of CNIL's order, arguing that the right to be forgotten "is not the law globally," that France has no authority to impose its laws outside its jurisdiction, and that the agency's order risks imposing "serious chilling effects on the web."[162] CNIL rejected the appeal[163] and is now authorized to begin fining Google for its non-compliance. While CNIL currently can fine Google only around €300,000 for its refusal to comply with the order, legislation is pending in the European Union that would increase the fine to as much as 2-to-5% of Google's *global* revenue--easily over $1 billion.

### 3. Germany

Germany recently bolstered its cybersecurity regime with its passage of the Act to Increase the Security of Information Technology Systems ("IT Security Act") in July 2015. This new law applies only to certain sectors of the German economy identified as providing "critical infrastructure" to the public--specifically, the energy, IT, telecommunications, transportation, health, water, food, finance, and insurance industries--and aims to strengthen their technical and organizational safeguards against

cyberattack. In addition, the law requires providers of so-called tele media services (*e.g.*, online shops and other companies offering services through media like the Internet) to implement "state of the art" security measures (expressly including secure encryption technologies) for the protection of their IT infrastructure and the data of their customers.

The full scope and operation of the IT Security Act, including the precise definition of what will qualify as "critical infrastructure," will not be clear until an implementing directive will enter into force, which is expected for later in 2016. Once that directive enters into force, the "critical infrastructure" industries will be required to implement sector-specific "state of the art" IT security measures within two years. Each sector will have the opportunity to work with the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, or "BSI") in developing the standards that will govern it. The IT Security Act also requires regulated entities to (1) prove to the BSI their compliance with security requirements at least once every two years, through audits, certifications, or examinations; (2) designate a liaison to the BSI within six months from the entry into force of the implementing directive; and (3) notify the BSI immediately if their IT systems are disrupted or compromised. Violations of the law may result in administrative fines of up to €100,000.

### D. Asia-Pacific Developments

#### 1. China

China has experienced several large-scale data breaches in recent years. In September 2015, the XcodeGhost malware was found to have compromised hundreds of iOS apps, including popular Chinese apps WeChat, Didi Taxi, and Gaode Maps, affecting millions of Chinese users.[164] In October 2015, hundreds of apps using an advertising SDK developed by Youmi, including Chinese online mail service provider NetEase, were reportedly compromised, potentially affecting over one hundred million users.[165] Against this general backdrop, Beijing has continued its efforts in legislating data privacy and cybersecurity protections in 2015, releasing a draft Network Security Law and amending the Criminal Law provision on illegally obtaining, selling and providing personal information.

The draft Network Security Law ("NSL"), released for public comment in June 2015, is the closest China has come to enacting a comprehensive data privacy law. The draft law proposes to codify some of the information security measures previously set forth in other laws and authorities, such as the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection* (2012),[166] and *Information Security Technology: Guidelines for Personal Information Protection on Public and Commercial Service Information Systems* (2013) ("MIIT Guidelines").[167] For example, the draft NSL requires network operators to keep citizens' personal information confidential, and to give notice to obtain consent from the data subject when collecting and using personal information. Unlike the MIIT Guidelines, however, the draft NSL does not describe in detail what information must be included in the data privacy notice, nor does it distinguish between the forms of consent required to collect sensitive and non-sensitive personal information. In addition, the draft NSL obligates a network operator to take immediate remedial actions, notify

affected users, and report to relevant authorities in the event of a data breach. The draft law also holds operators of "key information infrastructures" to higher data security standards, requiring operators of basic information networks, in key industries, military and government networks, and large ISPs to store personal information within the People's Republic of China, absent a security assessment indicating true necessity for storing personal data offshore.

The draft NSL references and anticipates other relevant laws, rules and regulations, including those yet to be enacted, and embeds a placeholder for the designation of data privacy enforcement authorities. One of the laws that should be read in conjunction with the NSL is Article 253-1 of the PRC Criminal Law, which criminalizes illegally obtaining, selling, and illegally providing citizens' personal information. As originally enacted in 2009, liability was limited to staff members of State Organs or financial, telecommunication, transportation, education, and medical institutions who illegally obtain citizens' personal information in the course of fulfilling their job duties or providing services and then sells or illegally provides the information to others. In 2013, the owners of a business intelligence firm, ChinaWhys, were convicted under Article 253-1 for buying household registration, mobile phone, and border entry/exit records of Chinese nationals and selling reports incorporating such information to clients that included multinational companies.[168] The *ChinaWhys* case raised questions regarding downstream liability for recipients of personal information that may have originated from government or quasi-governmental institutions.

In November 2015, China promulgated the Ninth Amendment to its Criminal Law, which included an amendment of Article 253-1. The amended statute broadened the scope of criminal liability, sanctioning *anyone* who obtains citizens' personal information *in violation of State requirements* and sells or provides the information to others. Penalties are increased where the information was obtained in the course of fulfilling job duties or providing services, with the maximum prison term increasing from three years to seven years. Under the new amendment, private companies (*e.g.*, Internet service providers or online retailers) and individuals (*e.g.*, employees of private companies, business intelligence consultants, or hackers) may all be subject to criminal sanctions for leaking ill-gotten personal information, even if they do not receive compensation for the information. Given the developing landscape of China's data privacy laws, however, it can be difficult to know exactly what types of information were improperly obtained. Therefore, companies should be careful when handling personal information and ensure that information was obtained from public sources, with the data subject's consent, or otherwise comports with current local requirements.

While Chinese data privacy laws increasingly restrict information from leaving China, these restrictions may not be recognized by United States courts as sufficient reason to refrain from producing documents in discovery, creating a potential legal dilemma for multinational corporations. The recent decisions in *Gucci America, Inc. v. Weixing Li* illustrate the problem. In *Gucci*, plaintiff trademark holders requested alleged counterfeiters' bank account records from a third party, Bank of China ("BOC"). *Gucci Am., Inc. v. Weixing Li*, No. 10 CIV. 4974 RJS, 2015 WL 5707135, at *1 (S.D.N.Y. Sept. 29, 2015). BOC resisted the subpoenas, citing Chinese bank secrecy laws and opinion letters from Chinese regulators to argue that the bank could not release the requested records without violating Chinese law. *Id.* at *10. District Judge Richard Sullivan disagreed, finding no support for BOC's assertion that the Chinese bank secrecy laws are actually enforced, and that the

United States' interest in enforcing trademark laws "clearly outweigh BOC's interest in resisting compliance [with the subpoena] and China's interest in its bank secrecy laws." *Id.* at *11. The judge ordered BOC to comply with the subpoena and, when it failed to do so, held BOC in contempt and imposed a daily fine of $50,000 until BOC produces the subpoenaed records. *Gucci Am.*, No. 10 CIV. 4974 RJS, slip op. at 12 (Nov. 30, 2015), ECF No. 176. BOC immediately applied to the U.S. Court of Appeals for the Second Circuit to stay Judge Sullivan's order. Brief of Non-Party Appellant Bank of China at 12-13, *Gucci Am., Inc. v. Weixing Li*, No. 15-3850 (2d Cir. Dec. 1, 2015), ECF No. 9-2. Following briefing on the merits, the Second Circuit panel denied BOC's motion for a stay of Judge Sullivan's order. *Gucci Am.*, No. 15-3850, slip op. at 1 (2d Cir. Jan. 12, 2016), ECF No. 72.

### 2. South Korea

South Korea had an eventful year on the data privacy front. On July 23, 2015, a South Korean data protection criminal task force announced the indictment of 23 individuals and ten companies for violations of the Personal Information Protection Act. The cases involve the collection and transfer of health and prescription data without consent. The task force investigation commenced in 2013, and reports suggest that the breaches affected approximately 44 million individuals. The country's National Intelligence Service also announced in October that North Korean hackers stole sensitive data, including government audit data, and confidential files from the computers of South Korean lawmakers, and successfully hacked into servers at the presidential Blue House.

Following on the 2014 amendments to its data protection regime, the South Korean government has continued to press ahead with additional legislative efforts in response to a number of major data breaches. Under a new amendment to the *Personal Information Protection Act* published on July 7, 2015, which comes into effect in July 2016, those who mishandle personal data may be liable to pay punitive damages of up to three times the actual damage from a data breach. The amendment also allows consumers to claim damages of up to KRW 3 million (~USD 2,640). The Personal Information Protection Committee has been given greater enforcement powers to recommend policy and system changes and to handle dispute resolution. The Korean Communications Commission, the country's data protection authority, has also produced a guide on the collection and use of personal information through mobile apps and smartphone operating systems, which was enforceable beginning in October 2015.

A number of other amendments to Korean data privacy laws came into effect throughout the year, including revisions to the *Use and Protection of Credit Information Act* in September 2015 and the *Standards of Personal Security Measures* in late December 2014. The former was partially amended to enhance the protection of personal credit information and to require credit information companies to financially compensate for personal data breaches, while the latter is intended to address gaps in the legislation pertaining to third-party data processing outsourcing and the use of mobile devices in processing personal information.

### 3. Singapore

The data protection regime in Singapore remains fairly nascent given the recent operation of the Personal Data Protection Act 2012 ("PDPA") in 2014. The PDPA comprises two broad areas of data protection: (i) the Do Not Call ("DNC") Registry and (ii) the main data protection rules. The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, text messages, and faxes from marketers. The main data protection rules govern the collection, use, disclosure and care of personal data. These rules also prescribe the rights of access and correction of personal data, as well as regulate the transfer of personal data outside of Singapore.

Enforcement of the PDPA has been swift since its operation in 2014. However, many of the breaches concern the DNC Registry rather than the main data protection rules. To date, two companies have been brought to court for multiple breaches of the DNC Registry, receiving fines of SGD 30,000 (~USD 21,000) and SGD 80,000 (~USD 57,000), respectively. The Personal Data Protection Commission ("PDPC") has also issued advisory notices to about 2,000 organizations regarding minor isolated breaches. Separately, the PDPC has also been active in publishing industry-specific guidelines to aid organizations in complying with data protection requirements. Telecommunications, education, real estate, and healthcare industries are some examples where sector-specific issues have been addressed. Recently, the PDPC also clarified that mobile application developers in Singapore have to observe the data protection requirements in the law.

Moving forward, companies in Singapore are still not required to report data breaches, distinguishing the country from jurisdictions such as the United States and Canada. However, recent guidelines issued by the PDPC do encourage organizations to report data breaches so that preventive measures can be implemented.

### 4. Japan

In May 2015, hackers compromised the Japan Pension Service ("JPS") exposing the names, identification numbers, birth dates, and addresses of more than 1.2 million individuals. JPS staff computers were improperly accessed by an external virus embedded in an e-mail attachment disguised as a health ministry document.

Japan also passed amendments to its personal information protection act, known as *The Act on the Protection of Personal Information* ("APPI"), in September 2015. One of the most significant changes is the establishment of a Personal Information Protection Committee, which combines certain advisory, investigatory, and enforcement functions currently exercised by separate bodies under the APPI. The amendments to the APPI also include specific restrictions on the collection of sensitive information, the export of data to third parties outside of Japan, and the disclosure of "anonymized" personal data. Companies and their employees may be charged with criminal liability if they are found to have stolen or transferred personal information for improper gain. Perhaps most fundamental is the expanded definition of "personal information," which now includes biometric data and identifying numbers.

The APPI amendments have been introduced alongside a controversial personal identification system intended to simplify the administration of tax, pension, health care, and other official services. Starting in October 2015, each Japanese resident is to receive a personal identification number, popularly known as "My Number," which took effect in January 2016. The aim of the system is to help authorities combat tax evasion and the receipt of improper gains, and will culminate in the linking of My Numbers to individual bank accounts, among other possible available uses. Critics of the measure cite data privacy concerns.

#### 5. Malaysia

A day after Malaysia Airlines Flight MH370 disappeared en route from Kuala Lumpur to Beijing, several government agencies in Malaysia fell victim to a cyberattack, resulting in the loss of classified data from around 30 computers in the Department of Civil Aviation, the National Security Council, and Malaysia Airlines. According to media reports, government departments were sent a virus disguised as a news story about the disappearance of the plane. The attack was traced back to Chinese hackers and halted by CyberSecurity Malaysia.

### E. Other International Developments of Note

Elsewhere in the world, more countries have introduced privacy-related regulations ranging from data breach laws, to restrictions on data transfer, and even additions of a right to be forgotten. In particular, data breaches continue to affect both the public and private sectors. One of India's most popular music streaming websites was hacked, potentially exposing the records of 10 million users' data.[169] The Saudi Arabian government also suffered a breach, involving access to around 3,000 of its computers, revealing potentially sensitive government information.[170] In the first half of 2015 alone, there were 33 notifications of data breaches in Canada, 19 in Australia, 8 in New Zealand, and possibly many more unreported or unknown by the organizations managing the data.[171] As a result of the massive number of worldwide breaches and in a concern over the safety of individuals and the public, some countries have taken steps to protect consumers and citizens by mandating the reporting of data breaches under certain circumstances.

While Canada has a patchwork of data breach notification requirements in a few of its provinces, the federal Digital Privacy Act received Royal Assent in June of this year, amending the Personal Information Protection and Electronic Documents Act ("PIPEDA") with important data breach requirements for the entire country.[172] The major provisions related to breach reporting and notification--located in Section 10 of the Act--will be in force once the regulations containing specific requirements are set out by the federal government.[173] Once in force, Section 10 will require that, if a data breach poses a "real risk of significant harm" to affected individuals, the organization must take remedial steps.[174] "Significant harm" includes bodily harm, reputational damage, loss of employment, financial loss, and identity theft.[175] The organization must report the breach to the Office of the Privacy Commissioner of Canada, and must notify the affected individuals as soon as possible.[176] Additionally, organizations must retain a record of all breaches involving personal information.[177] Failure to notify the Commissioner or affected individuals or to maintain an adequate record can result in fines up to $100,000.[178]

Australia also unveiled its own proposed data breach notification requirements. Under the current Privacy Act 1988, notification of a breach of personal data is voluntary.[179] However, a December 2015 draft bill would amend the Privacy Act, and a mandatory data breach notification system would come into effect twelve months after the bill receives Royal Assent.[180] This new system would apply to those organizations covered under the existing Privacy Act, including most Australian Government agencies and most private organizations with over $3 million in annual turnover.[181] The organization would be required to notify the Australian Information Commissioner and the affected individuals if a "serious data breach" occurs.[182] In the current draft bill, a serious data breach would occur if one of the following is subject to unauthorized access or disclosure and would put individuals at real risk of serious harm: personal information, credit reporting information, credit eligibility information, or tax file number information.[183] Further details of what amounts to a serious data breach will be set out in regulations once the draft bill receives Royal Assent.[184] Failure to comply with the data breach notification requirements could result in a binding determination by the Australian Information Commissioner, civil penalties, or both.[185] The draft bill is set to be introduced into Parliament some time in 2016.[186]

Amid privacy watchdog's concerns over an increased surveillance state, Australia also recently enacted the Telecommunications Interception and Access Amendment Data Retention Act 2015 ("Data Retention Act"), which received Royal Assent in April of 2015.[187] The Data Retention Act requires that all telecommunication companies and Internet service providers retain their customers' metadata for two years.[188] This metadata contains the customers' communications information, including who was communicated with, when the communication took place, how the communication took place, how long the communication lasted, and the location of the equipment used in the communication.[189] However, the metadata does not include the substance of the customers' communications.[190] The data must be stored for two years in an encrypted and secure manner, and will be subject to the aforementioned draft bill's data breach notification requirements.[191]

In July 2015, Russian President Vladimir Putin signed into law the "right to be forgotten" legislation requiring Internet search engines to remove links to Russian citizens' personal information upon demand.[192] The law came into effect on January 1, 2016, and allows both private and public figures to request that information be erased.[193] Under the law, search engines have ten business days to comply with a request to delete a specific hyperlink from a search result.[194] Also, on September 1, 2015, Russia's Data Localization Law took effect.[195] First enacted in July 2014, Federal Law No. 242-FZ was originally scheduled to come into force in September 2016, however, a subsequent amendment passed at the end of 2014 accelerated its effective date.[196] The Data Localization Law requires "data operators"--which encompass public and private entities that process personal data--to collect, store, and process Russian citizens' personal data using databases located within Russian territory.[197] The Russian Data Protection Authority (Roskomnadzor) has the authority to block websites that violate the law and list offenders in a registry of privacy infringers.[198] Operators are allowed to transfer Russian personal data to foreign databases so long as the data was initially collected in a Russian database and the transfers comport with Russian data protection requirements.[199]

Rounding out the efforts to govern ever-growing data privacy issues, New Zealand appears to be close to issuing its own proposed data breach notification mandate.[200] Currently, New Zealand--like

Australia--has a voluntary breach notification system.[201] While it is unclear when proposals for mandatory data breach notifications will be made, the reporting is likely to be similar to the laws in Canada and Australia, requiring notification both to the Privacy Commissioner and to affected individuals.[202] Additionally, failing to report a breach would carry a fine of up to $10,000.[203]

## IV. U.S. Government Data Collection

### A. Data Collection and Device Unlocking

#### 1. Remote Access Warrants

A proposed amendment to Federal Rule of Criminal Procedure 41 would expand law enforcement agencies' ability to remotely search computers.[204] The proposed amendment would allow a judge to grant a warrant to remotely search a computer, no matter where it is geographically located, when the computer's location is unknown.[205] Additionally, the proposed amendment would permit law enforcement to get a single search warrant for any investigation where the computers to be searched are spread among five or more districts.[206] The amendment would set a "reasonable efforts" standard for law enforcement to inform a user that his or her computer was subject to a remote-access search.[207]

In February 2015, during the period for public comment, numerous civil liberties groups announced their opposition to the proposed amendments, arguing that the changes would expand law enforcement's reach by permitting the FBI to target millions of computers, including computers outside of the United States.[208] The Department of Justice issued a public response to this backlash, stating that the proposed amendment was a necessary update to close a procedural gap that emerged when prosecuting 21st-century cybercrimes.[209] On September 17, 2015, the Judicial Conference of the United States approved the proposed amendment and subsequently passed the proposed amendment to the Supreme Court.[210] The Supreme Court has until May 1, 2016, to adopt the proposed amendment and transmit it to Congress.[211] Unless Congress takes contrary action, the amendment will take effect on December 1, 2016.[212]

#### 2. Compelled Production of Passwords

There were several notable case law developments this year concerning the compelled production of electronic passwords. In September 2015, a Pennsylvania federal district court held that two former employees could invoke their Fifth Amendment right against self-incrimination and refuse to disclose their personal passcodes for company-issued smartphones to government officials. *SEC v. Huang*, No. CV 15-269, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015). Whether providing the passcode to an encrypted device is "testimonial" evidence protected by the Fifth Amendment has divided district courts for some time.[213] However, as biometric passcodes become more prevalent, the issue may recede in importance. For example, in *Commonwealth v. Baust*, a Virginia appellate court held that requiring a defendant to provide a fingerprint (which can be used to unlock many contemporary smartphones and laptops) is not testimonial in nature. 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

### 3. Warrantless Cell Location Tracking

Another notable development is an emerging circuit split concerning whether obtaining cell phone location data without a warrant violates the Fourth Amendment. Three circuits have directly wrestled with whether law enforcement can compel wireless carriers to turn over historical cell-site location information under the Stored Communications Act ("SCA").[214] In 2013, the Fifth Circuit held that the data amounted to unprotected business records and could be obtained without a warrant.[215] In May last year, in an *en banc* decision, the Eleventh Circuit reached the same conclusion.[216] However, in August 2015, a Fourth Circuit panel held that the government's procurement of historical cell-site data was an unreasonable search, and *explicitly* disagreed with the Fifth and Eleventh Circuit rulings.[217] The Fourth Circuit has agreed to an *en banc* review, and the rehearing is scheduled to take place in March 2016.[218]

### 4. Interactions with Tech Companies

Tech companies shifted towards encryption-by-default in 2015. Jumpstarted by the release of Apple's iOS 8 operating system in late 2014, an increasing number of mobile devices encrypt their users' data by default.[219] For example, although Google's Android operating system has had encryption capabilities for some time, only recently has it defaulted to encrypt user data, including photos, messages, e-mails, contacts, call history, calendar, etc.[220] The encryption standards used by these devices are designed to resist so-called "brute force" attacks, and have no encryption "backdoors." Because Apple and Google do not store a user's decryption password, they are incapable of decrypting a user's device for law enforcement.[221]

The rapid proliferation of unbreakable encryption has alarmed law enforcement officials, who worry that such encryption will hinder investigations into terrorism, child pornography, and other crimes. Former U.S. Attorney General Eric Holder,[222] Federal Bureau of Investigation Director James Comey,[223] and Manhattan District Attorney Cyrus Vance[224] have all publicly expressed concerns that default encryption renders information important to public safety inaccessible to law enforcement, even after law enforcement obtains a warrant. Law enforcement officials have now called for technology companies to build backdoors that would allow the manufacturer of the device or the government (with a warrant) to access encrypted user data.[225] Technology companies, along with civil liberties groups and cryptologists, have publicly lobbied against any weakening of encryption standards.[226] In October 2015, the Obama administration decided against seeking a legislative remedy from Congress on the encryption issue, instead opting to continue lobbying technology companies for a decryption backdoor.[227]

## B. Subpoena Extraterritoriality

One of the most significant data-privacy issues probed in 2015, and likely to be decided in 2016, concerns requests by United States law enforcement agencies for electronic data stored overseas, but maintained or controlled by domestic entities. In July 2014, Judge Loretta Preska of the Southern District of New York ordered Microsoft to give the U.S. Department of Justice access to Outlook.com e-mails stored on servers in Ireland, which the Department had sought in connection with a criminal

investigation. After hearing oral argument, Judge Preska affirmed[228] a Magistrate Judge's conclusion that the Stored Communications Act (SCA) requires an Internet service provider such as Microsoft to produce information stored on servers located overseas when presented with a SCA-compliant warrant because they do not violate the presumption against extraterritorial application of American law.[229]

Microsoft immediately appealed the order, arguing that the SCA does not extend to electronic communications stored outside the United States because the SCA contains no provision that overrides the presumption against the extraterritorial application of statutes.[230] In response, the United States argued that the SCA governs Microsoft's obligations because it maintains custody and control of the e-mails regardless of where they are stored.[231] Dozens of amici chimed in to support Microsoft's position, ranging from privacy-rights organizations to major media and tech companies, the government of Ireland, and a member of the European Union Parliament, who warned that a ruling in the Department of Justice's favor would flaunt EU data privacy law and further erode Europeans' trust in American IT providers. The Second Circuit held oral argument in September 2015.

---

[1] 66 F. Supp. 3d 1154 (D. Minn. 2014).

[2] *See also Longenecker-Wells v. BeneCard Servs., Inc.*, No. 1:15-CV-00422, 2015 WL 5576753 (M.D. Pa. Sept. 22, 2015); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015); *Smith v. Triad of Alabama, LLC*, No. 1:14-CV-324-WKW, 2015 WL 5793318 (M.D. Ala. Sept. 29, 2015).

[3] Despite the court's holding in *Neiman Marcus*, offering such services to affected individuals may still be required, as some states require providing free credit monitoring following a reportable data breach. Moreover, even where there is little or no risk of harm, offering free credit monitoring may help reestablish goodwill with affected individuals and potentially moot affected individual's out-of-pocket expenses for credit monitoring or identity protection that would otherwise be used to try to establish Article III standing.

[4] In 2015, LinkedIn agreed to settle a case for $13 million in which plaintiffs accused the company of "breaking into" their third-party e-mail accounts, downloading e-mail addresses and sending out e-mails, on behalf of the user himself, and advertising LinkedIn to nonmembers, without the users' consent, in violation of the SCA, Wiretap Act, ECPA, and various California privacy laws. Complaint, *Perkins et al v. LinkedIn Corp.*, No. 13-CV-04303-LHK, 2013 WL 5220959 (N.D. Cal. Sep. 17, 2013). In June 2014, Judge Koh dismissed plaintiffs' SCA and Wiretap Act claims, finding LinkedIn's disclosures clear enough to establish consent for the practice of collecting users' e-mail addresses, but leaving intact claims related to LinkedIn's use of the e-mail addresses due to lack of clear disclosures regarding that practice. *Perkins et al v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1213–14, 1216–17 (N.D. Cal. 2014). The settlement in this case underscores the importance of having clear disclosures, as courts appear disinclined to find consent at the motion to dismiss phase.

[5] Patrick Lunsford, *Judge Approves Third Largest TCPA Settlement Ever with Credit Card Issuer*, Insidearm (March 9, 2015), *available at* http://www.insidearm.com/daily/credit-card-accounts-receivable/credit-card-receivables/judge-approves-third-largest-tcpa-settlement-ever-with-credit-card-issuer; *see also Pines Nursing Home, Inc. v. PharMerica Corp*, No. 1:13-cv-23924 (S. D. Fla.) ($15 million settlement); *Kolinek v. Walgreen Co.*, No. 1:13-cv-04806, 2015 WL 7450759 (N.D. Ill. Nov. 23, 2015) ($11 million settlement); *Chimeno-Buzzi v. Hollister Co. et al.*, No. 1:14-cv-23120 (N.D. Ill.) ($10 million); *Douglas v. Western Union Co.*, No. 1:14-cv-01741 (N.D. Ill.) ($8.5 million settlement).

[6] *See, e.g.*, *Glauser v. GroupMe, Inc.*, No. C 11-2584, 2015 WL 475111 (N.D. Cal. Feb. 4, 2015) (holding that a system is only considered an "autodialer" if it has the present capacity to dial numbers randomly or sequentially, regardless of any potential capacity if the technology were reconfigured); *Gragg v. Orange Cab Co.*, 995 F. Supp. 2d 1189 (W.D. Wash. 2014); *Dominguez v. Yahoo!*, *Inc.*, 8 F. Supp. 3d 637 (E.D. Pa. 2014). The Third Circuit remanded *Dominguez v. Yahoo!*, *Inc.*, No. 14-1751, 2015 WL 6405811 (3d Cir. Oct. 23, 2015), for a decision responsive to the FCC's order, specifically requiring further evidence with respect to the device-in-question's present and potential autodialing capacity.

[7] Since the FCC order was issued, courts have continued to dispose of cases where there was evidence that the calls were dialed with the aid of human intervention. *See, e.g.*, *Estrella v. LTD Financial Services*, *LP*, No. 14-2624, 2015 U.S. Dist. LEXIS 148249 (M.D. Fla. Nov. 2, 2015) (granting partial summary judgment where the record evidenced that each of the alleged calls at issue had been dialed manually); *McKenna v. WhisperText*, *LLC*, No. 5:14-CV-00424, 2015 WL 5264750 (N.D. Cal. Sept. 9, 2015) (granting motion to dismiss with prejudice because the plaintiff's pleadings admitted that the transmission of text messages required human intervention); *Derby v. AOL*, *Inc.*, No. 5:15-CV-00452, 2015 WL 5316403 (N.D. Cal. Sep. 11, 2015) (granting motion to dismiss with prejudice, finding the challenged text messages, as alleged in the pleadings, sent through "human intervention").

[8] In September 2015, the Eastern District of North Carolina adopted a magistrate judge's recommendation that summary judgment be entered in favor of the defendant because the defendant had a good faith belief that it obtained consent to call the plaintiff. *See Danehy v. Time Warner Cable Enterprises*, No. 5:14-CV-133-FL, 2015 WL 5534285 (E.D.N.C. Sept. 18, 2015). It remains to be seen whether courts will adopt this reasoning in light of the FCC's order.

[9] In so doing, the FCC has signaled that it agrees with the Third Circuit and other jurisdictions that view the TCPA as a "remedial statute" that "should be construed to benefit consumers." *Leyse v. Bank of Am. Nat. Ass'n*, 804 F.3d 316, 327 (3d Cir. 2015) (quotations omitted) (recognizing that the balance of interests favors consumer plaintiffs in TCPA cases).

[10] Rite Aid Corp. also separately filed an additional brief, contending that communications protected by the Health Insurance Portability and Accountability Act that were previously exempt are now subject to three different standards under the TCPA, depending on the type of telephone number being called.

[11] *See* Andrea Peterson, *How a failed Supreme Court bid is still causing headaches for Hulu and Netflix*, Washington Post (Dec. 27, 2013), *available at* https://www.washingtonpost.com/news/the-switch/wp/2013/12/27/how-a-failed-supreme-court-bid-is-still-causing-headaches-for-hulu-and-netflix/. The Act was amended in 2011 to incorporate a more company-friendly consent provision (Netflix, among others) heavily advocated for the amendment). Previously, the act had allowed disclosure of PII only if the video provider had specific written consent. The amendment clarifies that consumers may consent to disclosure of their video viewing information: 1) in advance, for a set period of time (2 years or until consent is withdrawn, whichever comes sooner); 2) through an electronic means using the Internet; and 3) in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer. The video provider must also allow the consumer to withdraw consent on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election.

[12] In light of its decision on Plaintiff's failure to qualify as a "subscriber," the appeals court "express[ed] no view on the district court's reading of the term 'personally identifiable information' in the VPPA." *Id*. at 1258 n.2.

[13] While the court dismissed the claim against AMC on these grounds, it rejected AMC's Article III standing argument, holding instead that Congress can confer standing through statutory enactment and that the VPPA provides right of relief to plaintiffs alleging wrongful disclosure even without additional injury. *Id*. at 668.

[14] *See, e.g.*, *Adjamian v. L'Oreal USA S/D*, *Inc.*, No. B257403, 2015 WL 4400119, at *9 (Cal. Ct. App. July 20, 2015) (denying class certification where cashiers had only the capacity to record the personal information of customers, but there was no evidence customers had given any information involuntarily or as a condition to a transaction).

[15] In one study, 43% of respondent companies reported suffering a data breach in 2014, which is a significant rise from 33% in 2013. Ponemon Institute, 2014 Second Annual Study on Data Breach Preparedness (September 2014), *available at* http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf. Another study found an annualized growth rate of 66% in cybersecurity incidents worldwide from 2009 to 2014 (PWC, *PWC Global State of Information Security Survey 2015*, 7 (2014), *available at* http://www.pwccn.com/webmedia/doc/635527689739110925_rcs_info_security_2015.pdf) , and another found that 38% more security incidents were detected in 2015 than in 2014 (PWC, *PWC Global State of Information Security Survey 2016*, 2 (2015), *available at* http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html). In the wake of several of the higher-profile data breaches, Sony, Target, Anthem, and Neiman Marcus

[16] In June 2014, Securities and Exchange Commission Commissioner Luis Aguilar cautioned that "boards that choose to ignore or minimize the importance of cybersecurity oversight responsibility do so at their own peril." SEC Commission Luis Aguilar, *Boards of Directors*, *Corporate Governance and Cyber-Risks: Sharpening the Focus* (speech delivered on June 10, 2014), *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370542057946. Other federal agencies have also

exercised regulatory jurisdiction over data security issues in recent years, including the Federal Trade Commission and the Federal Communications Commission (within the telecommunications sector), and state attorneys general have also been increasingly active in this sphere.

[17] Alison Frankel, *Ugly-duckling shareholder derivative suits are poised for swandom*, REUTERS (Jan. 2, 2015), *available at* http://blogs.reuters.com/alison-frankel/2015/01/02/ugly-duckling-shareholder-derivative-suits-are-poised-for-swandom/.

[18] As one commentator recently noted, "[g]iven that . . . [corporate] data breaches themselves are almost certain to continue, the probabilities are that data breach-related [derivative] litigation will become an increasingly important part of the corporate and securities landscape." Kevin M. LaCroix, *The Breach-Related Derivative Suit Trend Continues*, Law360 (Sept. 15, 2015), *available at* http://www.law360.com/articles/702523/the-breach-related-derivative-suit-trend-continues.

[19] Ponemon Institute, *2015 Global Megatrends in Cybersecurity* (February 2015), *available at* http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

[20] *See*, *e.g.*, Order Granting Motion to Dismiss at n.1, *Palkon et al. v. Holmes et al.*, No. 2:14-cv-01234 (SRC) (D. N.J. October 20, 2014); Memorandum in Support of Defendants' Motion to Dismiss at 16, 18-22, *Bennek v. Ackerman et al.*, No. 1:15-cv-2999 (TWT) (N.D. Ga. October 30, 2015).

[21] *In re Caremark*, 698 A.2d at 961.

[22] *Id.* at 967.

[23] *See* Del. Code. Ann. tit. 8, § 145; *see also*, *e.g.*, *Homestore*, *Inc. v. Tafeen*, 888 A.2d 204, 211-13 (Del. 2005).

[24] Verified Shareholder Derivative Complaint at ¶¶ 2-3, *Palkon et al. v. Holmes et al.*, No. 2:14-cv-01234 (SRC) (D. N.J. February 25, 2014).

[25] Order Granting Motion to Dismiss at 3, 9-10, *Palkon et al. v. Holmes et al.*, No. 2:14-cv-01234 (SRC) (D. N.J. Oct. 20, 2014).

[26] *Id.* at 11.

[27] Verified Shareholder Derivative Complaint, *Bennek v. Ackerman et al.*, No. 1:15-cv-2999 (TWT) (N.D. Ga. Sept. 2, 2015).

[28] Verified Shareholder Derivative Complaint at ¶ 82.

[29] *Bennek v. Ackerman et al.*, No. 1:15-cv-2999 (TWT), Dkt. 17-1, at *16 (N.D. Ga. Oct. 30, 2015).

[30] *Id.* at *19-20.

[31] *See In re Target Corporate Shareholder Derivative Litigation*, No. 0:14-cv-00203-PAM-JJK (D. Minn. Jan. 21, 2014). Additionally, in the wake of this breach, at least one prominent proxy advisory firm (Institutional Shareholder Services, Inc.) advised shareholders to vote out seven of Target's ten board members for their alleged failure to appropriately "manage risk and protect Target from [a] massive data breach." *See* Linda Chiem, *7 Target Board Members in ISS' Crosshairs Over Data Breach*, Law360 (May 28, 2014), *available at* http://www.law360.com/articles/542228/7-target-board-members-in-iss-crosshairs-over-data-breach.

[32] Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis (May 2014); *available at* http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf ; *c.f.*, Ponemon Institute, 2015 Cost of Data Breach Study: United States (May 2015), *available at* http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEW03055USEN.

[33] National Association of Insurance Commissioners, *The National System of State Regulation and Cybersecurity*, *available at* http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last visited Jan. 26, 2016).

[34] *Rice v. InSync, et al*., No. 30-2014-00701147-CU-NP-CJC (Cal. Sup. Ct. Jan. 27, 2014).

[35] *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal.) (filed May 7, 2015).

[36] Complaint at ¶¶ 4-5, 7, 26-29, *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal. May 7, 2015), ECF No. 1.

[37] Order Granting Motion to Dismiss at 3, *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432 (C.D. Cal. July 17, 2015), ECF No. 22 (finding failure to exhaust non-judicial remedies).

[38] Remarks by Deputy Secretary Sarah Bloom Raskin at The Center For Strategic And International Studies Strategic Technologies Program (Sept. 10, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/j10158.aspx.

[39] Memorandum from Benjamin M. Lawsky to All NYS-Chartered or Licensed Banking Institutions regarding New Cyber Security Examination Process (Dec. 10, 2014), *available at* http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf.

[40] U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations (OCIE) 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[41] *Id*. at 2.

[42] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015).

[43] *Id.* at 241-42.

[44] First Amended Complaint for Injunctive and Other Equitable Relief at ¶ 24, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d. Cir. 2015) (No. 14-3514).

[45] *Wyndham*, 799 F.3d at 247.

[46] *Id.* at 247-48.

[47] Allison Grande, *FTC Tips Data Security Hand In Wyndham Pact*, Law 360 (Dec. 10, 2015, 10:21 PM), *available at* http://www.law360.com/privacy/articles/736584?nl_pk=ff8b9493-af0a-4368-80ed-c5a325b6e825&utm_source=newsletter&utm_medium=e-mail&utm_campaign=privacy.

[48] *Id.*

[49] *Id.*

[50] Allison Grande, *Wyndham Agrees To Audits To End FTC Data Breach Suit*, Law 360 (Dec. 9, 2015, 11:48 AM), *available at* http://www.law360.com/articles/735984/wyndham-agrees-to-audits-to-end-ftc-data-breach-suit-.

[51] *Id.*

[52] Grande, FTC Tips Data Security Hand In Wyndham Pact, *supra* note 47.

[53] *See In the Matter of LabMD*, *Inc.*, *Order Denying Respondent LabMD's Motion to Dismiss*, Dkt. No. 9357, (Jan. 16, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf; *see also* Allison Grande, *11th Circ. Turns Away LabMD in FTC Data Security Row*, Law360 (Jan. 20, 2015, 4:16 PM), *available at* http://www.law360.com/articles/613049/11th-circ-turns-away-labmd-in-ftc-data-security-row.

[54] LabMD states that it went out of business due to the "debilitating effects" of the FTC's practices and investigation. *See* Greg Slabodkin, *FTC Appeals Decision to Dismiss Complaint against LabMD*, (Nov. 30, 2015), *available at* http://www.healthdatamanagement.com/news/FTC-appeals-decision-to-dismiss-compliant-against-LabMD-51640-1.html.

[55] Initial Decision at 13-14, *In the Matter of LabMD*, *Inc.*, No. 9357 (F.T.C. Nov. 13, 2015).

[56] *Id*.

[57] *Id*.

[58] Slabodkin, *supra* note 54.

[59] *Id.*

[60] Allison Grande, *FTC Adds Image-Matching Method to COPPA Consent Options*, Law360 (Nov. 20, 2015), *available at* http://www.law360.com/articles/729854/ftc-adds-image-matching-method-to-coppa-consent-options.

[61] *Id.*

[62] Joe Van Acker, *LifeLock Pays Record $100M Fine to Settle FTC False Ad Lawsuit*, Law360 (Dec. 17, 2015), *available at* http://www.law360.com/privacy/articles/739303?nl_pk=ff8b9493-af0a-4368-80ed-c5a325b6e825&utm_source=newsletter&utm_medium=e-mail&utm_campaign=privacy.

[63] *Federal Trade Commission v. LifeLock, Inc.*, No. CV-10-00530-PHX-MHM (D. Ariz. July 21, 2015).

[64] Press Release, Federal Trade Commission, *FTC Approves Final Order In TRUSTe Privacy Case*, (Mar. 18, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-truste-privacy-case.

[65] *Id*.

[66] Press Release, Federal Trade Commission, *Retail Tracking Firm Settles FTC Charges It Misled Consumers About Opt Out Choices* (Apr. 23, 2015), *available a*t https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers.

[67] *Id.*

[68] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015).

[69] John L. Mills and Pedro M. Allende, *FTC Consent Decrees Are Best Guide to Cybersecurity Policies*, Daily Business Review (Sept. 21, 2015), *available at* http://www.dailybusinessreview.com/id=1202737711574/FTC-Consent-Decrees-Are-Best-Guide-to-Cybersecurity-Policies?slreturn=20151110181134.

[70] Press Release, Federal Trade Commission, *FTC Kicks Off "Start With Security" Business Education Initiative* (June 30, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.

[71] Federal Trade Commission, *Start with Security: A Guide for Business*, *Lessons Learned from FTC Cases* (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[72] Teri Robinson, "R.T. Jones reaches settlement with SEC in data breach case," SC Magazine (Sept. 23, 2015), *available at* http://www.scmagazine.com/sec-hits-security-adviser-with-75000-penalty-in-breach-settlement/article/440268/.

[73] SEC, *Cybersecurity Examination Sweep Summary*, National Exam Program Risk Alert, Vol. IV, Issue 4 (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[74] *Id*. at 2.

[75] *Id*. at 4.

[76] SEC, *OCIE Cybersecurity Initiative*, National Exam Program Risk Alert, Vol. IV, Issue 8 (Sept. 15, 2015), *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[77] *Id.* at 2-3.

[78] Robinson, *supra*, note 72.

[79] *Id*.

[80] Press Release, Securities and Exchange Commission, *SEC Charges Investment Advisor with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach* (Sept. 22, 2015), *available at* https://www.sec.gov/news/pressrelease/2015-202.html.

[81] *Id.*

[82] *Id.*

[83] *See* FCC: *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report* (Mar. 2015); FINRA: *Report on Cybersecurity Practices* (Feb. 2015); DOJ: *Best Practices for Victim Response and Reporting of Cyber Incidents* (Apr. 2015); OMB: *Improving Cybersecurity Protections in Federal Acquisitions* (Fall 2015, proposed).

[84] Y. Peter Kang, *Conn. AG Launches Lenovo Probe Over Superfish Adware*, Law360 (Mar. 2, 2015), *available at* http://www.law360.com/privacy/articles/626871?nl_pk=ff8b9493-af0a-4368-80ed-c5a325b6e825&utm_source=newsletter&utm_medium=e-mail&utm_campaign=privacy.

[85] For example, on November 9, 2015, the New York State Department of Financial Services ("NYDFS") issued a letter to the Financial and Banking Information Infrastructure Committee (FBIIC) setting forth proposed cybersecurity requirements for financial institutions regulated by NYDFS. The proposed rules are derived from the results of a NYDFS survey of cybersecurity programs from regulated banking institutions and regulated insurers, as well as risk assessments of other covered entities. Covered entities would be required to implement and maintain written cyber security policies and procedures that address 12 areas of concern, including information security, systems and network security, vendor management, customer data privacy, and incident response planning. *See* Albanese, Anthony J., Acting Superintendent of Financial Services, New York State Department of Financial

Services, "Potential New NYDFS Cyber Security Regulation Requirements" (Nov. 9, 2015), *available at* http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

[86] Marina Koren, *About Those Fingerprints Stolen in the OPM Hack* (Sept. 23, 2015), *available at* http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/.

[87] S. 754, 114th Cong., preamble (2015).

[88] *Id.* § 106; *see* Daniel Wilson, *Senate Passes Cybersecurity Information Sharing Act*, Law360 (Oct. 27, 2015, 6:30 PM), *available at* http://www.law360.com/privacy/articles/719328?nl_pk=f6e2b761-9e8f-436b-9326-cb6fb8c493fa&utm_source=newsletter&utm_medium=e-mail&utm_campaign=privacy.

[89] Brian Fung, *Apple and Dropbox say they don't support a key cybersecurity bill*, *days before a crucial vote*, Wash. Post.: The Switch (Oct. 20, 2015), *available at* https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/apple-says-its-against-a-key-cybersecurity-bill-days-before-a-crucial-vote/.

[90] *See* Danny Weitzner, *The new US cybersecurity bill will invade your privacy, but it won't keep you safe*, Quartz (Nov. 8, 2015), *available at* http://qz.com/543692/americans-should-probably-be-more-freaked-out-about-that-new-cybersecurity-bill/.

[91] *See* Executive Office of the President, *Statement of Administration Policy*, *S. 754 – Cybersecurity Information Sharing Act of 2015* (Oct. 22, 2015).

[92] *Data Breach Notification Bills: What You Need to Know* (Jun. 9, 2015), *available at* https://cayan.com/data-breach-notification-bills-what-you-need-to-know.

[93] H.R. 1770, 114th Cong., § 1 (2015).

[94] *Id.* § 3.

[95] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway--With Me in it*, Wired (July 21, 2015, 6:00 AM), *available at* http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Senator Markey's spokesperson insisted that the introduction of the bill was not related to the story. *Id.*

[96] S. 1806, 114th Cong. (2015).

[97] *Congressmen Lieu Introduces Bipartisan SPY Car Study Act to Help Ensure Safe Automobile Operating Systems* (Nov. 5, 2015), *available at* https://lieu.house.gov/media-center/press-releases/congressman-lieu-introduces-bipartisan-spy-car-study-act-help-ensure.

[98] The Location Privacy Protection Act would require companies to obtain customer consent before collecting geolocation data. The law creates a private cause of action, and total damage award

could amount to $1 million or more. *See* Jimmy Hoover, *Sen. Franken Introduces Bill Banning GPS-Stalking Apps*, Law 360 (Nov. 12, 2015, 6:34 PM), *available at* http://www.law360.com/privacy/articles/726295?nl_pk=f6e2b761-9e8f-436b-9326-cb6fb8c493fa&utm_source=newsletter&utm_medium=e-mail&utm_campaign=privacy.

[99] S. 1563, 114th Cong., §§ 2, 3 (2015). For more information on the California Eraser law, *see* Alexander Southwell and Joshua Jessen, *California's New 'Digital Eraser' Evaporates Embarrassment, Part 2 of 2: New California Privacy Laws Will Make It Easier For Kids To Remove Inappropriate Posts From Websites* (Nov. 19, 2013), *available at* http://www.gibsondunn.com/publications/Documents/SouthwellCaliforniaPrivacyPartTwo.pdf.

[100] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

[101] S. 512, 114th Cong., § 2 (2015).

[102] Mario Trujilo, *House members push bill limiting gov access to e-mails stored overseas,* The Hill (Feb. 27, 2015, 12:40 PM), *available at* http://thehill.com/policy/technology/234121-house-members-drop-bill-limiting-gov-access-to-overseas-e-mail.

[103] H.R. 699, 114th Cong., § 3 (2015); Julian Hattem, *With half of House, lawmakers push e-mail privacy bi*ll, The Hill (Feb. 4, 2015, 7:01 AM), *available at* http://thehill.com/policy/technology/231677-with-half-of-house-lawmakers-push-e-mail-privacy-bill.

[104] Brendan Sasso, *Why is the wildly popular E-mail Privacy Act still stuck in Congress?,* NextGov (Dec. 2, 2015), *available at* http://www.nextgov.com/defense/2015/12/why-wildly-popular-e-mail-privacy-act-still-stuck-congress/124126/.

[105] Cal. Penal Code § 1546(d) (2015).

[106] "CalECPA" is not the first statute to impose such a requirement. Other states with similar laws include Minnesota, Utah, Virginia, and Washington.

[107] *Id.* § 1546.1(c)(5).

[108] *Id.* § 1546.2(a)

[109] *Id.* § 1546.2(b).

[110] An Act to Add Chapter 35 to Division 8 of the Business and Professions Code, Relating to Business, A.B. 1166, Reg. Sess. 2015 (Cal. 2015).

[111] Alabama, one of the states without a data breach notification law, considered enacting one this year, but postponed its consideration indefinitely.

[112] Cal. Civ. Code §§ 1798.29(h)(4) and 1798.82(i)(4) (2015).

[113] Cal. Civ. Code §§ 1798.29(d) and 1798.82(d) (2015).

[114] For example, Oregon added health insurance policy number or identification numbers, medical information, and biometric data. *See* An Act Relating to Enforcement of Notification Requirements for Breaches of Security Involving Personal Information, S.B. 601, 78th Leg., Reg. Sess. 2015 (Or. 2015). Montana's notification law now covers medical record information, taxpayer identification numbers, and account numbers in combination with passwords to a financial account. *See* An Act Revising Data System Security Breach Notification Laws, H.B. 74, 64th Leg. Reg. Sess. 2015 (Mont. 2015).

[115] An Act Establishing Privacy Protections for Student Online Personal Information, H.B. 520, Reg. Sess. 2015 (N.H. 2015).

[116] An Act Relating to Student Privacy, S.B. 187, 78th Leg., Reg. Sess. 2015 (Or. 2015).

[117] In January 2015, for example, an off-duty federal employee accidentally crashed his friend's drone onto the White House lawn. *See* Michael D. Shear & Michael S. Schmidt, *White House Drone Crash Described as a U.S. Worker's Drunken Lark*, The New York Times (Jan. 27, 2015), *available at* http://www.nytimes.com/2015/01/28/us/white-house-drone.html. In August 2015, Maryland authorities caught two men who they believed were about to use a drone to deliver porn, drugs, and a firearm to prisoners. *See* Dominique Debucquoy-Dodley & Greg Botelho, *Authorities foil drone-delivery of porn*, *drugs*, *and gun to Maryland prison*, CNN (Aug. 24, 2015, 8:50 PM), *available at* http://www.cnn.com/2015/08/24/us/maryland-prison-drone/.

[118] However, a few states, including Maine and Virginia, passed laws that place significant restrictions on police use of drones. *See* An Act to Regulate Domestic Unmanned Aerial Vehicle Use, L.D. 25, 127th Leg., Reg. Sess. 2015 (Me. 2015); An Act Relating to Use of Unmanned Aircraft Systems by Public Bodies; Search Warrant Required, H.B. 2125, Reg. Sess. 2015 (Va. 2015).

[119] An Act Relating to Surveillance by a Drone, S.B. 766, Reg. Sess. 2015 (Fla. 2015).

[120] An Act Relating to Certain Images Captured by an Unmanned Aircraft, H.B. 2167, 84th Leg., Reg. Sess. 2015 (Tex. 2015).

[121] *See* Patrick McGreevy, *With strong message against creating new crimes*, *Gov. Brown vetoes drone bills*, Los Angeles Times (Oct. 3, 2015, 3:24 PM), *available at* http://www.latimes.com/politics/la-me-pc-gov-brown-vetoes-bills-restricting-hobbyist-drones-at-fires-schools-prisons-20151003-story.html.

[122] *See* Charter of Fundamental Rights of the European Union 2000/C 364/01, 2000 O.J. (C 364), 1-22, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[123] *See id.* at 10.

[124] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, 1995 O.J. (L281) 31-50, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

[125] *See id.* at 47.

[126] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 FR 45666-01.

[127] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the European Council on the Adequacy Of The Protection Provided By The Safe Harbor Privacy Principles And Related Frequently Asked Questions by the U.S. Department of Commerce, 2000 O.J. (L 215) 7-47, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

[128] *See* European Commission Press Release IP/13/1166, *Restoring Trust in the EU-US Data Flows – Frequently Asked Questions* (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[129] *See* Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," EUR. PARL. DOC. 2013/2188(INI), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//EN.

[130] *See* Press Release, *Federal Trade Commission, FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework* (Jan. 21, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

[131] *See Schrems v. Data Prot. Comm'n* [2014] IEHC 310 for a procedural history of the *Schrems* case in Irish courts and the High Court ruling.

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

[133] *See* Case C-362/14, *Maximilian Schrems v. Data Prot. Comm'n*, 2015 E.C.R. I-1-35, *available at* https://cdt.org/files/2015/10/schrems.pdf.

[134] *See id.*

[135] *See id.*

[136] *See* European Commission Statement/15/7582, First Vice-President Timmermans and Commissioner Jourová's Press Conference on Safe Harbour Following the Court Ruling in Case C-362/14 (Schrems) (Oct. 6, 2015), *available at* http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.

[137] *See id.*

[138] *See* European Commission Press Release IP/15/6015, Commission Issues Guidance on Transatlantic Data Transfers and Urges the Swift Establishment of a New Framework Following the Ruling in the Schrems Case (Nov. 6, 2015), *available at* http://europa.eu/rapid/press-release_IP-15-6015_en.htm.

[139] *See* Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM (2015) 566 final (Nov. 6, 2015), *available at* http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

[140] The European Commission provides model contractual clauses. *See* Commission Decision 2001/497/EC, 2001 O.J. (L 181) 19-31; Commission Decision 2004/915/EC, 2004 O.J. (L 385) 74-84; and Commission Decision 2010/87/EU, 2010 O.J. (L 349) 48, *available at* http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[141] *See* Statement of the Article 29 Working Party, European Commission (Oct. 16, 2015), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[142] *See* Commissioner Julie Brill, *Federal Trade Comm'n, Keynote Address, Transatlantic Privacy after Schrems: Time for An Honest Conversation* (Oct. 23, 2015), *available at* https://www.ftc.gov/public-statements/2015/10/transatlantic-privacy-after-schrems-time-honest-conversation.

[143] *See id.*

[144] Press Release, European Union, *MEPs Close Deal With Council on First Ever EU Rules on Cybersecurity* (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.

[145] Case Câ€‘230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (Oct. 1, 2015). *available at* http://curia.europa.eu.

[146] *See* Article 29 Working Party, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual Clauses" Considered as Compliant with the EC Model Clauses* (Article 29 Working Doc. WP 226, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf.

[147] *See* European Union, *Frequently Asked Questions Relating to Transfers of Personal Data From the EU/EEA to Third Countries*.

[148] *See* Article 29 Work Party, *Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party* (Article 29 Working Doc. WP 227, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf.

[149] *See* Article 29 Work Party, Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes (Article 29 Working Doc. WP 228, 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

[150] *See* Article 29 Work Party, Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes (Article 29 Working Doc. WP 215, 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

[151] *See* Article 29 Work Party, Explanatory Document on the Processor Binding Corporate Rules (Article 29 Working Doc. WP 204 rev. 1, 2015), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf.

[152] *See* Article 29 Work Party, *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing* (Article 29 Working Document WP 232, 2015), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf.

[153] *See* Press Release, Article 29 Working Party, *Statement of the Article 29 Working Party* (Oct. 16, 2015), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf; *see also* Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, *available at* http://curia.europa.eu (Oct. 6, 2015).

[154] *Google v. Vidal-Hall*, Case No. A2/2014/0403 (Supreme Court of the United Kingdom, July 28, 2015); *see also Google v. Vidal-Hall* [2015] EWCA Civ 311 (lower court opinion, Mar. 27, 2015).

[155] *Google v. Vidal-Hall* [2015] EWCA Civ 311, at ¶¶ 2-5.

[156] *Id.* at ¶ 51.

[157] *Id.* at ¶¶ 6-11.

[158] *Id.* at ¶¶ 82-94.

[159] The Supreme Court of the United Kingdom's July 28, 2015 order is available at https://www.supremecourt.uk/news/permission-to-appeal-decisions-28-july-2015.html.

[160] *See* CNIL's June 12, 2015 Press Release, *CNIL orders Google to apply delisting on all domain names of the search engine*, *available a*t http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/.

[161] *See* Google's July 30, 2015 Public Statement, Implementing a European, not global, right to be forgotten, *available at* http://googlepolicyeurope.blogspot.com/2015/07/implementing-european-not-global-right.html.

[162] Leila Abboud, *France rejects Google appeal on cleaning up search results globally*, Reuters (September 21, 2015) *available a*t http://www.reuters.com/article/us-france-google-idUSKCN0RL13J20150921 (quoting public remarks offered by Peter Fleischer, Google's global privacy counsel).

[163] *See* CNIL's September 21, 2015 Press Release, *Right to delisting: Google informal appeal rejected*, *available at* http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/.

[164] Joe Rossignol, *Apple Lists Top 25 Apps Compromised by XcodeGhost Malware*, MacRumors (Sept. 24, 2015, 6:00 AM), *available at* http://www.macrumors.com/2015/09/24/xcodeghost-top-25-apps-apple-list/.

[165] Lisa Eadicicco, *Hundreds of Apps Have Been Banned from Apple's App Store for Spying on Your Personal Information*, Business Insider (Oct. 19, 2015, 1:16 PM), *available at* http://www.businessinsider.com/apple-removes-apps-youmi-sdk-personal-information-2015-10?utm_content=buffer34d5e&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer .

[166] Laney Zhang, *China: NPC Decision on Network Information Protection*, Library of Congress: Global Legal Monitor (Jan. 4, 2013),*available at* http://www.loc.gov/law/foreign-news/article/china-npc-decision-on-network-information-protection/.

[167] Graham Greenleaf & George Tian, *China Expands Data Protection through 2013 Guidelines: A 'Third Line' for Personal Information Protection (With a Translation of the Guidelines)*, 122 Privacy Laws & Bus. Int'l Rep. 1 (2013), *available at* http://ssrn.com/abstract=2280037 .

[168] David Barboza, *In China*, *British Investigator Hired by Glaxo*, *and Wife*, *Sentenced to Prison*, The New York Times (Aug. 8, 2014), *available at* http://www.nytimes.com/2014/08/09/business/international/in-china-british-investigator-hired-by-glaxo-and-his-wife-are-sentenced-to-prison.html?_r=0 (providing background regarding the case).

[169] *Gaana.com Confirms Its User Database Was Hacked*, Gadgets360 (May 28, 2015), *available at* http://gadgets.ndtv.com/internet/news/gaanacom-allegedly-hacked-details-of-all-users-exposed-697111; *see also 2015 First Half Review: Findings from the Breach Level Index*, Gemalto 1, 4, *available at* http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf.

[170] *Yemeni Group Hacks 3,000 Saudi Govt* [sic] *Computers to Reveal Top Secret Docs* [sic], Reuters (May 22, 2015), *available at* https://www.rt.com/news/261073-yemen-cyber-hack-saudi/; *see also 2015 First Half Review: Findings from the Breach Level Index*, Gemalto 1, 4, *available at* http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf.

[171] *2015 First Half Review: Findings from the Breach Level Index*, Gemalto 1, 12–13, *available at* http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf.

[172] *The Digital Privacy Act*, Office of the Privacy Commissioner of Canada 1, 1, *available at* https://www.priv.gc.ca/resource/fs-fi/02_05_d_63_s4_e.asp.

[173] *Id*.

[174] *Id*. at 4.

[175] *Id*. at 5.

[176] *Id*.

[177] *Id*.

[178] *Id*.

[179] *Discussion Paper--Mandatory Data Breach Notification*, Attorney-General's Department (December 2015), *available at* https://www.ag.gov.au/Consultations/Pages/serious-data-breach-notification.aspx.

[180] *Id* at 5.

[181] *Id*.

[182] *Id*.

[183] *Id*.

[184] *Id*. at 6.

[185] *Id*. at 7.

[186] *Id.* at 3.

[187] *Data Retention*, Attorney-General's Department, *available at* https://www.ag.gov.au/dataretention.

[188] *Id*.

[189] *Id*.

[190] *Id*; *see also* Caroline Simson, *Australia OKs Data Retention Bill Despite Privacy Concerns*, Law360 (Mar. 27, 2015),*available at* https://www.law360.com/articles/636319/australia oksdataretentionbilldespiteprivacyconcerns.

[191] *Data Retention: Guidelines for Service Providers*, Attorney-General's Department (July 2015), 3–4, *available at* http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Industry-Implementation-of-data-retention.aspx.

[192] Vera Shaftan, *Russia Signs Controversial "Right to be Forgotten" Bill Into Law*, Data Protection Report (July 23, 2015), *available at* http://www.dataprotectionreport.com/2015/07/russia-signs-controversial-right-to-be-forgotten-bill-into-law/.

[193] *Id*.

[194] *Id*.

[195] Sergei Blagov, *Multinationals to Meet Russia Data Localization Rules*, Bloomberg BNA (Sept. 2, 2015), *available at* http://www.bna.com/multinationals-meet-russia-n17179935650/.

[196] Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, Bloomberg BNA (Aug. 5, 2015), *available at* http://www.bna.com/russia-clarifies-looming-n17179934521/.

[197] Ania Nussbaum, *Russia's Data Law Will Hurt Its Economy –Think Tank*, WSJ Digits (June 18, 2015), *available at* http://blogs.wsj.com/digits/2015/06/18/russias-data-law-will-hurt-its-economy-think-tank/; *see also id*.

[198] Daria Litvinova, *Russia's New Personal Data Law Will Be Hard to Implement*, *Experts Say*, The Moscow Times (Sept. 1, 2015), *available at* http://www.themoscowtimes.com/article/529195.html.

[199] Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, Bloomberg BNA (Aug. 5, 2015), *available at* http://www.bna.com/russia-clarifies-looming-n17179934521/.

[200] *Privacy Law Changes to Strengthen Protection*, The Beehive (May 28, 2014), *available at* http://www.beehive.govt.nz/release/privacy-law-changes-strengthen-protection.

[201] *See id*.

[202] *Id*.

[203] *Id*.

[204] Memorandum from Jeffrey S. Sutton, Committee on Rules of Practice and Procedure, to Scott S. Harris, Clerk of the Supreme Court of the United States, Summary of Proposed Amendments to Federal Rules, 7 (Oct. 9, 2015), *available at* http://www.uscourts.gov/file/18641/download..

[205] *Id*.

[206] *Id*.

[207] Memorandum from James C. Duff, Judicial Conference of the United States, to The Chief Justice of the United States and Associate Justices of the Supreme Court, Transmittal of Proposed Amendments to the Federal Rules of Criminal Procedure, 11, 13 (Oct. 9, 2015), *available at* http://www.uscourts.gov/file/18641/download.

[208] *See*, *e.g.*, American Civil Liberties Union, Comment on Proposed Amendment to Rule 41 Concerning Remote Searches of Electronic Storage Media (Apr. 4, 2014), *available at* https://www.aclu.org/sites/default/files/assets/aclu_comments_on_rule_41.pdf.

[209] David Bitkower, Department of Justice Criminal Division, Response to Post on Proposed Amendment to Rule 41 (Oct. 20, 2014), *available at* http://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0055&attachmentNumber=1&disposition=attachment&contentType=pdf.

[210] Memorandum from Rebecca Womeldorf, Administrative Office of the United States Courts, to Scott Harris, Clerk of the Supreme Court of the United States (Oct. 9, 2015), *available at* http://www.uscourts.gov/file/18641/download.

[211] Memorandum from Jeffrey S. Sutton, Committee on Rules of Practice and Procedure, to Scott S. Harris, Clerk of the Supreme Court of the United States, Summary of Proposed Amendments to Federal Rules, 1 (Oct. 9, 2015), *available at* http://www.uscourts.gov/file/18641/download.

[212] *Id*.

[213] *Compare In re Grand Jury Subpoena Duces Tecum Dated Mar. 25*, *2011*, 670 F.3d 1335 (11th Cir. 2012) (holding that providing a password is a testimonial act), *and In re The Decryption of a Seized Data Storage System*, Order Denying Application to Compel Decryption, Case No. 13-M-449 (E.D. Wisc. Apr. 19, 2013) (same), *with United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012) (holding production of unencrypted drive by defendant did not implicate Fifth Amendment right against self-incrimination), *and Commonwealth v. Gelfgatt*, SUCR2010-10491 (Sup. Ct. Mass. Nov. 6, 2014) (holding defendant in contempt for failure to unlock password protected drives).

[214] The type of data in question is generated whenever a cellphone communicates with the closest cell phone tower to make calls or exchange data. The resulting records can arguably provide a rough approximation of where the cell phone (and presumably its owner) was located at various points in time.

[215] *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 611–15 (5th Cir. 2013).

[216] *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

[217] *United States v. Graham*, 796 F.3d 332, 355–57 (4th Cir. 2015).

[218] *United States v. Graham*, No. 12-4659 (L), 2015 WL 6531272, at *1 (4th Cir. Oct. 28, 2015).

[219] *See* Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8*, *Making Handover to Cops Moot*, Ars Technica (Sept. 18, 2014, 12:57 AM), *available at* http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/; Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC News (Sept. 19, 2014), *available at* http://www.bbc.com/news/technology-29276955.

[220] Lucian Constantin, *Google Makes Full-Disk Encryption and Secure Boot Mandatory for Some Android 6.0 Devices*, IT World (Oct. 20, 2015), *available at* http://www.itworld.com/article/2995437/android/google-makes-full-disk-encryption-and-secure-boot-mandatory-for-some-android-60-devices.html.

[221] However, the encryption only applies to data stored on the user's device. Information stored on cloud computing platforms (*e.g.*, Apple's iCloud service or Dropbox) is not necessarily subject to the default encryption standards and can be accessed by the service provider (such as Apple or Dropbox).

[222] David Kravets, *US Top Cop Decries Encryption*, *Demands Backdoors*, Ars Technica (Oct. 1, 2014, 1:30 PM), *available at* http://arstechnica.com/tech-policy/2014/10/us-top-cop-decries-encryption-demands-backdoors/.

[223] Brent Kendall, *FBI Director Raises Concerns About Smartphone-Security Plans*, Wall Street J. (Sept. 25, 2014, 2:57 PM), *available at* http://www.wsj.com/articles/fbi-director-raises-concerns-about-smartphone-security-plans-1411671434?mod=WSJ_TechWSJD_NeedToKnow.

[224] Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety (Nov. 2015), *available at* http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

[225] While the Communications Assistance for Law Enforcement Act ("CALEA") requires telecommunications companies to make their telephone networks accessible for lawful government wiretaps, it does not apply to Internet service providers or manufacturers of smartphones. *See* 47 U.S.C. §§ 1001-07; 18 U.S.C. § 2522.

[226] Letter to Barack Obama (May 19, 2015), *available at* http://cdn.arstechnica.net/wp-content/uploads/2015/05/cryptoletter.pdf; David Kravets, *Tech Sector Tells Obama Encryption Backdoors "Undermine Human Rights,"* Ars Technica (May 19, 2015, 12:48 PM), *available at*

http://arstechnica.com/tech-policy/2015/05/tech-sector-tells-obama-encryption-backdoors-undermine-human-rights/.

[227] Ellen Nakashima & Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data – For Now*, Wash. Post (Oct. 8, 2015), *available at* https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[228] Order at 1, *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.* (*In re Warrant*), 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 13-MJ-2814), ECF No. 80.

[229] *In re Warrant*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014)

[230] Brief for Appellant, *In re Warrant*, No. 14-2985 (2d Cir. Dec. 8, 2014), ECF No. 47.

[231] Brief for the United States of America, *In re Warrant*, No. 14-2985 (2d. Cir. Mar. 9, 2015), ECF No. 212.

*The following Gibson Dunn lawyers assisted in preparing this client alert: Alexander H. Southwell, Debra Wong Yang, Sean Royall, Michael Li-Ming Wong, Joshua Jessen, Eric D. Vandevelde, Ryan T. Bergsieker, Michael Walther, Andres Font Galarza, Patrick Doris, Penny Madden, Kai Gesing, Sarah Wazen, Eryk L. Dziadykiewicz, Alejandro Guerrero Perez, Jeana Bisnar Maute, Priyanka Rajagopalan, Ashley Rogers, Danielle Serbin, Kamola Kobildjanova, Amy Chmielewski, Henry Pistell, Grace Tsou, Alex Murchison, Alexander Zbrozek, Michael C. Short, Mark Dittrich, Michael Adelman, Melissa Goldstein, Lindsey Young, Chanelle A. McCoy, Jennifer Bracht, Cary McClelland, Stephanie Silvano, Adam Yarian, Michelle Camp, Eugene Chao, and Timothy W. Loose.*

*Gibson, Dunn & Crutcher's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection Group:*

***United States***

*M. Sean Royall - Co-Chair, Dallas (+1 214-698-3256, sroyall@gibsondunn.com)*
*Alexander H. Southwell - Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)*
*Debra Wong Yang - Co-Chair, Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)*
*Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)*
*Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)*

*Shaalu Mehra - Palo Alto (+1 650-849-5282, smehra@gibsondunn.com)*
*Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)*
*Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)*
*Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)*
*Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)*
*Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)*

***Europe***
*James A. Cox - London (+44 207 071 4250, jacox@gibsondunn.com)*
*Andrés Font Galarza - Brussels (+32 2 554 7230, afontgalarza@gibsondunn.com)*
*Bernard Grinspan - Paris (+33 1 56 43 13 00, bgrinspan@gibsondunn.com)*
*Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)*
*Jean-Philippe Robé - Paris (+33 1 56 43 13 00, jrobe@gibsondunn.com)*
*Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)*
*Nicolas Autet - Paris (+33 1 56 43 13 00, nautet@gibsondunn.com)*
*Eryk L. Dziadykiewicz - Brussels (+32 2 554 72 03, edziadykiewicz@gibsondunn.com)*
*Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerreroperez@gibsondunn.com)*
*Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)*
*Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)*

***Asia***
*Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)*
*Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)*
*Robert S. Pé - Hong Kong (+852 2214 3768, rpe@gibsondunn.com)*

*Questions about SEC disclosure issues concerning data privacy and cybersecurity can also be addressed to the following leaders and members of the Securities Regulation and Corporate Disclosure Group:*

*James J. Moloney - Orange County, CA (+1 949-451-4343, jmoloney@gibsondunn.com)*
*Elizabeth Ising - Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com)*
*Lori Zyskowski - New York (+1 212-351-2309, lzyskowski@gibsondunn.com)*