Privacy Developments: Private Litigation, Enforcement Actions, and Settlements

By John Black and James R. Steel***

I. Introduction

Over the last year there have been several record-setting settlements in privacy-related litigation. Privacy litigation has continued apace, while the Federal Trade Commission ("FTC") has sought to expand its enforcement role. Unsurprisingly, privacy compliance remains a fast-developing area of the law with significant traps for unwary businesses. This survey reviews some of the key developments in these areas over the past year.

II. Developments in Article III Standing

Last year's review discussed the U.S. Supreme Court's May 2016 decision in *Spokeo, Inc. v. Robins*,[1] which sought to clarify the requirements of Article III standing where plaintiffs allege they were harmed by statutory violations. In *Spokeo*, the Supreme Court reinforced the concrete injury-in-fact requirement for Article III standing, holding that an allegation of a "bare procedural violation" was not sufficient to allege the concrete injury required for Article III standing. The Court acknowledged that a concrete injury may be either tangible or intangible, but, according to the Court, the crucial element is an allegation of either the existence or the risk of actual harm.

The following discussion surveys some recent federal court decisions applying the guidance set forth in *Spokeo*.

A. Standing Under the FCRA

There have been a large number of cases dealing with standing issues in the context of Fair Credit Reporting Act ("FCRA") claims. Indeed, the FCRA was a very active area of litigation in 2016 with a reported 3,960 total filings in state

* Principal, Skarzynski Black, LLC.
** Associate, Skarzynski Black, LLC.
1. 136 S. Ct. 1540 (2016).

and federal court.[2] From the reported decisions in the area, a few trends in *Spokeo* standing challenges have emerged.

For instance, in *Thomas v. FTS USA, LLC*,[3] plaintiff brought a proposed class action against his employer under the FCRA, alleging that the defendants "did not provide Plaintiff with a written disclosure that they intended to obtain a copy of his consumer report for employment purposes," and that "Plaintiff did not provide Defendants with his written authorization for them to obtain his consumer report for employment purposes."[4] In examining the claims, the court noted that "Congress may create a legally cognizable right to information, the deprivation of which will constitute a concrete injury." The court held that the plaintiff alleged such an informational injury through his allegation that he "received a disclosure that does not satisfy" the clear-and-conspicuous notice requirements of the FCRA.[5] The court, therefore, allowed the case to proceed.

Relatedly, in *In re Horizon Healthcare Services Inc. Data Breach Litigation*,[6] plaintiffs brought suit against Horizon Healthcare Services, Inc. ("Horizon") following the theft of two laptops containing sensitive personal information. Four plaintiffs brought suit on behalf of themselves and other Horizon customers whose personal information was stored on the laptops, alleging willful and negligent violations of the FCRA. The district court dismissed the case for lack of standing. On appeal, the Third Circuit, addressing the standing issue, noted that plaintiffs did not allege "a mere technical or procedural violation of FCRA."[7] Rather, they challenged "the unauthorized dissemination of their own private information."[8] According to the court, this "*de facto* injury" satisfied the concreteness requirement for Article III standing.[9] Accordingly, the Third Circuit reinstated the plaintiffs' claims.

In other circumstances, the courts have required clear allegations of actual, particularized harm to satisfy standing requirements. For example, in *Moody v. Ascenda USA Inc.*,[10] the plaintiff contended that the defendant, a credit reporting agency, violated the FCRA by providing her employer with a credit report that contained false information concerning prior drug and theft convictions, resulting in her suspension from work. Plaintiff alleged that she lost "hundreds of dollars" which she never recovered.[11] In light of the allegations of concrete harm, the court concluded that the plaintiff had articulated an individualized basis for standing.[12]

2. *See 2016 Year in Review: FDCPA Down, FCRA & TCPA Up*, WebRecon (Jan. 24, 2017), http://webrecon.com/2016-year-in-review-fdcpa-down-fcra-tcpa-up/.
3. 193 F. Supp. 3d 623 (E.D. Va. 2016).
4. *Id.* at 634.
5. *Id.* at 635.
6. 846 F.3d 625 (3d Cir. 2017).
7. *Id.* at 640.
8. *Id.*
9. *Id.*
10. 193 F. Supp. 3d 1347, 1349 (S.D. 2016).
11. *Id.*
12. *Id.* at 1352.

But, where allegations of specific, concrete harm are absent, FCRA claims may fail. One such case is *Bultemeyer v. CenturyLink, Inc.*,[13] where the U.S. District Court for the District of Arizona held that a plaintiff lacked Article III standing to bring a lawsuit challenging CenturyLink's acquisition of consumer reports under the FCRA. Here, plaintiff alleged that CenturyLink obtained consumer credit reports of visitors to its website in an effort to assess whether the individual was eligible for high-speed Internet service packages. The court concluded that, even assuming CenturyLink had violated the FCRA by "running her credit report without a permissible business purpose," the plaintiff had still failed to identify a concrete injury.[14] According to the court, the plaintiff was required to specifically allege what CenturyLink had done with the information from the credit report that resulted in actual harm.[15] Because the plaintiff failed to identify any such harm, the case was dismissed for lack of standing.

Likewise, in *Dilday v. DirecTV, LLC*,[16] DirecTV allegedly obtained consumer credit reports in violation of the FCRA. The court noted however that the plaintiff "conspicuously omits any factual allegation regarding why DIRECTV obtained his credit report or how DIRECTV allegedly used it."[17] Here, the court similarly found that the plaintiff failed to allege any particularized harm resulting from the disclosure. The court noted that the plaintiff, when confronted with the court's concerns as to the Article III standing requirements under *Spokeo*, "neither took steps to defend the sufficiency of his factual allegations nor attempted to file an amended complaint bolstering his position."[18] The court therefore found that plaintiff had alleged only a "bare statutory violation" and dismissed the case for lack of standing.[19]

From these cases, some patterns are emerging. First, the actual unauthorized dissemination of personal information may be a *de facto* injury, as the court found in *Horizon*. In the employment context, as in *Thomas*, companies that violate the notice requirement may also be found to have committed an informational injury. In both contexts, procedural violations may rise to the level of an actual injury sufficient to satisfy Article III standing under *Spokeo*. Moreover, as in *Moody,* plaintiffs can demonstrate an actual, concrete injury by pointing to specific, adverse employment consequences flowing from the use of an improperly obtained credit report.

Where, however, the case arises from the alleged acquisition or use of a consumer credit report without a permissible purpose, plaintiffs may be held to a higher standard. As demonstrated by the decisions in *Bultemeyer* and *Dilday*, courts appear to be more skeptical of such claims, requiring plaintiffs to articulate the actual injuries flowing from the procedural violations of the FCRA. In

13. No. CV-14-02530-PHX-SPL, 2017 WL 634516 (D. Ariz. Feb. 15, 2017).
14. *Id.* at *3.
15. *Id.* at *4.
16. No. 3:16CV996-HEH, 2017 WL 1190916 (E.D. Va. Mar. 29, 2017).
17. *Id.* at *1.
18. *Id.*
19. *Id.* at *5.

practice, plaintiffs seem to face the challenge of demonstrating not only that their credit reports were obtained without a permissible purpose, but also what specifically the defendant did with the information that caused a perceptible harm to the plaintiff. Absent such allegations of actual harm, courts seem inclined to dismiss "permissible purpose" FCRA claims under the *Spokeo* guidance.

B. Standing Under the TCPA

Litigation under the Telephone Consumer Protection Act ("TCPA") mushroomed in 2016, with 4,860 filed actions in state and federal court.[20] The total filings represented a 31.8 percent increase over 2015, which was itself a 20.8 percent increase over the number of filings in 2014.[21] TCPA litigation has resulted in further guidance as to the standing requirements in the wake of *Spokeo*.

In *Rogers v. Capital One Bank*,[22] the plaintiffs alleged that defendant used an automated telephone dialer to make unsolicited phone calls to plaintiffs in violation of the TCPA. The court held that the plaintiffs had alleged a particularized and concrete injury by asserting that the "their cell phone lines were unavailable for legitimate use during the unwanted calls."[23]

Similarly, in *Johnson v. American Education Services*,[24] the plaintiff contended that she had suffered "emotional and mental pain and anguish" due to her receipt of numerous debt collection phone calls from the defendant that were made in violation of the TCPA.[25] In evaluating the standing issue, the court noted that the allegations of emotional distress were sufficient to confer standing.[26]

If these decisions evidence a trend, it appears that standing challenges in typical TCPA litigation are unlikely to be successful. Between the impact on the use of a telephone line from an unwanted call and the availability of an emotional distress injury as sufficient to confer standing, it would appear that the standing would not prove to be a significant barrier to successful litigation.

C. Standing in Data Breach Litigation

Finally, challenges to standing in data breach litigation have also provided some helpful guidance as to the contours of the post-*Spokeo* standing requirements.

In *Galaria v. Nationwide Mutual Insurance Co.*,[27] the Sixth Circuit considered a standing challenge to claims brought against Nationwide in connection with a network data breach. In October 2012, Nationwide suffered a computer network breach that exposed the personal information of approximately 1.1 million individuals. Plaintiffs whose information had been exposed brought class actions al-

20. *See 2016 Year in Review: FDCPA Down, FCRA & TCPA Up*, *supra* note 2.
21. *Id.*
22. 190 F. Supp. 3d 1144 (N.D. Ga. 2016).
23. *Id.* at 1147.
24. No. 3:16-CV-00710-CRS, 2017 WL 938325 (W.D. Ky. Mar. 9, 2017).
25. *Id.* at *3.
26. *Id.*
27. 663 F. App'x 384 (6th Cir. 2016).

leging claims of negligence, invasion of privacy by public disclosure of private facts, bailment, and violation of the FCRA. In addressing the Article III standing issues, the Sixth Circuit noted that the plaintiffs asserted that the "theft of their personal data places them at a continuing, increased risk of fraud and identity theft."[28] According to the court, "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."[29] The court also held that plaintiffs' expenditures in the wake of the data breach to protect themselves from the risk of identity theft and fraud were cognizable injuries inasmuch as the expenditures were made "to mitigate an imminent harm."[30]

The Fourth Circuit, however, reached a different conclusion in *Beck v. McDonald*.[31] In *Beck*, the court considered whether plaintiffs had standing to pursue claims for violation of the Privacy Act of 1974 and the Administrative Procedure Act in connection with thefts of a laptop computer and physical medical records from the Veterans Affairs Medical Center in Columbia, South Carolina. The Fourth Circuit held that in this case the risk of identity theft was too attenuated.[32] Critical to the court's determination was the nature of the breach. The court distinguished *Galaria* on the ground that the circumstances in *Beck* did not involve a targeted data breach meant to obtain the plaintiffs' personal information because there was no indication the stolen items (i.e., the laptop and the medical records) were targeted "for the personal information they contained."[33] Given the lack of any indication that there had been identity theft arising from the data breach, or that the information was targeted for the purposes of attempted identity theft, the court was unwilling to find a concrete and particularized injury sufficient to support Article III standing.[34]

III. FTC Enforcement Actions

The FTC has continued aggressive enforcement in cases involving consumer privacy issues. However, a pending Eleventh Circuit case may affect the scope of the FTC's authority.

A. Eleventh Circuit Considers FTC Enforcement Authority in *LabMD*

In *LabMD Inc. v. FTC*,[35] the Eleventh Circuit is currently considering the scope of the FTC's authority to police privacy and data security issues. This case arises from an investigation into LabMD's data security practices that began in 2010.

28. *Id.* at 388.
29. *Id.*
30. *Id.* at 389.
31. 848 F.3d 262 (4th Cir. 2017).
32. *Id.* at 266.
33. *Id.* at 275.
34. *Id.* at 276.
35. 678 F. App'x 816 (11th Cir. 2016).

The investigation centered on evidence that a billing manager at LabMD installed a peer-to-peer file sharing program on her computer that exposed a document containing "sensitive personal information for roughly 9,300 patients, including their names, birthdates, and Social Security numbers."[36] Given that the file was accessible on the file-sharing network, it could have been downloaded by anyone. However, the only evidence of an actual download of the file was that a data security company obtained the file via the file-sharing network and then sought to offer its data security services to LabMD. When LabMD refused to purchase the services, the data security firm notified the FTC of the breach.

After finding that LabMD had acted in violation of the FTC Act and that this failure caused (or was likely to cause) substantial consumer injury, the FTC ordered LabMD to adopt various compliance measures, "including creating a comprehensive information security program; undergoing professional routine assessments of that program; providing notice to any possible affected individual and health insurance company; and setting up a toll-free hotline for any affected individual to call."[37] LabMD determined that the FTC's compliance regimen was too onerous and ceased operations in January 2014.

Thereafter, LabMD sought a stay of the FTC's order pending appeal. In considering LabMD's request, the Eleventh Circuit held that LabMD had raised a "serious legal question" about whether the FTC's interpretation of its enforcement powers was reasonable.[38] Specifically, the Eleventh Circuit determined it was not clear that the FTC's enforcement powers extended to harm that was "purely conceptual" or speculative.[39] The court of appeals appeared troubled that there was no evidence that the file had been downloaded by anyone but a data security firm that was only attempting to use the file to sell its data security service, which was not a privacy harm to any individual.[40]

The Eleventh Circuit, therefore, granted the stay. The case is currently pending before the Eleventh Circuit, and may provide some interesting guidance as to the scope of the FTC's enforcement powers later this year.

B. FTC Enforcement Proceeding for Deceptive Privacy Policy

The FTC has continued to be active in seeking to hold companies to the statements in their privacy policies. The consent decision and order in *In re Turn Inc.*[41] provides a recent example of the FTC's focus in this area as the business use of technology increases in sophistication.

Turn, Inc. operates an advertising platform enabling targeted digital advertisements to consumers. Turn's privacy policy informed customers that Turn used

36. *Id.* at 818.
37. *Id.* at 819.
38. *Id.* at 822.
39. *Id.* at 821.
40. *Id.* at 819.
41. No. C-4612 (F.T.C. Apr. 6, 2017).

two types of tracking technologies: cookies[42] and web beacons.[43] However, Turn also participated in a Verizon Wireless program that enabled the injection of tracking headers into its users' mobile Internet traffic.[44] Verizon users had no means of preventing the header injection, allowing Turn to avoid any attempt by Verizon users to limit Turn's tracking of their mobile Internet traffic.

The FTC alleged that Turn's failure to convey this information concerning the Verizon program to its users in its privacy policy resulted in misrepresentations about the users' ability to stop the tracking by blocking cookies or stop tailored advertising on mobile applications by opting out on Turn's opt-out page.[45] The FTC's consent order bars Turn from misrepresenting the extent of its online tracking or the ability of users to limit or control the company's use of their data, and requires Turn to engage in continued compliance monitoring and reporting.[46]

C. FTC Enforcement Proceeding for Deceptive Geotracking

The FTC also recently settled a case against InMobi Pte Ltd.,[47] a Singapore-based advertising company, over charges that, to develop geotargeted advertising, InMobi deceptively tracked the locations of hundreds of millions of consumers—including children—without their knowledge or consent.

The FTC alleged that InMobi mispresented that its advertising software would only track consumers' locations and serve geotargeted advertisements on an opt-in basis, using the location services of the consumer's mobile phone.[48] The FTC accused InMobi of tracking consumer locations regardless of whether the apps using InMobi's software sought such opt-ins, or even in some cases where the consumers had expressly denied the apps access to their location data, using information derived from the Wi-Fi networks in the consumer's vicinity.[49]

The FTC also alleged that InMobi violated the Children's Online Privacy Protection Act ("COPPA") by collecting this information from apps that were clearly directed at children without first obtaining parental consent.[50]

Under the terms of its settlement with the FTC, InMobi is subject to a $4 million civil penalty, which is suspended to $950,000 based on the company's financial condition. In addition, the company will be required to delete all information it collected from children and is prohibited from further violations of COPPA.[51]

42. "Cookies" are text files stored in a consumer's browser that allow a company to recognize that consumer when the consumer's browser makes a connection to the company's servers.

43. "Web beacons" are embedded codes in web pages that instruct the browser to connect to third-party servers.

44. Complaint at para. 8, *In re* Turn Inc., No. C-4612 (F.T.C. Apr. 6, 2017).

45. *Id.* at paras. 16–20.

46. *In re* Turn, Inc., No. C-4612, slip op. at 3–4 (F.T.C. Apr. 6, 2017) (decision and order).

47. Complaint, United States v. InMobi, No. 3:16-CV-3474 (N.D. Cal. June 22, 2016).

48. *Id.* at paras. 34–35.

49. *Id.* at paras. 51–54.

50. *Id.* at paras. 57–60.

51. Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. InMobi, No. 3:16-CV-3474 (N.D. Cal. June 27, 2016).

IV. A Series of Record Setting Privacy Settlements and Verdicts

While still only halfway over, the year 2017 has already been a banner year for claimants in privacy-related litigation.

On June 23, 2017, Anthem, Inc. announced that it had agreed to pay $115 million to settle consumer claims over a 2015 data breach that compromised the personal data of 78.8 million individuals.[52] This is the largest proposed data breach settlement in history. The compromise was reportedly the result of a mediator's proposal after a lengthy mediation process.[53] At the time of this writing approval is still pending before the U.S. District Court.

Target Corporation set the first benchmark for a global data breach settlement with state attorneys general. Target, of course, was the subject of a widely reported consumer credit card data breach in 2013 that exposed the information of 40 million customers. The data breach resulted in a variety of consumer and financial-institution class action lawsuits.[54] The breach also resulted in investigations by most states' attorneys general into Target's data security practices. Those investigations culminated earlier this year in an $18.5 million settlement with forty-seven states and the District of Columbia over Target's mishandling of consumer data.[55]

More recently, Nationwide Mutual Insurance Company reached a settlement with thirty-three states' attorneys general of an investigation concerning an October 2012 data breach, which exposed the personal information of 1.27 million customers.[56] The lost data included Social Security numbers, driver's license numbers, credit scoring information, and other personal data initially collected to provide insurance quotes to consumers applying for Nationwide insurance plans—many of whom did not ultimately become insured by the company. In addition to agreeing to improve its data security, Nationwide agreed pay a total of $5.5 million.[57] The Anthem, Target, and Nationwide settlements provide some insight into the costs of settling both ongoing and future data breach related investigations.

TCPA litigation also hit a high-water mark with the largest TCPA damages jury award in history. Earlier this year, a jury awarded $280 million against Dish Net-

52. Joint Administrative Motion to File Under Seal Portions of Plaintiffs' Memorandum in Support of Motion for Preliminary Approval of Class Action Settlement and Exhibits to Settlement Agreement, *In re* Anthem, Inc. Data Breach Litig., No. 5:15-MD-2617 (N.D. Cal. June 23, 2017), ECF No. 869.

53. *See id.*

54. *See*, *e.g.*, *In re* Target Corp. Consumer Data Sec. Breach Litig., MDL No. 14-2522, 2017 WL 2178306 (D. Minn. May 17, 2017) (certifying plaintiff class).

55. *See* Press Release, N.Y. State Att'y Gen., A.G. Schneiderman Announces $18.5 Million Multi-State Settlement with Target Corporation Over 2013 Data Breach (May 23, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.

56. *See* Press Release, N.Y. State Att'y Gen., A.G. Schneiderman Announces $5.5 Million Multi-State Settlement with Nationwide Mutual Insurance Company Over 2012 Data Breach (Aug. 9, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-55-million-multi-state-settlement-nationwide-mutual.

57. *Id.*

work ("Dish") for violations of the TCPA.[58] The suit was brought by the federal government and the states of California, Illinois, North Carolina, and Ohio, alleging "millions and millions" of individual violations of the TCPA.[59] Dish sought and was granted a stay of the judgment pending its appeal of the verdict.[60] Dish has argued that the record evidence does not support the court's conclusion that over a four-month period 13,523,115 calls were placed to residential numbers.[61] Dish has argued that many of those calls were placed to businesses and has sought a drastic reduction of the award.[62] Obviously, a jury award of this magnitude is likely to embolden class plaintiffs in their efforts to extract maximum value for their claims.

A record verdict was also reached for an FCRA claim when TransUnion was hit with a $60 million verdict in class litigation.[63] Specifically, the jury awarded each of the 8,185 class members $984 in statutory damages and $6,353 in punitive damages.[64] The award stems from claims that TransUnion improperly identified the individual class members as terrorists or criminals in consumer credit reports that impacted the ability of the affected individuals to obtain credit or employment.[65] The jury found that TransUnion had failed to provide consumers with appropriate notice under the FCRA and otherwise failed to maintain the accuracy of the records in its systems.[66]

Finally, Google has nearly resolved a long-running dispute in the multidistrict litigation over its alleged practice of bypassing Internet browser privacy settings to spy on users' communications and track usage. The suit, filed in 2012, alleged that Google hacked the popular Safari web browser to bypass privacy settings designed to prevent Google's use of cookies.[67] The case was dismissed in October 2013 on standing grounds.[68] In November 2015, however, the Third Circuit revived certain of the suit's California state law and tort claims.[69]

Under terms of the settlement, Google will create a $5.5 million settlement fund of which up to $3 million will be available for attorneys and settlement

58. United States v. Dish Network LLC, No. 09-3073, 2017 WL 2427297 (C.D. Ill. June 5, 2017).
59. *Id.* at *134.
60. United States v. Dish Network LLC, No. 09-3073 (C.D. Ill. June 26, 2017).
61. Dish Network L.L.C.'s Motion to Alter or Amend the Judgment or in the Alternative to Amend the Findings of Fact and Conclusions of Law, United States v. Dish Network LLC at 2–3, No. 09-3072 (C.D. Ill. July 3, 2017), ECF No. 807.
62. *Id.* at 5–6.
63. Final Verdict Form; Verdict Form Punitive Damages, Ramirez v. Trans Union, LLC, No. 12-cv-00632-JSC (N.D. Cal. June 20, 2017), ECF Nos. 305, 306.
64. *Id.*
65. *See* Complaint at para. 1, Ramirez v. Trans Union, LLC, No. 12-cv-00632-JSC (N.D. Cal. Feb. 9, 2012), ECF No. 1.
66. *See supra* note 63.
67. *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 439 (D. Del. 2013), *aff'd in part, vacated in part, remanded*, 806 F.3d 125 (3d Cir. 2015).
68. *Id.*
69. *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125 (3d Cir. 2015).

administrator fees.[70] The remainder of the fund will be distributed as *cy pres* payments to the Berkeley Center for Law & Technology, the Berkman Center for Internet & Society at Harvard University, the Center for Democracy & Technology (Privacy and Data Project), Public Counsel, Privacy Rights Clearinghouse, and the Center for Internet & Society at Stanford University (Consumer Privacy Project).[71] The case, however, is once again on appeal to the Third Circuit after settlement objectors complained that the settlement provided millions of dollars to class counsel and groups the company favors, but nothing to class members.[72]

Should the settlement become final it will put an end to a saga that saw Google agree to pay $17 million to state attorneys general and another $22.5 million to the FTC, following the public disclosure of Google's cookie hack.[73]

V. VPPA—Defining Personally Identifiable Information

Finally, an interesting potential split of authority has developed between the Third Circuit and the First Circuit as to what constitutes personally identifiable information under the Video Privacy Protection Act of 1988 ("VPPA").[74] The VPPA was enacted in response to the disclosure of Robert Bork's video rental history during the debate over Bork's nomination to the U.S. Supreme Court. Among other provisions, the VPPA generally bans the disclosure of personally identifiable video rental information unless the consumer has consented to such disclosure in writing.[75] Any "video tape service provider"[76] who violates the VPPA can be held liable for a statutory minimum award of $2,500 per disclosure.[77]

Two recent circuit court cases have tested the scope of "personally identifiable information" within the meaning of the VPPA. The Third Circuit took up the issue in *In re Nickelodeon Consumer Privacy Litigation*,[78] where plaintiffs alleged that Google and Viacom violated the VPPA when Viacom transmitted to Google the identity of movies that children watched on Nick.com. Although plaintiffs sought to hold both Google and Viacom liable for violations of the VPPA, the

70. *In re* Google, Inc. Cookie Placement Consumer Privacy Litig., No. 12-MD-2358, 2016 WL 7242562 (D. Del. Sept. 2, 2016).

71. *Id.*

72. Notice of Appeal, *In re* Google, Inc. Cookie Placement Consumer Privacy Litig., No. 12-MD-2358 (D. Del. Mar. 1, 2017), ECF No. 174.

73. *See* N.Y. State Att'y Gen., A.G. Schneiderman Announces $17 Million Multistate Settlement with Google Over Tracking of Consumers (Nov. 18, 2013), https://ag.ny.gov/press-release/ag-schneiderman-announces-17-million-multistate-settlement-google-over-tracking; Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

74. 18 U.S.C. § 2710 (2012).

75. *See id.* § 2710(b)(2)(B).

76. The VPPA defines "video tape service provider" as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." *Id.* § 2710(a)(4). Based on this definition, courts have readily extended the VPPA to forms of video delivery other than old-fashioned tapes, such as online streaming of video content.

77. *Id.* § 2710(c)(2).

78. 827 F.3d 262 (3d Cir. 2016).

Third Circuit, following decisions in both the Sixth and Seventh Circuits, determined that Google could not be liable because only a disclosing party—the video tape service provider—could be liable under the Act.[79]

Having determined that only Viacom was potentially liable under the VPPA, the court turned to the question of whether Viacom had disclosed "personally identifiable information." Plaintiffs claimed that Viacom disclosed, among other information, three critical pieces of identity information to Google: (1) the user's IP address; (2) the user's browser and operating system settings—a so-called "browser fingerprint"; and (3) the computing device's "unique device identifier."[80] Plaintiffs contended that these three pieces of information allowed Google to "track the same computer across time."[81] Essentially, Google could use this information to match a user's Google search with the viewing of a video on Nick.com. In this way, plaintiffs argued that the information was personally identifying. Viacom challenged the argument by asserting that the information, standing alone, did not identify an individual, but instead identified a particular computing device connected to the Internet.[82]

The court noted that the "parties' contrasting positions reflect a fundamental disagreement over what kinds of information are sufficiently 'personally identifying' for their disclosure to trigger liability under the Video Privacy Protection Act."[83] Although the court admitted that the issue was "not straightforward," it agreed with Viacom's interpretation.[84]

An important ground of the court's decision was Congress's retention of the 1988 definition of "personally identifiable information" when it amended the Act in 2013. The court noted that Congress could have easily incorporated a broader definition to capture the disclosure of persistent digital identifiers, but chose not to.[85] The court held that "personally identifiable information" under the VPPA means the kind of information that would readily permit an ordinary person—not Google—to identify a specific individual's video-watching behavior.[86] Here, the information did not meet the standard of personally identifiable information under the VPPA.[87]

On the other hand, in *Yershov v. Gannett Satellite Information Network, Inc.*,[88] the First Circuit held that similar information did constitute "personally identifiable information" under the VPPA. Every time a user views a video clip on Gannet's USA Today mobile app, Gannet sends to Adobe Systems Corp. a data analytics and online marketing company, "(1) the title of the video viewed, (2) the GPS coordinates of the device at the time the video was viewed, and (3) certain

79. *Id.* at 281.
80. *Id.* at 269.
81. *Id.* at 281–82.
82. *Id.* at 282.
83. *Id.*
84. *Id.* at 284.
85. *Id.* at 288–89.
86. *Id.* at 290.
87. *Id.*
88. 820 F.3d 482 (1st Cir. 2016).

identifiers associated with the user's device, such as its unique Android ID."[89] As a result of providing such identifiers, "Adobe was able to identify Yershov and link the videos he had viewed to his individualized profile maintained by Adobe."[90] The court held that this information was sufficient to constitute "personally identifiable information" within the meaning of the VPPA.[91]

The contrasting decisions raise the potential for a split in authority. The Third Circuit, however, rejected any claim that its decision was at odds with *Yershov*. According to the Third Circuit, there was a key factual difference between the two cases: "in *Yershov*, the First Circuit focused on the fact that the defendant there allegedly disclosed not only what videos a person watched on his or her smartphone, but also the GPS coordinates of the phone's location at the time the videos were watched."[92] Unlike the IP address, device identifier, and browser fingerprint that were disclosed in *Nickelodeon*, GPS coordinates "would enable most people to identify what are likely the home and work addresses of the viewer."[93]

The Third Circuit, therefore, plainly sees a higher identification value to geolocation data than it does to an IP address or static identifier of a computing device. Still, there does not appear to be a clear distinction between Adobe's ability to identify an individual with the information supplied by Gannet as in *Yershov*, and Google's ability to identify an individual with the information supplied by Viacom as in *Nickelodeon*. The key to liability for the First Circuit appeared to be the reasonable and foreseeable likelihood that the identity of the individual would be determined from the information Gannet supplied.[94] Such foreseeability was also present in *Nickelodeon*, as the Third Circuit expressly noted.[95] It is, therefore, not clear that the First Circuit would have reached the same conclusion as the Third Circuit on this issue. Thus, while the Third Circuit was explicit in its argument that it was not creating a split in authority, the issue may not be quite as clear as the Third Circuit suggests.

VI. FCC ISP Privacy Rules

In late 2016, the FCC adopted new rules designed to require Internet service providers ("ISPs") to protect consumer privacy.[96] In summary, the rules required ISPs to obtain affirmative opt-in consent from consumers to share certain types of sensitive information, including geolocation data, financial information, health information, children's information, Social Security numbers, web browsing history, app usage history, and the content of communications. ISPs were

89. *Id.* at 484.
90. *Id.* at 485.
91. *Id.* at 486.
92. *Nickelodeon*, 827 F.3d at 289.
93. *Id.*
94. *See Yershov*, 820 F.3d at 486.
95. *See Nickelodeon*, 827 F.3d at 289–90.
96. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274 (Dec. 2, 2016).

allowed to share non-sensitive information as long as consumers could opt out of the sharing.[97] The rules were widely hailed by privacy advocates as a victory for consumers. However, in April 2017 the rules were rejected by joint resolution of Congress under the Congressional Review Act.[98]

VII. Conclusion

In sum, the last year has seen a number of significant privacy developments. One of the key takeaways is the recognition that the potential damages in privacy-related litigation are continuing to increase. An awareness of the changing legal landscape for privacy issues has never been more essential for business attorneys. Not surprisingly, the FTC continues to play an active role in pursuing privacy-related enforcement. The FCC, however, has been hamstrung in its efforts to push stronger privacy protections by the Republican-dominated Congress.

97. Press Release, Fed. Commc'ns Comm'n, FCC Adopts Privacy Rules to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data (Oct. 27, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341937A1.pdf.

98. *See* Cecilia Kang, *Congress Moves to Overturn Obama-Era Online Privacy Rules*, N.Y. Times (Mar. 28, 2017), https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html.