DIGITAL SURVEILLANCE AND THE SCOPE OF THE WIRETAP ACT'S PARTY EXCEPTION

Kathryn Wilson*

INTRODUCTION

Surveillance and data collection are growing increasingly omnipresent, especially in the digital realm.[1] Everyday Google searches and scrolls through Facebook may seem like relatively simple and inconsequential activities. But behind those ordinary actions are sophisticated surveillance systems designed to monitor peoples' online movements, musings, habits, and ponderings.[2] Leading technology companies are perpetually collecting data about what people think, say, and do privately.[3] At the same time, the internet and other modern technologies are revolutionizing how people communicate, share information, and participate in society.[4] As a result, there is a growing tension between embracing new technologies that monitor people's everyday activities and preserving the long-standing right to privacy.[5]

As society becomes increasingly dependent on the internet for economic, educational, and connectivity purposes, private actors are swooping in to collect and exploit vast amounts of data from consumers' internet usage.[6] This has given rise to what scholars call "surveillance capitalism," where digital companies collect and sell personal data in order

* J.D. (2022), Washington University School of Law.

1. *See* Arthur Holland Michel, *There Are Spying Eyes Everywhere—and Now They Share a Brain*, WIRED (Feb. 4, 2021, 12:00 PM), https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/ [https://perma.cc/RCR3-E9VP].

2. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 2–3 (2015); *see also* Matt Burgess, *Chrome's Cookie Update Is Bad for Advertisers but Good for Google*, WIRED (Feb. 3, 2021, 9:00 AM), https://www.wired.com/story/chrome-cookie-update-advertisers-google/ [https://perma.cc/HB8S-W2EV].

3. *See* RICHARDS, *supra* note 2, at 2–3.

4. *Id.*

5. *Id.*

6. *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. OF INFO. TECH. 75, 75–79 (2015).

to generate enormous profits.[7] Large companies like Google and Facebook acquire personal data from their users and sell this to advertisers in the form of targeted online advertisements.[8] And because this business model relies on copious amounts of data, companies are incentivized to collect more and more personal data about internet users.[9] In response, privacy advocates and concerned consumers are seeking to restrain certain data collection practices through legal means.[10] In particular, plaintiffs are turning to Title I of the Electronic Communications Privacy Act ("ECPA")—otherwise known as the Wiretap Act—to protect their online privacy rights.[11]

The Wiretap Act is designed to protect privacy interests by prohibiting unauthorized interceptions of electronic communications,[12] but the Act includes exemptions that allow certain defendants to lawfully intercept these communications.[13] Specifically, the "party exception" permits a defendant to intercept communications and collect personal data where the defendant is considered to be a "party" to the communications.[14] This raises complex legal issues in cases that involve online transactions, because Congress drafted these provisions well before the wide-spread use of the internet and pervasive data collection practices.[15]

Recently, the Third and Ninth Circuits considered whether the party exception may be extended to defendants who surreptitiously intercept and duplicate electronic communications without internet users' knowledge or consent.[16] The Third Circuit first examined this issue in 2015 and answered in the affirmative.[17] The Ninth Circuit, however, split with the Third Circuit in 2020 when it determined that the party exception does not apply to

7. *See id.* at 75–79.
8. *See id.* at 75.
9. *See id.* at 79.
10. *See, e.g.*, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596–97 (9th Cir. 2020).
11. *See* Patrick J. Carome, Samir Jain & Neil M. Richards, *The Electronic Communications Privacy Act and Internet Privacy Litigation*, MEDIA L. RES. CTR., INC., at 1–2 (2002).
12. *See* S. REP. NO. 99-541, at 1–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–57; *see also* 18 U.S.C. § 2511.
13. *See, e.g.*, 18 U.S.C. § 2511(2)(d).
14. § 2511(2)(d).
15. *See* Carome, *supra* note 11, at 24–25.
16. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 137–45 (3d Cir. 2015); *see also In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020).
17. *See In re* Google Cookie Placement, 806 F.3d at 144–45.

defendants who surreptitiously duplicate and communicate users' internet browsing data.[18]

This Note offers a solution to the circuit split concerning the extent of the Wiretap Act's party exception under § 2511(2)(d) and its applicability to entities that employ surreptitious means to intercept and collect communications in order to generate profits. Relying on statutory text and legislative history, this Note argues that the party exception does extend to parties that act surreptitiously, so long as they do not act with a criminal or tortious purpose. The Note further posits that the Wiretap Act, in its current form, is therefore insufficient to protect privacy interests against modern surveillance practices and argues that the time has come for Congress to enact new legislation. Part I discusses the legislative history and purpose of the Wiretap Act and the party exception. Part II discusses the technological landscape and the rise of surveillance capitalism as it relates to litigation involving the party exception. Part III examines the circuit split and analyzes the Third and Ninth Circuits' conflicting approaches. Part IV concludes by arguing that the party exception does apply to certain defendants who act deceptively and explores the privacy interests at stake today under the current provisions of the Wiretap Act.

I. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Modern wiretapping law can be traced back to two 1967 Supreme Court decisions that extended Fourth Amendment protections to certain telephone and in-person conversations.[19] In *Katz v. United States*, the Supreme Court held that people have a reasonable expectation of privacy in telephone conversations that take place in enclosed telephone booths.[20] Accordingly, the Court concluded that wiretapping such conversations constituted a search and seizure within the meaning of the Fourth Amendment and therefore required a warrant.[21] Similarly, in *Berger v. New York*, the Court held that the Fourth Amendment protects in-person conversations and that government officials must obtain a warrant in order to capture such

18. *See In re* Facebook Internet Tracking, 956 F.3d at 608.
19. Carome, *supra* note 11, at 3–4.
20. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
21. *See id.* at 353 (majority opinion).

conversations.[22] In so holding, the Court emphasized the great dangers arising out of technological advances in electronic communication and stated that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[23]

In response to the Supreme Court's rulings in *Katz* and *Berger*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968—commonly known as the Wiretap Act.[24] The Wiretap Act prohibited unauthorized interceptions of "any wire or oral communication" and provided both civil and criminal remedies for violations of the statute.[25] Congress designed the Wiretap Act in order to balance the need for crime prevention efforts with individual privacy rights.[26] To that end, the Wiretap Act permitted law enforcement to collect evidence consistent with the Fourth Amendment while also protecting privacy rights.[27] Congress established a private right of action that expanded the scope of the Act beyond merely government regulation of wiretapping.[28] The Wiretap Act consequently became the primary law governing the privacy and security rights of voice communications in the United States.[29] However, its provisions were "expressly limited to the unauthorized *aural* interception of wire or *oral* communications."[30] In other words, the Wiretap Act protected only verbal communication that could be heard and understood by the human ear.[31] This limitation soon inhibited the Wiretap Act's ability to protect new forms of communication as the mid-1980s saw a dramatic rise in advanced telecommunication and computer-based technologies.[32]

In 1986, Congress passed ECPA to update federal privacy protections in response to these rapidly advancing technologies and the widespread use

22. *See* Berger v. New York, 388 U.S. 41, 51 (1967).

23. *Id.* at 62–63.

24. Carome, *supra* note 11, at 4; *see also* S. REP. NO. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

25. Pub. L. No. 90-351, 82 Stat. 213 (1968) (current version at 18 U.S.C § 2511(1)(a)).

26. *See* S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

27. *See id.*

28. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 340 (Robert C. Clark et al. eds., 2016).

29. *See* S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

30. *See id.* (emphasis added).

31. *See id.*

32. *See id* at 2–3; *see also* Carome, *supra* note 11, at 5.

of computers.[33] Recognizing the inherent dangers posed by these increasingly sophisticated surveillance devices, Congress broadened the reach of the Wiretap Act "to protect against the unauthorized interception of *electronic* communications."[34] In particular, Congress was concerned about "overzealous law enforcement agencies, industrial spies and private parties [being able to readily] intercept . . . personal or proprietary communications" that occurred through electronic channels.[35]

The amended Wiretap Act comprises Title I of ECPA and prohibits the unauthorized interception of "any wire, oral, or electronic communication."[36] ECPA defines "electronic communications" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[37] Notably, the words "internet," "online" and "World Wide Web" do not appear within the text of the statute.[38] Nevertheless, courts have interpreted the Wiretap Act as applying to modern online transactions because of ECPA's broad definition of "electronic communications."[39] Additionally, the United States, unlike the European Union, does not have a federal statute that establishes comprehensive privacy rights and governs the collection of all personal data.[40] ECPA, therefore, continues to be an important federal statute in online privacy litigation.[41]

Section 2511(1)(a) of the Wiretap Act provides that any person[42] who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic

33. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat 1848; S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

34. *See* S. REP. NO. 99-541, at 1–3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–3557 (emphasis added); *see also* 18 U.S.C. §2511(1).

35. *Id.*

36. 18 U.S.C. § 2511(1); *see also* MCGEVERAN, *supra* note 28, at 340–42.

37. § 2510(12).

38. *See generally* § 2510; *see also* § 2511; Yonatan Lupu, *The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?*, 9 VA. J.L. & TECH. no. 3, at ¶ 9 (2004).

39. *See* Lupu, *supra* note 38, at ¶ 15.

40. *See* Carome, *supra* note 11, at 1–2.

41. *See id.*

42. *See* 18 U.S.C. § 2510(6) (Defining the term "person" to mean "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.").

communication . . . shall be punished . . . or shall be subject to suit."[43] Like its predecessor, the amended Wiretap Act creates criminal prohibitions and a private right of action for those injured by unlawful interceptions.[44] A successful plaintiff may recover equitable forms of relief and compensatory damages, including the greater of (A) actual damages and profits made by the defendant as a result of the violation, or (B) statutory damages of $100 per day of violation or $10,000, whichever is greater.[45]

The Wiretap Act includes several exceptions to its general prohibition against unauthorized interceptions of electronic communications.[46] One exception is the "party" exception under § 2511(2)(d), which provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication *where such person is a party to the communication* or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.[47]

In other words, a person may be exempt from liability under the Wiretap Act when that person is considered to be a party to the communication.[48] However, the term "party" is not defined within the text of the statute, and Congress did not elaborate on the meaning of the term when it last amended the Wiretap Act in 1986.[49] Courts have therefore been required to interpret the term and determine the scope of the party exception.[50]

The party exception is subject to limitations which have evolved over time. Since its enactment in 1968, the party exception has not applied where the person acted with the intent to commit a criminal or tortious act.[51] But

43. § 2511(1)(a).
44. § 2520; *see also* Carome, *supra* note 11, at 6.
45. § 2520(c); *see also* Carome, *supra* note 11, at 6–7.
46. *See* Carome, *supra* note 11, at 6.
47. § 2511(2)(d) (emphasis added).
48. *Id*.
49. § 2510.
50. *See*, *e.g.*, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607–08 (9th Cir. 2020).
51. *See* § 2511(2)(d).

prior to 1986, § 2511(2)(d) further provided that the party exception also did not apply where the interception was done "*for the purpose of committing any other injurious act*."[52] Over time Congress grew concerned that plaintiffs were attempting to use the "other injurious act" language to prevent defendants from asserting the party exception in contexts that threatened to chill First Amendment rights.[53] In particular, Congress was troubled by the interpretation and use of the "other injurious act" language in *Boddie v. American Broadcasting Companies.*[54]

In *Boddie*, the plaintiff agreed to be interviewed by journalists about an investigation.[55] During the interview, the defendant journalists secretly recorded the conversation with the plaintiff using hidden cameras and microphones.[56] The defendants later broadcasted part of this interview in a televised report.[57] The plaintiff argued that the defendants' surreptitious recording of the conversation violated the Wiretap Act.[58] In response, the defendants argued that they were entitled to a privileged immunity as parties to the conversation and thus were exempt from liability.[59] The plaintiffs countered that the defendants were not entitled to the party exception, because the defendants' purpose for the interception was "to cause . . . insult and injury."[60] Thus, the plaintiff argued that because the defendants intercepted the communication for injurious purposes, they were not exempt from liability as a party to the communication.[61] The Court in *Boddie* concluded that "the language and legislative history of the statute clearly demonstrate that the [party] privilege is not extended if the intercepting party acted with the purpose of committing . . . [an] injurious act."[62] The Court determined that the defendants' purpose for recording the conversation raised a question of fact for the jury and could not be decided

52. Pub. L. No. 90-351, 82 Stat. 213, 214 (1968) (emphasis added).
53. *See* S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.
54. *Id.*
55. Boddie v. Am. Broad. Cos., 731 F.2d 333, 335 (6th Cir. 1984).
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.* at 337.
60. *Id.* at 338.
61. Boddie v. Am. Broad. Cos., 731 F.2d 333, 338 (6th Cir. 1984).
62. *Id.*

as a matter of law.[63] Accordingly, the Court remanded the case for further proceedings.[64]

In response to *Boddie* and other similar cases, Congress amended § 2511(2)(d) by striking out the language "or for the purpose of committing any other injurious act."[65] In doing so, Congress noted that the defendant in *Boddie* had been a party to the conversation and that the "other injurious act" wording placed "a stumbling block in the path of even the most scrupulous journalist."[66] Congress expressed concern that such a limitation on the party exception created a threat that was "inconsistent with the guarantees of the first amendment."[67] Congress therefore revised § 2511(2)(d) to its current form and emphasized that the amended statute still afforded ample protection against unauthorized interceptions by prohibiting interceptions done for criminal or tortious purposes.[68]

When Congress amended the Wiretap Act in 1986, its discussion of the party exception under § 2511(2)(d) was limited to the striking out of the "other injurious act" wording.[69] Congress did not provide any additional guidance on the meaning of the term "party" nor the scope of the party privilege.[70] As use of the internet rapidly grew in popularity, questions soon emerged regarding the application of the party exception in online contexts. By the early 2000s, defendants were using the party exception to avoid liability under the Wiretap Act in cases involving online privacy litigation.[71]

A. In re DoubleClick, Inc. Privacy Litigation

In re DoubleClick, Inc. Privacy Litigation ("*DoubleClick*") was one of the first cases that addressed allegations of ECPA violations pertaining to targeted internet advertisements.[72] The defendant was the largest provider

63. *Id.*

64. *Id.* at 339.

65. S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571; *see also* Pub. L. No. 90-351, 82 Stat. 213, 214 (1968).

66. S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.

67. *See* S. REP. NO. 99-541, at 17–18 (1986) (noting that the "other injurious act" wording could subject journalists to civil and criminal suits, "even if the interception was made in the ordinary course of responsible news-gathering . . . and not for the purpose of committing a criminal act or a tort.").

68. *Id.*

69. *See id.*

70. *See id.*

71. *See, e.g.*, *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).

72. *See id.* at 500.

of internet advertisements and services in the world at the time.[73] To facilitate targeted online advertisements, the defendant compiled profiles on individuals who visited affiliated websites within its network, which included more than 1,500 websites and, among those, some of the most highly trafficked sites.[74] The defendant collected site users' data by placing "cookies" on their hard drives when they visited affiliated websites.[75] Using GET submissions,[76] the cookies then collected and stored information such as a user's activity on an affiliated website and the user's query strings.[77] The plaintiffs were internet users and alleged that the defendant's actions constituted a violation of the Wiretap Act.[78] The defendant conceded that its alleged conduct violated the Wiretap Act's general prohibitions but argued that it was nevertheless exempt from liability pursuant to the party exception in § 2511(2)(d), because the affiliated websites consented to its interceptions. This raised the question whether websites may be parties to communications under the Wiretap Act.[79]

The district court in *DoubleClick* held that the affiliated websites were "parties to the communication[s]" under the Wiretap Act and, therefore, could consent to interceptions of those communications by third parties pursuant to the party exception.[80] The court reasoned that users' GET submissions are "intended for" the requested websites, noting that "users voluntarily type-in information they wish to submit to the Web sites, information such as queries, commercial orders, and personal information."[81] Additionally, the court held that a "criminal" or "tortious" purpose will only prevent the application of the party exception where there is "a specific contemporary *intention to commit a crime or tort*."[82] In its analysis of § 2511(2)(d), the court focused on whether the interception was done with the specific intent to commit a criminal or tortious act—not

73. *Id.*
74. *Id.* at 502.
75. *Id.*
76. A GET request transmits information between a user's internet browser and the destination website. *See infra* pp. 24–27.
77. *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).
78. *Id.* at 503, 514.
79. *See id.* at 514.
80. *See id.* at 514–19.
81. *Id.* at 511.
82. *Id.* at 515 (emphasis added).

whether the interception *itself* was criminal or tortious in nature.[83] The court further explained that when a party consents to an interception, the plaintiff must show either "(1) that the primary motivation, or (2) that a determinative factor in the actor's . . . motivation for intercepting the conversation was to commit a criminal [or] tortious . . . act."[84] Because the court determined that the defendant in *DoubleClick* had not acted for the purpose of committing a tort, but instead to generate profit, the court concluded that § 2511(2)(d) exempted the defendant from liability under the Wiretap Act.[85]

B. In re Intuit Privacy Litigation

In re Intuit Privacy Litigation similarly involved alleged ECPA violations relating to the collection of personal data in order to facilitate targeted online advertisements.[86] In that case, the defendant operated the financial website quicken.com and partnered with a third-party advertiser to create targeted online advertisements.[87] The plaintiffs were internet users who had visited the quicken.com website and subsequently alleged that the defendant violated § 2511 by intercepting their electronic communications with a criminal or tortious purpose.[88] Specifically, the plaintiffs argued that the defendant: planted unauthorized cookies on their computers; repeatedly intercepted electronic communications without their knowledge or consent; and secretly tracked their online activity and collected personal information in order to send users targeted advertisements.[89] Although the plaintiffs acknowledged that the defendant was a participant to the communications, they maintained that the defendant could nevertheless be held liable for acting with a criminal or tortious purpose–thereby precluding the application of the party exception under § 2511(2)(d).[90] To support their claims, the plaintiffs asserted that the defendant's violations of § 2511 and

83. *See id.* at 516 (citing Sussman v. Am. Broad. Cos., 186 F.3d 1200 (9th Cir. 1999)).
84. *See id.* at 514–15 (quoting United States v. Dale, 991 F.2d 819, 841–42 (D.C. Cir. 1993)).
85. *Id.* at 519.
86. *See In re* Intuit Priv. Litig., 138 F. Supp. 2d 1272, 1278 (C.D. Cal. 2001).
87. *Id.* at 1274.
88. *Id.* at 1278.
89. *Id.*
90. *See id.*

two other federal statutory provisions demonstrated the requisite criminal or tortious purpose.[91]

Similar to *DoubleClick*, the court found here that the defendant was a party to the communications and therefore could consent to the interceptions of electronic communications between it and the plaintiffs.[92] The court further determined that the plaintiffs had failed to sufficiently show that the defendant intercepted these communications for the purpose of committing a criminal or tortious act.[93] Accordingly, the court concluded that the defendant was exempt from liability pursuant to § 2511(2)(d), reasoning that "[u]nder 2511, the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception–its intended use–was criminal or tortious. . . . Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere."[94] Accordingly, the court concluded that the plaintiffs had failed to allege that the defendant intercepted their communications for the purpose of facilitating violations of § 2511 and the other statutory provisions at issue.[95] In doing so, the court held that the plaintiffs' allegations were insufficient to survive a Rule 12(b)(6) motion to dismiss.[96]

C. In re Pharmatrak, Inc.

In re Pharmatrak, Inc. ("*Pharmatrak*") is another case concerning alleged ECPA violations where companies collected and tracked internet users' data.[97] In that case, the defendant sold a service called "NETcompare" to pharmaceutical companies, which was a tool that collected data in order to allow companies to conduct intra-industry comparisons of website traffic and usage.[98] Most of the pharmaceutical companies who purchased the service expressly stated that they did not want users' personal information or any identifying data collected.[99] Through the

91. *Id.* at 1278–79
92. *Id.*
93. *Id.* at 1277–79.
94. *Id.* at 1278–79 (quoting Sussman v. Am. Broad. Cos., 186 F.3d 1200 (9th Cir. 1999)).
95. *Id.*
96. *Id.*; *see also* Carome, *supra* note 11, at 15.
97. *In re* Pharmatrak, Inc., 329 F.3d 9, 12 (1st Cir. 2003).
98. *Id.*
99. *Id.* at 12, 15.

use of persistent cookies,[100] NETcompare collected "the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site . . . the visitor's IP address; and . . . the webpage the user viewed immediately before arriving at the client's site (i.e., the 'referrer URL')."[101] Although NETcompare was purportedly designed to not collect personal information, it nevertheless collected personal information on a small number of users, including: "names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website."[102] This personal information was collected in part because of an interaction between NETcompare and one of its client's computer code, which used the "GET" method.[103] The plaintiffs alleged that the defendant violated the Wiretap Act by intercepting electronic communications without the consent of either the plaintiffs or the pharmaceutical companies.[104]

The district court granted summary judgment in favor of the defendant, holding that § 2511(2)(d) shielded the defendant from liability because the pharmaceutical companies had consented to the interceptions by agreeing to use the NETcompare services.[105] On appeal, the First Circuit addressed the issue of whether the defendant was exempt from liability pursuant to § 2511(2)(d) based on the pharmaceutical companies' consent. The First Circuit began by recognizing that "[t]he paramount objective of the Wiretap Act is to protect effectively the privacy of communications."[106] The First Circuit then held that "[a] party may consent to the interceptions of only part of a communication or to the interception of only a subset of its communications."[107] It further provided that "a reviewing court must inquire into the *dimensions of the consent* and then ascertain whether the interception exceed those boundaries."[108] The First Circuit noted that while

100. *Id.* at 14 (explaining that "[a] persistent cookie is one that does not expire at the end of an online session.").

101. *Id.* at 13.

102. *Id.* at 15 (noting that out of approximately 18.7 million persistent cookies, just 232 user profiles contained personal information).

103. *Id.* at 15–16.

104. *Id.* at 12–13.

105. *Id.* at 17.

106. *Id.* at 18.

107. *Id.* at 19.

108. *Id.* (quoting Gilday v. Dubois, 124 F.3d 277, 297 (1st Cir. 1997)).

consent may be express or implied, "it should not be casually inferred,"[109] explaining that "[w]ithout actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."[110] The First Circuit made clear that the party seeking the benefit of the consent exception bears the burden of proof.[111] The First Circuit then determined that the pharmaceutical companies had expressly indicated that they did not want to collect personal or identifying data about users.[112] Accordingly, the First Circuit concluded that the pharmaceutical companies had not consented to the collection of personally identifiable information, and therefore, had not consented to NETcompare's interception of it.[113] Holding that the party exception did not apply, the court reversed and remanded the case.[114]

II. THE RISE OF SURVEILLANCE CAPITALISM

Given the technical nature of ECPA, it is helpful to consider it within the context of today's technological environment. The Information Age has revolutionized how society operates, creating unprecedented capacities to share, access, and collect information.[115] The internet is now a central part of how people connect with one another, conduct business, educate themselves, and participate in society.[116] As one scholar noted, people "must 'plug in' to join in" and "establish relationships with a panoply of companies."[117] Increasingly, people are dependent upon digital companies that collect, use, and sell their personal data.[118] Search engines, social media platforms, streaming services, fitness applications, video-meeting applications, and many other online service providers all collect information

109. *Id.* at 20 (quoting Griggs-Ryan v. Smith, 904 F.2d 112, 117–118 (1st Cir. 1990)).
110. *Id.* (quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998)).
111. *Id.* at 19.
112. *Id.* at 20.
113. *Id.*
114. *See id.* at 23.
115. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089–95 (2002); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013).
116. *See* RICHARDS, *supra* note 2, at 2–3.
117. *See* Solove, *supra* note 115, at 1089.
118. *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11 (2020); *see also* Richards, *supra* note 115, at 1938.

about their users.[119] Digital technologies and services now facilitate much of people's everyday lives and as a result, even the most ordinary tasks expose people to pervasive and covert surveillance and data collection.[120]

Private digital companies have transformed data collection and surveillance into multi-billion dollar businesses.[121] On a superficial level, the internet and social media platforms are free to use.[122] But in reality those services are made available for "free" in exchange for the right to collect vast amounts of personal data and to conduct pervasive surveillance.[123] Digital companies collect personal information and develop highly detailed user profiles in order to facilitate and sell individualized targeted advertisements.[124] The online advertising industry now generates billions of dollars in revenue each year and has led to the exponential growth of companies like Google and Facebook, both of which have built their companies around the sale of targeted online advertisements and are dominant in the big data industry.[125]

Through the collection and analysis of personal data from end users, targeted advertisements are able to deliver content to narrowly defined audiences.[126] Digital companies seek to maximize the advertising space they sell by tailoring content in order to appeal to individual users.[127] Such individualized content increases the amount of time those users spend on the site and drives greater engagement among end users.[128] This is significant because "advertising revenues depend on the amount of time and

119. Balkin, *supra* note 118, at 12-13.

120. *See* Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in A Digital World*, 4 GEO. L. TECH. REV. 1, 29 (2019); *see also* Balkin, *supra* note 118, at 13.

121. Richards, *supra* note 115, at 1938.

122. *See id.*

123. *See id.*; *see also* Jack M. Balkin, *Fixing Social Media's Grand Bargain* 1 (Hoover Inst., Aegis Series Paper No. 1814, 2018).

124. *See* Balkin, *supra* note 123, at 2; *see also* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1469 (2020) ("In order to maximize the value of the ad space it sells, Google mobilizes its vast troves of data to profile each user with increasing granularity.").

125. Sheila Dang, *Google, Facebook Have Tight Grip on Growing U.S. Online Ad Market: Report*, REUTERS (Jun. 5, 2019, 8:08 AM), https://www.reuters.com/article/us-alphabet-facebook-advertising/google-facebook-have-tight-grip-on-growing-u-s-online-ad-market-report-idUSKCN1T61IV [https://perma.cc/CEN3-RDP2] (projecting that the U.S. digital advertising industry will reach $160 billion by 2023); *see also* Richards, *supra* note 115, at 1938.

126. *See* Balkin, *supra* note 123, at 2.

127. *See id.*

128. *See id.*

attention [users spend] on the site."[129] Digital companies are able to sell more advertisements when there are more users on the site.[130] Thus, the more precisely digital companies can curate engaging content that maintains users' attention, the more valuable that advertising space becomes and the more profits digital companies earn as a result.[131] Business models centered around the sale of targeted advertisements therefore incentivize companies to collect increasing amounts of data on end users.[132]

A. Surveillance Capitalism

What makes the targeted advertising model particularly lucrative for digital giants like Google and Facebook is the potential to predict and modify human behavior.[133] In order to increase their predictive capacities, digital companies rely on massive data sets to extract and analyze behavioral patterns.[134] "Big data" refers broadly to the "creation and analysis of massive data sets."[135] An important and noteworthy aspect of big data is its ability to show relationships between data.[136] The value of collecting huge amounts of data ultimately arises from the "patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."[137] Using sophisticated algorithms, digital companies are able to analyze massive data sets and extract patterns in human behavior.[138] The relationships gleaned from this data are then used to draw extraordinary inferences and findings that digital companies use to sell targeted advertisements.[139] To strengthen their abilities to predict and modify consumer behavior, digital companies

129. *See id.*
130. *See* Zuboff, *supra* note 6, at 79.
131. *See* Balkin, *supra* note 123, at 2–3; *see also* Zuboff, *supra* note 6, at 79.
132. *See* Balkin, *supra* note 123, at 3.
133. *See* Zuboff, *supra* note 6, at 75, 79.
134. *See id.* at 79.
135. Richards, *supra* note 115, at 1939.
136. *Id.*; *see also* danah boyd & Kate Crawford, *Six Provocations for Big Data*, A Decade in Internet Time: Symposium on the Dynamics of the Internet & Soc'y, 1–2 (Sept. 21, 2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431.
137. Richards, *supra* note 115, at 1939 (quoting boyd & Crawford, *supra* note 136).
138. Zuboff, *supra* note 6, at 79; *see also* boyd & Crawford, s*upra* note 136.
139. *See* Richards, *supra* note 115, at 1939; *see also* Zuboff, *supra* note 6, at 79.

continue to collect ever increasing amounts of data and "[n]othing is too trivial or ephemeral for this harvesting."[140]

Big data is foundational to the rise of what scholars call *surveillance capitalism*.[141] Surveillance capitalism uses information derived from big data "to predict and modify human behavior as a means to produce revenue and market control."[142] Many digital companies design their products and services to collect "data exhaust,"[143] because all data has potential value—no matter how seemingly insignificant or inconsequential.[144] Harvard Business School professor emerita Shoshana Zuboff argues that surveillance capitalists view people as "objects from which raw materials are extracted and expropriated."[145] Zuboff emphasizes that the extraction of personal data is a one-way process that lacks productive reciprocity.[146] Within the surveillance capitalism model, revenue depends on the appropriation of data obtained from ubiquitous online transactions.[147] This level of data collection and surveillance occurs largely without detection by end users.[148]

B. How Data is Collected

Digital companies are able to track users across the internet using "cookies"—small text files that are placed on users' computer or mobile devices when they visit a website.[149] Cookies allow websites to track how users navigate a website, including the pages they visit and the amount of time they spend on each page.[150] Additionally, cookies can reveal browsing

140. Zuboff, *supra* note 6, at 79.
141. *Id.* at 75.
142. *Id.* at 75.
143. The term "data exhaust" refers broadly to the collection of information that flows from individuals' computer-mediated actions and includes "Facebook 'likes,' Google searches, emails, texts, photos . . . every click, misspelled word, page view, and more." *See id.* at 79.
144. *Id.* at 79.
145. Kapczynski, *supra* note 124, at 1469 (internal quotations omitted).
146. *See* Zuboff, *supra* note 6, at 79–80.
147. *Id.* at 80.
148. *Id.* at 79.
149. *See* Fern L. Kletter, Annotation, *Claims Concerning Use of "Cookies" To Acquire Internet Users' Web Browsing Data Under Federal Law*, 36 A.L.R. Fed. 3d Art. 5 (2018); *see also* Chris Jay Hoofnagle et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 276 (2012); EUROPEAN COMMISSION, https://ec.europa.eu/info/cookies_en [https://perma.cc/E6RN-56JP] (last visited Nov. 7, 2020).
150. Kletter, *supra* note 149, at § 2.

habits, online purchases, preferences, login information, and search terms.[151] Digital companies employ first-party and third-party cookies to track users online movements.[152] First-party cookies are those that are placed by the website the user is visiting.[153] Third-party cookies, on the other hand, are those placed by separate, third-party websites and commonly track users across their internet searches.[154] Using these cookies, digital companies are able to capture and aggregate users' data and activities, including those beyond their own websites.[155] The aggregation of this data enables digital companies to draw vast inferences about users, including those related to sensitive issues.[156] Although cookies often use only a string of numbers to identify and track a device, there are mechanisms to connect pseudonymous cookies to personally identifying information.[157]

In addition, digital companies use GET requests to collect personal data,[158] which enable communications to be transmitted between a user's web browser and the server hosting the requested website.[159] GET requests first communicate what information the user is requesting and then direct the website's server to send that information back to the user.[160] In doing so, GET requests send a referrer header—or Uniform Resource Locator (URL) information—to the website's server.[161] Notably, this URL information includes the user's query string.[162] As a general matter, this communication

151. *Id.* at § 18; *see also How to Protect Your Privacy Online*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0042-online-tracking#understanding_cookies [https://perma.cc/G97Z-TME2].

152. Hoofnagle, *supra* note 149, at 276. But notably dominant companies like Google and Apple are planning to remove third-party cookies from their web browsers and are currently seeking to implement alternative technologies to support their targeted online advertising efforts. *See* Sam Schechner, *Google Pursues Plan to Remove Third-Party Cookies*, WSJ (Jan. 25, 2021, 10:28 AM), https://www.wsj.com/articles/google-progresses-plan-to-remove-third-party-cookies-11611581604 [https://perma.cc/92HX-NYV8].

153. Hoofnagle, *supra* note 149, at 276.

154. *Id.*

155. *Id.*

156. *Id.*

157. *Id.* at 276–77.

158. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (9th Cir. 2020); *see also In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 268 (3d Cir. 2016).

159. *HTTP Request Methods*, W3SCHOOLS, https://www.w3schools.com/tags/ref_httpmethods.asp [https://perma.cc/W4VP-355K]; *see also In re Facebook Internet Tracking*, 956 F.3d at 607.

160. *In re Facebook Internet Tracking*, 956 F.3d at 607.

161. *Id.*

162. W3SCHOOLS, *supra* note 159; *see also In re Facebook Internet Tracking*, 956 F.3d at 607.

occurs between the user's browser and the requested website's server,[163] but the URL information in GET requests can also be sent to third-party servers in order to facilitate targeted online advertisements.[164] On websites showing targeted advertisements, a GET request is sent to the third-party server that hosts the advertisements, which responds by sending an advertisement to the user's browser.[165] From the user's perspective, the requested content and the advertisement appear simultaneously within a matter of milliseconds, and the user has no indication of the fact that their browsing data has just been collected.[166]

III. THE CIRCUIT SPLIT

In recent years, a circuit split has emerged regarding the extent of the Wiretap Act's party exception and its applicability to entities that surreptitiously duplicate users' GET requests and communicate that information to third-party servers for the purpose of collecting personal data.[167] The Third Circuit has held that the party exception under § 2511(2)(d) applies to the intended recipients of a communication and may still protect defendants who use deceptive practices to gain entrance to the conversation.[168] Conversely, the Ninth Circuit has held that the party exception does not exempt a defendant from liability where the defendant surreptitiously duplicates a communication.[169] The circuits thus differ in their interpretations of the scope of the party exception and its application to parties that act surreptitiously.

A. The Third Circuit's Approach: In re Google Inc. Cookie Placement Consumer Privacy Litigation

In re Google Inc. Cookie Placement Consumer Privacy Litigation ("*Google Cookie Placement*") addressed alleged ECPA violations involving the use of cookies and GET requests to collect personal data in order to

163. *In re Facebook Internet Tracking*, 956 F.3d at 607.
164. *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 130 (3d Cir. 2015).
165. *Id.*
166. *Id.*
167. *See id.* at 125; *see also In re Facebook, Inc. Internet Tracking*, 956 F.3d at 607.
168. *See In re Google Cookie Placement*, 806 F.3d at 142–44.
169. *See In re Facebook, Inc. Internet Tracking*, 956 F.3d at 607–08.

facilitate targeted online advertisements.[170] The plaintiffs alleged that the defendants, including Google and other internet advertisers, placed cookies on their personal computers "in contravention of their browsers' cookie blockers and defendant Google's own public statements."[171] The plaintiffs had enabled "cookie blockers" in order to prevent third-party cookies from being placed on their computers.[172] Google's Privacy Policy at the time stated that users "can reset [their] browser to refuse all cookies or to indicate when a cookie is being sent."[173] Google further assured their users that Apple's Safari web browser blocked all third-party cookies by default.[174] Despite Google's own assurances and the use of cookie blockers, the defendants nevertheless placed third-party cookies on users' computers.[175] A report revealed that "Google and the other defendants had discovered, and were surreptitiously exploiting, loopholes in both the Safari cookie blocker and the Internet Explorer cookie blocker."[176]

The plaintiffs argued that the defendants violated the Wiretap Act by intercepting their electronic communications while they were in transit from the plaintiffs' web browsers to the requested website's server.[177] In particular, the plaintiffs alleged that the defendants improperly tracked their web browsing history through the use of GET requests and third-party cookies.[178] The plaintiffs explained that after receiving a GET request, the first-party website's server would direct the plaintiff's web browser to send a GET request to a third-party server hosting the targeted advertisement. In the process of sending the advertisement to the requested webpage, the defendants placed cookies on the plaintiffs' devices. The plaintiffs alleged that the third-party cookies were associated with a unique browser on a device and thereby allowed the defendants to identify and track the plaintiffs' online activity across different websites.[179] In response, the defendants argued that "they were the intended recipients of – and thus

170. *In re Google Cookie Placement*, 806 F.3d at 130–34.
171. *Id.* at 130.
172. *Id.* at 132.
173. *Id.*
174. *Id.* at 132.
175. *Id.*
176. *Id.* at 132.
177. *See id.* at 140.
178. *See id.* at 140–42.
179. *See id.* at 141.

'parties' to – any electronic transmissions that they acquired and tracked."[180] Accordingly, the defendants claimed that they were exempt from liability under the Wiretap Act as parties to the communication.[181]

After concluding that at least some queried URLs qualify as content under the Wiretap Act, the Third Circuit addressed whether the defendants were "parties" to the communication pursuant to the party exception.[182] The Third Circuit determined that "the defendants acquired the plaintiffs' internet history information by way of GET requests that the plaintiffs sent *directly to* the defendants, and that the defendants deployed identifier cookies to make the information received from GET requests associable and thus trackable."[183] Accordingly, the Third Circuit held that the party exception applied to the defendants as "the intended recipients of the transmissions at issue" and therefore exempted the defendants from liability under the Wiretap Act.[184] In doing so, the Third Circuit explained that every communication consists of (1) a speaker/sender and (2) at least one intended recipient.[185] The Third Circuit concluded that an intended recipient of a communication is necessarily one of the parties to that communication.[186]

Notably, the Third Circuit rejected the plaintiff's argument that the party exception should not apply to the defendants in this case because the defendants had induced the plaintiffs to send the transmissions at issue by deceit and surreptitiously intercepted those communications.[187] Although the Third Circuit acknowledged that the defendants' conduct was troubling, it found it significant that the Wiretap Act does not include any language that specifically prohibits the application of the party exception where the communication was induced by fraud.[188] The Third Circuit explained that "[i]t is not unimaginable that the Wiretap Act would give legal effect to the fraudulent participation of a party to a conversation."[189]

To underscore this proposition, the Third Circuit pointed to the fact that Congress specifically referenced *United States v. Pasha* in its discussions

180. *Id.* at 139–40.
181. *See id.* at 140.
182. *Id.*
183. *Id.* at 142–43 (emphasis added).
184. *Id.*
185. *See id.*
186. *Id.*
187. *Id.* at 143.
188. *Id.*
189. *Id.* at 143.

of the party exception under § 2511(2)(c).[190] In *Pasha*, the Seventh Circuit held that an officer impersonating the intended recipient of a communication was an "immediate party" to a telephone conversation.[191] When Congress enacted the Wiretap Act in 1968, it stated that the term "'party' would mean the person actually participating in the communication" and cited to *Pasha*.[192] The Third Circuit agreed with the Sixth and Fifth Circuits' conclusion that "[b]y citing to *Pasha*, Congress strongly intimated that one who impersonates the intended receiver of a communication may still be a party to that communication for the purposes of the federal wiretap statue and that such conduct is not proscribed by the statute."[193] The Third Circuit concluded that Congress intentionally did not include language which would prohibit the application of the party exception where the defendant fraudulently procured the communication.[194] Accordingly, the Third Circuit held that the defendants were exempt from liability as parties to the communication under § 2511(2)(d).[195]

B. The Ninth Circuit's Approach: In re Facebook, Inc. Internet Tracking Litigation

In April 2020, the Ninth Circuit declined to follow the Third Circuit's reasoning.[196] The case of *In re Facebook, Inc. Internet Tracking Litigation* ("*Facebook Internet Tracking*") considered whether Facebook violated the Wiretap Act when it continued to track the plaintiffs' internet browsing histories after they had logged out of the social media platform.[197] Facebook conceded that it used plug-ins embedded on third-party websites to capture and compile the plaintiffs' internet browsing histories in order to facilitate

190. *Id.* at 143–44 (noting that 18 U.S.C. § 2511(2)(c) is "pari materia with § 2511(2)(d) and differs from that provision only in that § 2511(2)(c) applies to persons acting under color of law.").

191. United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (finding that "there was no tampering with the established means of communication. Indeed the officer was the immediate party to the call. The [sender] intended his words to reach the officer, albeit the [sender] thought he was someone else.").

192. S. REP. NO. 90–1097, at 93–94 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182.

193. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d at 144 (quoting Clemons v. Waller, 82 F. App'x 436, 442 (6th Cir. 2003)).

194. *Id.* at 143–144.

195. *Id.* at 145.

196. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020).

197. *Id.* at 596–97.

targeted online advertisements.[198] The Facebook plug-ins contained pieces of code designed "to replicate and send the user data to Facebook through a separate, but simultaneous, channel in a manner undetectable by the user."[199] On websites that included Facebook plug-ins, the code instructed the users' web browser to copy and send the users' GET requests to Facebook.[200] These GET requests included referrer headers that contained "personally-identifiable URL information," including the users' search terms and the precise documents the users viewed on a particular webpage.[201] The plaintiffs alleged that Facebook then compiled these referrer headers into user profiles using cookies stored on the plaintiffs' devices and continued to collect this information after they had logged out of Facebook.[202]

Through this process, the plaintiffs argued that Facebook collected "an enormous amount of individualized data" from millions of websites that included Facebook plug-ins.[203] The plaintiffs emphasized that Facebook constantly and indiscriminately collected this data "no matter how sensitive" the information was.[204] Additionally, the plaintiffs asserted that Facebook had failed to disclose that it would continue to track users' browsing history after they logged out of the platform.[205] The plaintiffs argued that "by correlating users' browsing history with users' personal Facebook profiles . . . Facebook gained a cradle-to-grave profile without users' consent" and caused harm or "a material risk of harm to [the plaintiffs'] interest in controlling their personal information."[206] The plaintiffs therefore asserted that Facebook's conduct violated their right to privacy under the Wiretap Act.[207]

At the outset, the Ninth Circuit recognized that the right to privacy "encompass[es] the individual's control of information concerning his or her person."[208] The Ninth Circuit acknowledged that technological advances

198. *Id.* at 596.
199. *Id.*
200. *Id.* at 607.
201. *Id.* at 596–607.
202. *Id.* at 596.
203. *Id.* at 603.
204. *Id.* at 598.
205. *Id.* at 602–03.
206. *Id.* at 599.
207. *Id.*
208. *Id.* at 598 (quoting Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017)).

could create increased risks for privacy violations and explained that "[i]n an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion ... that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data ... is untenable."[209] The Ninth Circuit therefore concluded that the plaintiffs had standing to pursue their claims under the Wiretap Act.[210]

Recognizing that the Wiretap Act does not define the term "party" within its exception from liability, the Ninth Circuit considered how other federal courts have supposedly interpreted the scope of the term.[211] In *Pharmatrak*, the First Circuit determined that the defendant could be held liable under the Wiretap Act where it "automatically duplicated part of the communication between a user and a [pharmaceutical company website] and sent this information to [the defendant]."[212] Similarly, in *United States v. Szymuszkiewicz*, the Seventh Circuit held that a defendant could be held liable under the Wiretap Act where he had used software to duplicate and contemporaneously forward all emails his employer received to his own inbox.[213] In considering these two cases, the Ninth Circuit concluded that both the "First and Seventh Circuits have implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to communications within the meaning of the Act."[214]

However, the Ninth Circuit acknowledged that the Third Circuit has held to the contrary.[215] The Ninth Circuit considered and rejected the Third Circuit's conclusion in *Google Cookie Placement* that "intended recipients" are necessarily parties to the communication, regardless of whether the defendant used fraudulent or deceitful practices to induce the communication.[216] In doing so, the Ninth Circuit reiterated that the

209. *Id.* at 599 (quoting *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 934 F.3d 316, 325 (3d Cir. 2019)).

210. *In re Facebook Internet Tracking*, 956 F.3d at 599.

211. *Id.* at 607.

212. *Id.* (noting that the First Circuit in *In re Pharmatrak* held that the defendant's conduct constituted an interception within the meaning of the Wiretap Act); *see also In re* Pharmatrak, Inc., 329 F.3d 9, 12–13, 22–23 (1st Cir. 2003).

213. *See In re* Facebook Internet Tracking, 956 F.3d at 607; *see also* United States v. Szymuszkiewicz, 622 F.3d 701, 703, 707 (7th Cir. 2010).

214. *Id.*

215. *Id.* at 608.

216. *Id.* (citing *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143–44 (3d Cir. 2015) and *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 275 (3d Cir. 2016) for the same).

"paramount objective of the [Wiretap Act] is to protect effectively the privacy of communications."[217] Pointing to the Act's legislative history, the Ninth Circuit determined that Congress intended for the Wiretap Act to prevent unauthorized acquisitions of content by third parties or "unseen auditor[s]."[218] The Ninth Circuit reasoned that "[p]ermitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule."[219] Accordingly, the Ninth Circuit held that "simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception."[220] Thus, the Ninth Circuit concluded that Facebook was not a party to the communications at issue and could be held liable under the Wiretap Act.[221]

IV. RESOLVING THE CIRCUIT SPLIT

The Third and Ninth Circuits' diverging interpretations on how Congress intended for the party exception to apply to those that surreptitiously intercept electronic communications clearly established an irreconcilable circuit split concerning the extent of the Wiretap Act's party exception.[222] Undecided circuit courts are currently confronted with two competing approaches: (1) the Third Circuit's interpretation that the party exception may still apply to entities that use deceptive practices without a criminal or tortious purpose, and (2) the Ninth Circuit's interpretation that the party exception does not apply to entities that employ deceptive data-transmission practices.[223] This part analyzes why the Third Circuit's approach is ultimately the correct one and why the Wiretap Act in its current form is insufficient to protect the privacy interests at stake today.

---

217. *Id.* at 608 (internal quotations omitted) (quoting Joffe v. Google, 746 F.3d 920, 931 (9th Cir. 2013)).

218. *Id.* at 608 (citing S. REP. NO. 90-1097, *reprinted in* 1986 U.S.C.C.A.N. 2112, 2154, 2182).

219. *Id.*

220. *Id.*

221. *Id.*

222. *See id.*; *see also In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 144 (3d Cir. 2015).

223. *See In re Google Cookie Placement*, 806 F.3d at 144; *see also In re Facebook Internet Tracking*, 956 F.3d at 608.

A. The Third Circuit is Correct

Notably, the text of the Wiretap Act does not proscribe deceptive or fraudulent acts, as the Third Circuit pointed out.[224] Instead, the language of § 2511(2)(d) provides only that the party exception does not apply where the communication is intercepted "*for the purpose of committing any criminal or tortious act*."[225] Courts have consistently interpreted this language narrowly, finding that the focus under § 2511(2)(d) is "not upon whether the interception itself violated another law; it is upon whether the purpose for interception—its intended use—was criminal or tortious."[226] In other words, even if the defendant's conduct is criminal or tortious, the party exception may nevertheless apply so long as the defendant lacked the requisite *mens rea*.[227] Accordingly, the plain language of the statute makes clear that the party exception is subject only to the limitation that the intercepting party must not act with a criminal or tortious purpose.

However, because Congress did not define the term "party," courts must still interpret the scope of the term.[228] The Third Circuit rightly pointed out that the Act's legislative history evidences that Congress intended for the term "party" to mean "the person actually participating in the communication."[229] This is consistent with the ordinary meaning of the term, which Merriam-Webster defines as "one (as a person or group) that takes part with others in an action or affair . . . [a] participant."[230] Furthermore, Congress specifically cited to *Pasha* when it explained the

224. *See generally* 18 U.S.C. § 2511.

225. § 2511(2)(d) (providing that it is not unlawful "for a person not acting under color of law to intercept a wire, oral, or electronic communication *where such person is a party to the communication* . . . unless such communication is intercepted for the purpose of committing any criminal or tortious act") (emphasis added).

226. *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 516 (S.D.N.Y. 2001) (internal quotations omitted) (quoting Sussman v. ABC, 186 F.3d 1200 (9th Cir.1999)); *see also In re* Intuit Priv. Litig., 138 F. Supp. 2d 1272, 1279 (C.D. Cal. 2001).

227. *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d at 516.

228. *See* 18 U.S.C. § 2510; *see also In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (9th Cir. 2020).

229. S. REP. NO. 90–1097, at 93–94 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182 (explaining the term within its discussion of § 2511(2)(c), which is identical to § 2511(2)(d) except that it applies to those acting under color of law); *see also In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 144 (3d Cir. 2015).

230. *Party*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1648 (3d ed. 1986) (alteration in original) (emphasis removed).

meaning of the term "party."[231] This is particularly significant because in *Pasha* the Seventh Circuit held that an officer who had misled the sender of a communication by impersonating the intended receiver was nevertheless an "immediate party" to the communication.[232] Congress's reference to *Pasha* suggests that it intended for the party exception to apply to those who directly participate in a communication and may still apply to those who use deceptive practices to gain entrance to the conversation, so long as they do not act with a criminal or tortious purpose.[233]

Congress's 1986 amendment to § 2511(2)(d) was made in response to *Boddie* and supports the proposition that Congress intended for the party exception to apply to those who participate directly in the conversation and may still apply to those who act surreptitiously.[234] In *Boddie*, the defendant reporter secretly recorded his conversation with the plaintiff using hidden cameras and microphones.[235] At the time, the statute provided that the party exception did not apply where the interception was done for the purpose of committing a "criminal, tortious, *or injurious act*."[236] The plaintiff argued that because the defendant surreptitiously recorded the conversation with the intent to cause her injury, he was not entitled to the party privilege.[237] The Court determined that it was a question of fact for the jury whether the defendant intercepted the communication for the purpose of committing an injurious act.[238] Concerned that *Boddie*'s interpretation of "injurious" could be used to chill First Amendment rights, Congress struck out the "other injurious act" wording from the statute.[239] In doing so, Congress recognized that the defendant in *Boddie* had been a party to the communication and expressed concern that the "other injurious act" language could be used in ways that conflicted with First Amendment guarantees.[240] The 1986

231. S. REP. NO. 90–1097, at 93–94 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182; *see also In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d at 144.

232. United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964).

233. *See In re Google Cookie Placement*, 806 F.3d at 144; *see also* Clemons v. Waller, 82 F. App'x 436, 442 (6th Cir. 2003).

234. *See* S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.

235. Boddie v. Am. Broad. Cos., 731 F.2d 333, 335 (6th Cir. 1984).

236. *See id.* at 337–38 (emphasis added) (quoting Meredith v. Gavin, 446 F.2d 794, 798 (8th Cir. 1971)).

237. *Id.* at 338.

238. *Id.*

239. *See* S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571; *see also In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 517 (S.D.N.Y. 2001).

240. *See* S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.

amendment to § 2511(2)(d) is significant, because it demonstrates that Congress intended for the party exception to apply to those who directly participate in the conversation without a criminal or tortious purpose, even if they act deceptively.[241]

Some have asserted that Congress intended to create a special rule for the press where surreptitious recordings are involved and that, for all other defendants, a "tortious purpose" may be established where intentional conduct is later determined to constitute a tort.[242] However, this argument is without merit. The court in *DoubleClick* rightly stated that "[a]lthough Congress deleted 'injurious' purpose from § 2511(2)(d) partly out of concern for press freedom, it in no way indicated that the press enjoyed special standing under the remaining terms of § 2511(2)(d)."[243] If Congress had wanted to create a special rule for the press, it could have done so expressly, but Congress made no such rule when it amended § 2511(2)(d).[244] In interpreting this section, courts have consistently treated media and non-media defendants the same, reasoning that "[Congress] treated journalists just like any other party who tapes conversations surreptitiously."[245] Thus, Congress's decision to strike out the "other injurious act" language rather than create an express carve out for the press indicates that it intended for the party exception to apply to both media and non-media defendants alike who act without a criminal or tortious purpose.[246]

Furthermore, in determining that the First and Seventh Circuits had implicitly assumed that defendants who surreptitiously duplicate communications between two parties are not themselves parties within the meaning of the Wiretap Act,[247] the Ninth Circuit reached a flawed conclusion. The Ninth Circuit based its conclusion largely on its interpretation of the First and Seventh Circuit's reasoning in *Pharmatrak* and *Szymuszkiewicz* respectively.[248] But the defendants in both *Pharmatrak* and *Szymuszkiewicz* were neither active participants in the communications

241. *Id.*
242. *In re DoubleClick*, 154 F. Supp. 2d at 517–18.
243. *Id.* at 517.
244. *Id.* at 517–18; *see also* 18 U.S.C. § 2511(2)(d); S. REP. NO. 99-541, at 17 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.
245. *In re DoubleClick*, 154 F. Supp. 2d at 518 (quoting Sussman v. Am. Broad. Cos., 186 F.3d 1200 (9th Cir. 1999)).
246. *Id.* at 518.
247. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607–08 (9th Cir. 2020).
248. *See id.* at 608.

nor the intended recipients of those communications.[249] Because the term "party" connotes one who actually participates in the communication, it is not surprising that the courts in *Pharmatrak* and *Szymuszkiewicz* did not find those defendants to be parties to the communications.[250] In neither case did the court suggest that it was the defendants' surreptitious conduct that precluded them from being parties to the communication and availing themselves of the party privilege.[251] Thus, the Ninth Circuit's conclusion that the First and Seventh Circuits have implicitly held that "simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception" reaches too far and lacks sufficient support.[252]

Although the Wiretap Act was in large part designed to protect the privacy of communications, Congress placed limitations on that right to privacy.[253] This is evidenced by the fact that § 2511(2)(d) provides for only a one-party consent exception—making it permissible for just one party to consent to an interception without the other's consent or knowledge.[254] Congress understood that it needed to balance privacy interests with other legitimate interests, including First Amendment rights and crime prevention needs.[255] For this reason, the Ninth Circuit's broad holding in *Facebook Internet Tracking* misses the mark.[256] The Third Circuit's reasoning in *Google Cookie Placement*, on the other hand, better captures the nuanced purposes of the Wiretap Act and the party exception that Congress

249. *See In re* Pharmatrak, Inc., 329 F.3d 9, 12 (1st Cir. 2003) (holding that defendant's use of a website traffic monitoring tool to intercept communications between the plaintiffs and the pharmaceutical companies went beyond the pharmaceutical companies' consent); *see also* United States v. Szymuszkiewicz, 622 F.3d 701, 707 (7th Cir. 2010) (holding the defendant liable for intercepting and forwarding his supervisor's emails to his own inbox).

250. *See* S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571; *see also In re Pharmatrak*, 329 F.3d at 12; *see also Szymuszkiewicz*, 622 F.3d at 707.

251. *See generally In re Pharmatrak*, 329 F.3d at 18–22; *see also Szymuszkiewicz*, 622 F.3d at 705–07.

252. *Facebook Internet Tracking*, 956 F.3d at 608; *see generally In re Pharmatrak*, 329 F.3d at 18–22; *see also Szymuszkiewicz*, 622 F.3d at 705–07.

253. *See* S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556; *see also In re Facebook, Inc. Internet Tracking*, 956 F.3d at 607–08.

254. *See* 18 U.S.C. § 2511(2)(d).

255. *See* S. REP. NO. 99-541, at 5, 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559, 3571.

256. *See In re Facebook, Inc. Internet Tracking*, 956 F.3d at 608 ("Simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception[]").

established in order to balance those competing interests.[257] Accordingly, undecided courts should follow the Third Circuit's approach.

B. The Wiretap Act Cannot Protect Modern Privacy Interests

Although the Third Circuit's reasoning provides a more compelling approach, the Ninth Circuit's concern that the party exception could swallow the rule and render permissible some of the most common methods of intrusion is not without force.[258] As people grow increasingly reliant on digital technologies and services, they are increasingly and unavoidably exposed to surveillance and data collection.[259] The extreme wealth generated by the online advertising industry and the rise of surveillance capitalism suggests that companies will continue to exploit opportunities for data collection and implement ever more pervasive surveillance practices.[260] This level of surveillance poses serious threats to individual privacy and harms society by chilling civil liberties and creating great power disparities between "the watcher and the watched."[261] *Google Cookie Placement* provides a clear example of how digital companies can intrude on individual privacy and yet escape liability under the Wiretap Act pursuant to the party exception.[262]

As the aforementioned cases illustrate, the Wiretap Act's one-party consent framework raises complex issues in online contexts.[263] The internet has led to ubiquitous online transactions and communications that often involve numerous parties.[264] This poses line-drawing issues as it becomes increasingly complicated to determine just who is a party to an electronic communication.[265] Legislative history offers some useful insight into how

257. *See* S. REP. NO. 99-541, at 5, 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559, 3571; *see also In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143–45 (3d Cir. 2015).

258. *See In re Facebook, Inc. Internet Tracking*, 956 F.3d at 608.

259. *See* Balkin, *supra* note 118, at 11; *see also* Richards, *supra* note 115, at 1936–38.

260. *See* Zuboff, *supra* note 6, at 75–79.

261. Richards, *supra* note 115, at 1935.

262. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 145 (3d Cir. 2015).

263. *See* Carome, *supra* note 11, at 24–25.

264. *Id.* at 24; *see also* Zuboff, *supra* note 6, at 86.

265. *See* Carome, *supra* note 11, at 24.

Congress intended for the party exception to apply in such cases,[266] but modern electronic communications are far more complex than the two-way telephone conversations that Congress first concerned itself with in 1968.[267] And although Congress attempted to modernize the Wiretap Act in 1986, it did so before the widespread use of the internet and at a time when certain technological advances were not reasonably foreseeable.[268] As a result, the Wiretap Act is difficult to apply to many contemporary digital transactions and provides less privacy protections in those scenarios.[269] This is largely due to the statutory language in § 2511(2)(d), which requires just one of the parties to the communication to consent to an interception.[270] Consequently, the Wiretap Act permits digital companies to intercept and collect increasing amounts of communications without users' knowledge or consent.[271] For these reasons, the Wiretap Act has failed to provide sufficient privacy protections for modern electronic communications sent through online channels.[272]

Given the shortcomings of ECPA, Congress must once again reckon with how to protect privacy interests as new technologies and the proliferation of data collection threaten individual privacy in unprecedented ways.[273] To do this, Congress must limit the scope of the party exception in online environments and consider relevant issues on a case-by-case basis, such as: (1) whether an interception would violate the sender's reasonable expectations of privacy; (2) whether the party has a legitimate interest in intercepting the communication; and (3) whether those legitimate interests, if any, outweigh the sender's reasonable expectations of privacy.[274] But notably these considerations raise other difficult questions about what it means to have a "reasonable expectation of privacy" in today's digital world. Thus, while a newly amended Wiretap Act with stricter limitations

266. *See, e.g.*, S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182; *see also* S. REP. NO. 99-541, at 17 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.

267. *See* Carome, *supra* note 11, at 24.

268. *See* Lupu, *supra* note 38, at ¶¶ 8–9; *see also* Carome, *supra* note 11, at 2.

269. *See* Carome, *supra* note 11, at 25.

270. 18 U.S.C. §2511(2)(d).

271. *See* Zuboff, *supra* note 6, at 83 ("Big Other exists in the absence of legitimate authority and is largely free from detection or sanction.").

272. *See* Zuboff, *supra* note 6, at 83.

273. *See* Balkin, *supra* note 118, at 11–13, 30.

274. *Cf.* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Berger v. New York, 388 U.S. 41, 51 (1967).

on the party exception would help protect privacy interests, such measures cannot fully protect the privacy interests at stake.[275] Congress must therefore enact a comprehensive federal data protection statute that, at a minimum, imposes fiduciary obligations on those that handle personal data.[276]

CONCLUSION

Section 2511(2)(d)'s current statutory language and legislative history make clear that the party exception extends to those that actually participate in the conversation, and even applies to those that act surreptitiously, so long as they do not intercept communications for criminal or tortious purposes.[277] In its analysis, the Third Circuit recognized that § 2511(2)(d) does not proscribe deceptive or fraudulent behavior and made it clear that Congress intended for the term "party" to refer to those who actually participate in the conversation.[278] The Third Circuit's careful approach accurately accounted for the party exception's nuanced purpose under the Wiretap Act. For these reasons, the Third Circuit's understanding of the scope of the party exception is correct, and courts should follow this approach. Still, Congress should heed the concerns of the Ninth Circuit and once again enact new legislation to protect more effectively the privacy interests at stake today.[279] The party exception currently reaches widely across online communications and consequently offers little privacy protections against private actors seeking to collect vast amounts of personal data. Some of the most powerful companies today rely on data-driven business models that increasingly expose people to pervasive surveillance and data collection practices.[280] Simply put, the existing Wiretap Act can no longer offer sufficient privacy protections. Thus, while the Third Circuit's approach is legally correct, it leads to troublesome results that highlight significant loopholes in the current statute and underscore the need for new

275. *See* Balkin, *supra* note 118, at 11–13 (explaining society's increasing dependence on and vulnerability to digital companies).

276. *See* Balkin, *supra* note 118, at 11, 13–16.

277. *See* 18 U.S.C. § 2511(2)(d); *see also* S. REP. NO. 99-541, at 17–18 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.

278. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143–45 (3d Cir. 2015).

279. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020).

280. *See* Zuboff, *supra* note 6, at 75–79.

legislation that appropriately safeguards the long-standing right to privacy in today's digital environment.