Privacy Developments: Private Litigation, Enforcement Actions, Legislation, and Administrative Actions

By John Black and James Steel***

I. Introduction

In recent years, two principal areas of privacy-related legal exposure for businesses maintaining consumer personal information have been private litigation under the Telephone Consumer Protection Act ("TCPA")[1] and enforcement actions by the Federal Trade Commission ("FTC"). However, in the last year, other federal and state regulators have become more active in policing and enforcing privacy, and plaintiffs have enjoyed success in expanding the use of existing federal and state statutes to pursue privacy litigation. This survey reviews the key developments in these areas in the past year, including the highly publicized legal battle between the U.S. Department of Justice and Apple, Inc. over access to the encrypted iPhone used by one of the terrorists in the San Bernardino attacks.

II. Private Actions Under the TCPA

TCPA litigation continued apace in 2015, with 3,710 filed actions in state and federal court—a 45 percent increase over the number of filings in 2014.[2] Plaintiffs' firms continue to find the prospect of $500 to $1,500 in statutory damages an effective source of settlements and fee awards, while many companies, unwilling to forgo the potentially lucrative telemarketing opportunities, have continued to wrangle with an uncertain regulatory compliance landscape.

* John Black is a member of Skarzynski Black LLC in Chicago.

** James Steel is an sssociate at Skarzynski Black LLC in New York.

1. 47 U.S.C.A. § 227 (West 2014 & Supp. 2016); *see id.* § 227(b)(3) (providing for a private cause of action to recover actual monetary damages or $500 for each violation, whichever is greater, and empowering the court to increase the award, by no more than three times, if the defendant willfully or knowingly violated the statute or applicable regulations); *id.* § 227(c)(5) (same).

2. *See Out Like a Lion . . . Debt Collection Litigation & CFPB Complaint Statistics, Dec 2015 & Year in Review*, WebRecon, http://webrecon.com/out-like-a-lion-debt-collection-litigation-cfpb-complaint-statistics-dec-2015-year-in-review/ (last visited Sept. 6, 2016). Staff at WebRecon noted that the recent discovery of a PACER database that collected TCPA litigation "had a visible impact on the overall statistics." *Id.*

In May 2016, the U.S. Supreme Court handed down one of the most anticipated decisions concerning a plaintiff's ability to maintain a civil action under the TCPA. Unfortunately, rather than adding clarity to an area already fraught with uncertainty, the Court's decision appears destined to spawn further legal battles.

The Supreme Court's decision in *Spokeo, Inc. v. Robins*[3] clarified the requirements for Article III standing. Spokeo is a regulated "consumer reporting agency" under the Fair Credit Reporting Act ("FCRA"), operating a website that enables a user to input an individual's name, e-mail address, or phone number to conduct a broad search in a variety of databases to obtain information concerning the individual.[4] In *Spokeo*, the plaintiff alleged an unspecified individual had conducted a Spokeo search for information about him, and that the information Spokeo provided in response contained certain inaccuracies. Upon learning of the inaccurate information, he filed a class-action complaint, alleging Spokeo willfully violated the FCRA.[5]

Although the district court dismissed the lawsuit for lack of standing, the U.S. Court of Appeals for the Ninth Circuit reversed. The Supreme Court, in an opinion authored by Justice Alito, explained that, under existing case law, the "irreducible constitutional minimum" of standing requires three elements: (1) an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.[6]

Focusing on the injury-in-fact requirement, the Court noted the plaintiff bore the burden of establishing an injury that is both "concrete and particularized."[7] While the plaintiff had established the injury caused by Spokeo's delivery of inaccurate information was "particularized," as it affected the plaintiff in a personal way, the Ninth Circuit's analysis had failed to consider properly whether the injury was "concrete."[8] As Justice Alito noted, it is not enough that an injury be unique to an individual; the injury must also be "real" and not "abstract."[9] Thus, the Court drew a strong distinction between concreteness and particularization.

In considering whether an injury is concrete, the Court noted that it was not necessary to determine whether an injury resulted in tangible harm because intangible injuries may also be concrete.[10] While the Court was deferential to a congressional determination to "elevate" an intangible harm to the status of a legally cognizable injury, the Court made it clear that Congress could not grant Article III standing to plaintiffs by fiat.[11] Regardless of the congressional deter-

3. 136 S. Ct. 1540, 1545 (2016).
4. *Id.* at 1546 (citing 15 U.S.C. § 1681a(f)).
5. *Id.*
6. *Id.* at 1547.
7. *Id.* at 1548 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).
8. *Id.*
9. *Id.* (quoting Webster's Third New International Dictionary 472 (1971); Random House Dictionary of the English Language 305 (1967)).
10. *Id.* at 1549.
11. *Id.* (quoting *Lujan*, 504 U.S. at 578).

mination, Article III standing requires the existence of a concrete injury, even in the context of a statutory violation.[12]

The statutory context of the FCRA informed the Court that Congress "sought to curb the dissemination of false information."[13] However, an allegation of a mere violation of the FCRA's procedural requirements would not necessarily result in concrete harm. It was the plaintiff's obligation to allege the basis for concluding a concrete harm was suffered, and the Ninth Circuit's duty to evaluate the sufficiency of that allegation. Because the Ninth Circuit had failed to evaluate the injury for concreteness, its decision was reversed, and the Supreme Court remanded the case for further proceedings.

Spokeo has obvious implications for pleading sufficiency under the TCPA. According to the Court's logic, it is not enough to allege a technical violation of the TCPA—regardless of the congressional judgment as to the nature of the harm. Rather, to satisfy Article III's standing requirements, a plaintiff must also establish that the TCPA violation resulted in concrete harm to the plaintiff. In sum, the standing requirement of injury in fact is not obviated by a congressional determination as to the availability of statutory damages.

Not surprisingly, the battle lines on this issue have already begun to emerge. Ten days after the Supreme Court issued its *Spokeo* decision, Facebook filed a motion to dismiss a TCPA class action based, in part, on the Supreme Court's standing analysis in *Spokeo*.[14] In its motion, Facebook argued the plaintiff alleged only a statutory violation, consisting of text messages sent in violation of the TCPA, and failed to allege a concrete injury arising from his receipt of those messages.[15] While Facebook admitted the plaintiff had alleged that he "incurs charges for incoming messages," Facebook argued he failed to assert that he pays for each individual message or was otherwise charged more than he would have been.[16] According to Facebook, the allegations were therefore insufficient under *Spokeo*.

At least one court has already rejected the *Spokeo* standing argument in a TCPA lawsuit. In *Booth v. Appstack, Inc.*,[17] the court was satisfied that the plaintiffs had demonstrated a "concrete injury" in their TCPA claims. According to the *Booth* court, the plaintiffs alleged that the TCPA violations forced them to waste time answering or otherwise addressing widespread robocalls. The court noted that "[t]he use of the autodialer, which allegedly enabled Defendants to make massive amounts of calls at low cost and in a short period of time, amplifies the severity of this injury."[18] The court, therefore, was satisfied that the alleged injury was sufficient to confer Article III standing.[19]

12. *Id.*
13. *Id.* at 1550.
14. Facebook, Inc.'s Notice of Motion and Motion to Dismiss Plaintiff's First Amended Complaint and Memorandum in Support at 8–9, Duguid v. Facebook, Inc., No. 3:15-cv-00985-JST (N.D. Cal. May 26, 2016).
15. *Id.* at 9.
16. *Id.* (quoting First Amended Complaint).
17. No. C13-1533JLR, 2016 WL 3030256, at *5 (W.D. Wash. May 25, 2016).
18. *Id.*
19. *Id.*

The distinction between phone calls and text messages may be crucial. In an age of unlimited messaging plans, as Facebook argues, there may be little, if any, cognizable, concrete harm to a consumer who merely endures the occasional nuisance of a text message. Perhaps a sharp distinction will be drawn between the nuisance caused by a text message and an automated robocall, which may be an active area of inquiry for courts faced with TCPA lawsuits, as defendants seek to test the scope of permissible standing following *Spokeo*.

Many commentators expected the Court to draw a bright line limiting Article III standing. Following issuance of the opinion, some in the business community appealed to Congress for relief. With remarkable timing, the Senate Commerce Committee held a hearing on the efficacy of the TCPA two days after the Court's decision in *Spokeo*.[20] At the hearing, Senate Republicans pushed to ease TCPA restrictions and met sharp resistance from Democrats. Whether the hearing will result in action to amend the TCPA is an issue to watch in coming months.

III. FTC Privacy Enforcement Actions

The FTC has historically been one of the federal agencies most active in protecting consumer privacy. Under section 5 of the FTC Act, which declares unlawful "unfair or deceptive acts or practices in or affecting commerce,"[21] the FTC has often brought enforcement actions to address unfairness and deception in collecting, handling, and disposing of consumer personal information. As new technologies and issues have arisen, the FTC has also shifted the focus of its efforts. For example, in its January 2015 report, *Internet of Things: Privacy & Security in a Connected World*,[22] the FTC examined the applicability of Fair Information Practice Principles to smart devices underlying the Internet of Things ("IoT"), signaling its concern about the adequacy of consumer privacy protections associated with these devices. In the past year, the FTC brought two particularly notable privacy enforcement actions, which reflect the shifting focus of FTC enforcement efforts.

A. ASUSTeK Computer, Inc.

A year after releasing its *Internet of Things* report, the FTC brought an enforcement action against a Taiwan-based computer hardware maker for producing routers with critical security flaws that put at risk the home networks of consumers. According to the complaint in *In re ASUSTeK Computer, Inc.*,[23] the routers'

20. *The Telephone Consumer Protection Act at 25: Effects on Consumers and Business: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 114th Cong. (2016), http://www.commerce.senate.gov/public/index.cfm/2016/5/the-telephone-consumer-protection-act-at-25-effects-on-consumers-and-business.

21. Federal Trade Commission Act § 5(a)(1), 15 U.S.C. § 45(a)(1) (2012).

22. Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 19–46 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

23. Complaint, *In re* ASUSTeK Computer, Inc., No. 142-3156 (F.T.C. Feb. 23, 2016).

insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing sensitive personal information on the Internet. In February 2014, hackers used readily available tools to locate vulnerable ASUS routers and exploited these security flaws to gain unauthorized access to over 12,900 storage devices.

According to the complaint, the interfaces to the routers had numerous vulnerabilities, including using unencrypted means to transfer files and permitting the bypassing of authentication mechanisms and the remote retrieval of log-in credentials stored in clear text. The complaint alleged ASUS failed timely to fix these vulnerabilities or notify affected users. In addition, ASUS did not notify consumers about the availability of security updates, and often incorrectly informed consumers that their routers employed the most current firmware available. ASUS also marketed its routers as including security features that would "protect computers from any unauthorized access, hacking, and virus attacks" and "protect [the] local network against attacks from hackers."[24] ASUS's router also featured services that purportedly allowed a consumer to plug a USB drive into the router to create a secure "cloud" storage accessible from any device, although the services had serious security flaws.

The FTC and ASUS entered into a consent order requiring ASUS to establish a comprehensive security program, subject to independent audits for the next twenty years. In addition, the order requires ASUS to notify consumers of software updates and other steps they can take to protect themselves from security flaws, and prohibits ASUS from misleading consumers about the security of the company's products, including whether a product is using current software.[25]

B. Very Incognito Technologies, Inc.

The FTC also settled its first enforcement case under the new Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR"). The CBPR system, developed by participating APEC countries to build trust in cross-border transfers of personal information, requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework's nine information privacy principles and receive certification of compliance from an APEC-recognized accountability agent. The FTC's complaint in *In re Very Incognito Technologies, Inc.*[26] alleged that Vipvape, a maker of handheld vaporizers, violated section 5(a) of the FTC Act by falsely representing in its website privacy policy that it was certified to participate in the APEC CBPR system.

The FTC and Vipvape entered into a consent order prohibiting Vipvape and its personnel from misrepresenting its participation in any privacy or security

24. *Id.* at 2 & exh. A (quoting ASUS marketing materials).

25. Agreement Containing Consent Order, *In re* ASUSTeK Computer, Inc., No. 142-3156 (F.T.C. Feb. 23, 2016).

26. Complaint, *In re* Very Incognito Techs., Inc., No. C-4580 (F.T.C. June 21, 2016). Very Incognito Technologies, Inc. also does business as Vipvape. *Id.* at 1.

program.[27] The order requires Vipvape to provide a copy of the consent order to its personnel and also to maintain compliance records for twenty years.

IV. Privacy Enforcement Actions by Other Regulatory Bodies

Although regulators, such as the FTC and the Office for Civil Rights of the Department of Health and Human Services, have been active for several years in protecting personal information, other federal and state regulatory bodies have recently become more active in promoting privacy best practices and enforcing privacy laws and regulations. Below are some of the more notable enforcement actions in the last year.

A. *CFPB v. EZCORP, Inc.*

The Consumer Financial Protection Bureau ("CFPB"), under its authority to prevent unfair or deceptive practices in violation of the Consumer Financial Protection Act of 2010,[28] has become active in privacy enforcement. In December 2015, the CFPB entered into a consent order with EZCORP, Inc., a Texas payday/installment loan company, over deceptive and unfair business practices, including illegally disclosing the existence of the debt to third parties during collection visits to debtors' homes and places of employment. EZCorp also exposed consumers to fees through electronic withdrawal attempts, often making three attempts electronically to withdraw money from a consumer's bank account for a loan payment and making withdrawals earlier than promised. As a result, consumers incurred bank fees, which made it harder for them to climb out of debt when behind on payments. Under the consent order, EZCORP must refund $7.5 million to 93,000 consumers who made payments after illegal in-person collection visits or who paid fees to EZCORP or their banks because of unauthorized or excessive electronic withdrawal attempts. EZCORP must also cease both collecting or selling remaining payday and installment debt and illegal debt collection practices and pay a $3 million civil penalty to the CFPB Civil Penalty Fund.[29]

B. *In re* Cellco Partnership

In December 2015, the Federal Communications Commission ("FCC") entered into a consent decree with Cellco Partnership ("Verizon") to resolve its investigation into whether Verizon failed to disclose to consumers that it was inserting Unique Identifier Headers "(UIDH") (i.e., "supercookies") into their Internet traffic in violation of section 222 of the Communications Act and the FCC's Open Internet Transparency Rule on informed choice. The FCC found

27. *In re* Very Incognito Techs., Inc., No. C-4580, slip op. at 2 (F.T.C. June 21, 2016) (decision and order).

28. 12 U.S.C. §§ 5531, 5536 (2012).

29. *In re* EZCORP, Inc., No. 2015-CFPB-0031 (Dec. 15, 2015) (consent order).

that Verizon began inserting the UIDH into consumers' Internet traffic in December 2012, but did not disclose this practice until October 2014, and did not update its privacy policy until March 2015 to include information about the UIDH. The FCC also found that at least one of Verizon's advertising partners used the UIDH for unauthorized purposes to circumvent consumers' privacy choices by restoring deleted cookies, and that Verizon inserted the UIDH into the Internet traffic from mobile device lines that were not eligible to participate in Verizon's targeted advertising programs. The consent decree required payment of a $1,350,000 fine, disclosure, designation of a compliance officer to monitor compliance, and the implementation of a three-year compliance plan requiring Verizon to obtain customer opt-in consent prior to sharing the customer's UIDH with a third party to deliver targeted advertising.[30]

C. New York Attorney General's Settlement with Uber

In January 2016, the New York Attorney General announced a settlement with Uber over the Attorney General's investigation into Uber's collection, maintenance, and disclosure of rider personal information. The investigation arose from reports that Uber executives had access to rider locations and displayed this information in an aerial view, referred to internally as "God View." The settlement required Uber to adopt security practices to protect personal information, including encrypting rider geolocation information and adopting multifactor authentication before employees access sensitive personal information. The settlement also included a $20,000 penalty for failing to timely notify drivers and the Attorney General's Office of a data breach in September 2014.[31]

IV. Notable Privacy Litigation

A. Biometric Privacy Litigation

The Illinois Biometric Information Privacy Act ("BIPA")[32] was adopted in 2008, but recently has become the subject of class action litigation with at least six putative class action complaints having been filed since early 2015. Among its provisions, BIPA prohibits any private entity[33] from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric information or a biometric identifier, defined as "a retina or iris

30. *In re* Cellco P'ship, No. DA 16-242 (F.C.C. Mar. 7, 2016) (order). Cellco Partnership does business as Verizon Wireless. *Id.* at 1.

31. Press Release, N.Y. St. Office of the Att'y Gen., A.G. Schneiderman Announces Settlement with Uber to Enhance Rider Privacy (Jan. 6, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy.

32. 740 Ill. Comp. Stat. Ann. 14/1 *et seq.* (West 2014).

33. "Private entity" is defined as an "individual, partnership, corporation, limited liability company, association, or other group," but not a state or local government agency, court, judge, or court clerk. *Id.* § 10.

scan, fingerprint, voiceprint, or scan of hand or face geometry,"[34] without first informing the person in writing that biometric information or a biometric identifier is being collected or stored and the specific purpose and length of time for which it is being collected, stored, and used, and obtaining a valid written release.[35] Under BIPA, a prevailing plaintiff can recover actual damages or liquidated damages of $1,000 to $5,000 per violation, as well as attorney's fees and costs,[36] which may have spurred the interest of plaintiffs' attorneys in pursuing lawsuits for alleged violations of the Act. Only Texas has a similar biometric information statute,[37] although other states have considered similar legislation.[38]

Putative class actions have been brought under BIPA against Shutterfly and Facebook, among others,[39] for collecting the facial features of non-website users from photos uploaded by users without first obtaining appropriate consent. Several of these cases recently were the subject of court decisions concerning whether the cases should continue.

In *Norberg v. Shutterfly, Inc.*,[40] the U.S. District Court for the Northern District of Illinois denied a motion to dismiss a complaint against the photo-sharing website for collecting biometrics of non-users from photos in which they appear. Shutterfly argued BIPA does not regulate "biometric identifiers, [such as] hand or face geometry, derived from photographs,"[41] because photographs are specifically excluded as a biometric identifier under BIPA, but the court rejected this argument. Noting that a "scan of hand or face geometry" is a biometric identifier under BIPA and that protected biometric information includes "information . . . based on an individual's biometric identifier," the court drew a distinction between a photograph and a facial pattern derived from a scanned photograph.[42] Based on the plaintiff's allegation that he did not use the defendant's website, did not agree to its privacy policy, and did not upload his facial image (which was taken from a photo uploaded by a website user), the court denied the motion to dismiss.[43]

In *In re Facebook Biometric Information Privacy Litigation*,[44] the U.S. District Court for the Northern District of California denied Facebook's motion for summary judgment. Facebook argued that the plaintiffs had agreed to its terms of

34. *Id.* "Biometric information" means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

35. *Id.* § 15(b).

36. *Id.* § 20.

37. Tex. Bus. & Com. Code Ann. § 503.001 (West 2015).

38. *See* Justin Lee, *States Considering Biometrics Capture Laws May Look to Illinois Privacy Laws*, Biometric Update (Aug. 5, 2015), www.biometricupdate.com/201508/states-considering-biometrics-capture-laws-may-look-to-illinois-privacy-laws.

39. *See* Class Action Complaint at 1–3, Rivera v. Google, Inc., No. 1:16-cv-02714 (N.D. Ill. Mar. 1, 2016) (alleging a similar suit against Google over Google Photos).

40. 152 F. Supp. 3d 1103 (N.D. Ill. 2015).

41. *Id.* at 1105.

42. *Id.* at 1106 (quoting 740 Ill. Comp. Stat Ann. 14/10 (West 2014)).

43. *Id.*

44. No. 15-cv-03747-JD, 2016 WL 2593853 (N.D. Cal. May 5, 2016).

use, including a clause designating California as the applicable law for disputes, which rendered inapplicable the Illinois statute. The court applied California choice-of-law rules, according to which the contractual designation of governing law would apply unless that law is contrary to a "fundamental policy" of another state and the latter state has "a materially greater interest" in the matter than the former state.[45] The court held that those two conditions were met, and that BIPA was therefore applicable. The court also rejected Facebook's argument that BIPA's exclusion of photographs from "biometric information" should encompass all information drawn from photographs, such as facial geometry from scanned photos, noting that Facebook's reading would undercut the statutory intent to address emerging biometric technology and that BIPA's exclusion of photographs is better understood as meaning paper prints of photographs.[46]

B. *Yershov v. Gannett Satellite Information Network, Inc.*

In *Yershov v. Gannett Satellite Information Network, Inc.*,[47] the U.S. Court of Appeals for the First Circuit reversed a district court's dismissal of a putative class action lawsuit against Gannett Satellite Information Network, Inc. ("Gannett"), which publishes *USA Today*, for allegedly disclosing information about the plaintiff to a third party in violation of the Video Privacy Protection Act of 1988.[48] The district court determined that Gannett had disclosed "personally identifiable information," but held that the plaintiff was not a "renter, purchaser, or subscriber" of Gannett video content and therefore was not protected under the Act.[49] The plaintiff, Alexander Yershov, was a mobile phone user who had signed up to use Gannett's *USA Today* app, by which he watched video clips. Gannett would send the video title, phone identifier, and geolocation data concerning Yershov to a third party analytics company whenever Yershov downloaded a video. However, Gannett failed to obtain Yershov's consent to share his personally identifiable information. The First Circuit determined that Yershov was a "subscriber" under the Act, even if he was not a paying customer, because he provided consideration for the app's service in the form of his phone ID and geolocation information.[50]

C. *United States v. Apple, Inc.*

In a widely publicized case that raised intriguing issues concerning the conflict between physical security and privacy, the U.S. Attorney for the Central District of California obtained an order compelling Apple, Inc. to assist in decrypting an Apple iPhone used by a terrorist involved in the San Bernardino attacks on

45. *Id.* at *9 (quoting Wash. Mut. Bank, FA v. Super. Ct., 15 P.3d 1071, 1079 (Cal. 2001)).
46. *Id.* at *12.
47. 820 F.3d 482 (1st Cir. 2016).
48. 18 U.S.C.A. § 2710 (West 2015).
49. *Yershov*, 820 F.3d at 485 (quoting 18 U.S.C.A. § 2710(a)(1), (3) (defining "consumer" to mean "any renter, purchaser, or subscriber . . ." and also defining "personally identifiable information")).
50. *Id.* at 487–89.

December 2, 2015. The phone had been seized pursuant to a warrant executed the day after the attacks. Apple had refused to voluntarily decrypt the phone, even though the government identified Apple as the only party with the technical means to do so. The owner of the phone, the terrorist's employer, had consented to the search and to Apple providing decryption assistance. The government feared that attempting to crack the code would trigger the phone's auto-erase function and requested that Apple write code that would operate only for that phone to disable the auto-erase function.[51]

The government proceeded under the All Writs Act, "a residual source of authority to issue writs that are not otherwise covered by statute."[52] The government contended that Apple would not be unreasonably burdened and that Apple's assistance was necessary to effectuate the warrant. In response, Apple filed a motion to vacate, which was followed by further motions on both sides. However, the government eventually found a third party that was able to provide access and so advised the court, which led to the court vacating the order on March 29, 2016.[53]

V. Notable Developments in Privacy Legislation and Regulation

A. USA Freedom Act

The USA Freedom Act of 2015,[54] enacted in response to the Edward Snowden revelations, extends provisions of the USA Patriot Act that had expired and imposes limits on the bulk collection of telecommunication metadata on U.S. citizens by U.S. intelligence agencies.[55] The Act was adopted after active debate in the House and Senate over a two-year period, with the substantial involvement of human rights, national security, and business and trade groups. Among the key issues addressed in the Act are bulk collection, pen registers, and trap and trace devices; the FISA Court;[56] and disclosure requirements.

51. Government's Motion to Compel Apple Inc. to Comply with This Court's Feb. 16, 2016 Order Compelling Assistance in Search at 1–7, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 19, 2016).

52. Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

53. *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP, slip op. at 1 (C.D. Cal. Mar. 29, 2016) (vacating order of Feb. 16, 2016).

54. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (to be codified in scattered sections of the U.S.C.).

55. The USA Freedom Act extends the Patriot Act until December 15, 2019. *Id.* § 704, 50 U.S.C.A. § 1805 note (West 2015 & Supp. 2016).

56. The FISA Court, a U.S. federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978, addresses applications submitted by the U.S. government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. *See About the Foreign Intelligence Surveillance Court*, U.S. Foreign Intelligence Surveillance Ct., www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited Sept. 21, 2016).

Title I bans bulk collection under section 215 of the USA Patriot Act,[57] requiring the government to apply for call detail records from electronic communication service or remote computing service providers based on a "specific selection term" identifying "a person, account, address, or personal device" to limit "the scope of information sought."[58] It permits the government to apply for records that are within one or two degrees of separation from the suspect. The government may apply for an initial set of call records from the providers if the government (1) states "reasonable grounds to believe that the call detail records sought to be produced based on [a] specific selection term . . . are relevant to [an authorized] investigation,"[59] and (2) has "a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor."[60] This first set of selection terms may then be sent as query requests to providers to obtain a second set of call records, but the government must first apply for the second set of records by specifying "session-identifying information or a telephone calling card number identified by the specific selection term"[61] used to produce call detail records within the first set. As a safeguard, the government is required to "adopt minimization procedures" calling for "the prompt destruction of all call detail records" determined not to be "foreign intelligence information."[62] In addition, the FISA Court may impose "additional, particularized minimization procedures" for any "nonpublicly available information concerning unconsenting United States persons."[63] Also, pen registers and trap and trace devices are banned per Title II, unless obtained by an application based on a "specific selection term."[64] The effect of these amendments is to require the government to apply to the FISA Court for specific individual call detail records for surveillance, rather than to obtain such metadata on bulk basis.

Reforms of the FISA Court are addressed in Title IV, one of which is the appointment of amici curiae to assist the FISA Court on a limited basis, such as providing "legal arguments or information regarding . . . area[s] relevant to the issue presented to the court," if the FISA Court desires assistance in cases involving novel or significant legal interpretations.[65] Limited appellate review of FISA Court decisions is permitted by both the FISA Court of Review and the U.S. Supreme Court.[66] Title IV also requires the Director of National Intelligence

57. 50 U.S.C.A. § 1861 (West 2015 & Supp. 2016).
58. *Id.* § 1841(4)(A).
59. *Id.* § 1861(b)(2)(C)(i).
60. *Id.* § 1861(b)(2)(C)(ii).
61. *Id.* § 1861(c)(2)(F)(iv).
62. *Id.* § 1861(c)(2)(F)(vii)(I); *see id.* § 1861(c)(2)(F)(vii)(II) (requiring the destruction of such records).
63. *Id.* § 1861(g)(3).
64. *Id.* § 1842(c)(3).
65. *Id.* § 1803(i)(4)(C).
66. *Id.* § 1803(b). The FISA Court of Review is composed of three federal judges designated by the Chief Justice. *Id.*; *see id.* § 1871(e)(2).

to perform a declassification review of any opinion by the FISA Court or the FISA Court of Review that includes a "significant construction or interpretation of any provision of law" and, following such declassification review, make certain parts of any such opinion publicly available.[67] The effect of these amendments is to provide additional support to assist the FISA Court in addressing novel or significant legal issues and to expand the opportunity for appellate review of FISA Court decisions.

Title VI prescribes additional disclosure about applications to and orders issued by the FISA Courts. Under sections 601 and 602, the U.S. Attorney General must disclose to specified congressional committees specific information about FISA Court activity, including the number of orders sought and received, estimates of the number of people targeted and affected by surveillance, and the number of appointments of amici curiae.[68]

Title VII addresses the targeting of non-United States persons, creating an emergency exception as to non-United States persons lawfully targeted and located outside the United States who suddenly appear in the United States. Those persons may be targeted for a brief period after they appear in the United States, provided "a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person."[69]

B. FAST Act

The FAST Act,[70] which was enacted to improve the country's transportation infrastructure, contains four notable privacy-related provisions. First, the Act modifies annual privacy notice requirements under the Gramm-Leach-Bliley Act, providing an exception if a financial institution does not share nonpublic personal information with non-affiliated third parties (other than as permitted under certain enumerated exceptions) and its policies and practices for disclosing nonpublic personal information did not change since its last distribution of its policies and practices to customers.[71] Also, any investment advisers and private funds that meet these criteria need not provide annual privacy notices.[72] Second, the act directs the Department of Energy to address the cybersecurity of electricity and defense electricity critical infrastructure.[73] Third, the act includes the Driver Privacy Act, which provides that data on a data event recorder in a vehicle belongs either to the vehicle's owner or lessee and cannot be accessed without consent, except under limited circumstances.[74] Fourth, the Act provides funding for intelligent transportation systems to "assist in

67. *Id.* § 1872.
68. *See id.* §§ 1862, 1871, 1881f.
69. *Id.* § 1805(f)(1)(A).
70. Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 Stat. 1312 (2015) (to be codified in scattered sections of the U.S.C.) [hereinafter FAST Act].
71. *Id.* § 75001, 15 U.S.C.A. § 6803(f) (West 2009 & Supp. 2016).
72. *See id.*
73. *Id.* § 61003, 16 U.S.C.A. § 824o-1 (West Supp. 2016).
74. *Id.* § 24302, 49 U.S.C.A. § 30101 note (West 2016).

the development of cybersecurity research . . . to help prevent hacking, spoofing, and disruption of connected and automated transportation vehicles,"[75] and directs that a report be created on how the IoT may improve transportation services, including a discussion of IoT security and privacy.[76]

C. FCC Proposed Privacy Rules for ISPs

In April 2016, the FCC released a notice of proposed rulemaking regarding the privacy of broadband users and the related requirements for Internet service providers ("ISPs").[77] The notice proposes to protect consumer privacy through greater transparency in the ISPs' privacy policies concerning disclosures of practices for collecting and sharing personal information, heightened protections for financial information or geolocation data, choice, and data security applied to customer proprietary information.[78] Data breach notifications would also be required.[79] The rulemaking would protect customer proprietary network information, including geolocation information, MAC and IP addresses, and personally identifiable information that ISPs acquire from customers.[80] To address security, all providers would be required to establish and perform regular risk management assessments and promptly address any weaknesses identified, train employees, contractors, and affiliates that handle customer personal information, appoint a senior manager to oversee security, establish and use robust customer authentication procedures, and take responsibility for the use of customer personal information by third parties with whom the information is shared.[81]

75. *Id.* § 6006, 23 U.S.C.A. § 514(b)(10) (West 2014 & Supp. 2016).

76. *Id.* § 3024.

77. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 23360 (proposed Apr. 20, 2016) (to be codified at 47 C.F.R. pt. 64).

78. *Id.* at 23408–10 (to be codified 47 C.F.R. §§ 64.7001–64.7005).

79. *Id.* at 23410–11 (to be codified at 47 C.F.R. § 64.7006) (addressing broadband internet access service providers (BIAS)); *see also id.* at 23407–08 (to be codified at 47 C.F.R. § 64.2011) (addressing telecommunications carriers).

80. *Id.* at 23408 (to be codified at 47 C.F.R. § 64.7000) (defining "customer proprietary information" or "customer PI"); *see also id.* at 23363–64 (seeking comment on proposal to interpret CPNI with respect to BIAS as including MAC (Media Access Control) and IP (Internet Protocol) addresses).

81. *Id.* at 23410 (to be codified at 47 C.F.R. § 64.7005); *see also id.* at 23386 (seeking comment on how to ensure security, confidentiality, and integrity of customer personal information once a BIAS provider shares it with a third party).