Fordham Law Review

Volume 90 | Issue 2 Article 17

2021

Cacophony or Concerto?: Analyzing the Applicability of the Wiretap Act's Party Exception for Duplicate GET Requests

David Koenig
Fordham University School of Law

CACOPHONY OR CONCERTO?: ANALYZING THE APPLICABILITY OF THE WIRETAP ACT'S PARTY EXCEPTION FOR DUPLICATE GET REQUESTS

*David Koenig**

The Electronic Communications Privacy Act ("Wiretap Act") prohibits the intentional interception of an electronic communication. However, "parties to a communication" can intercept a communication without Wiretap Act liability. Parties include the intended recipients of a communication. When internet users navigate the internet, they communicate with websites using GET requests. The users' GET requests call out to websites and websites respond by providing the websites' content to the users. During this process, websites receive user data. This data can include information about the website visited, the search terms used to locate the website, and referral data identifying the last web page the users visited.

Digital advertisers may populate websites users visit with advertisements or plug-ins that allow users to "like" content. In doing so, advertisers generate secondary GET requests between users and advertisers. Secondary GET requests are duplicates of the GET requests between users and websites insofar as they share user data. Advertisers retain and identify this data.

In the Third and Ninth Circuits, internet users argued that digital advertisers used the duplicate GET requests to intercept user data contained in the GET requests between users and websites—arguably a violation of federal law under the Wiretap Act. Digital advertisers invoked the party exception, arguing that advertisers were parties to the duplicate GET request between internet users and advertisers. If so, the advertisers would be parties to the user data received in the duplicate GET requests and exempt from Wiretap Act liability. The Third Circuit held that the party exception applied to the advertisers' duplicate GET requests. The Ninth Circuit rejected this approach and held that the party exception did not apply.

This Note argues that digital advertisers are unintended recipients that are ineligible for the party exception. First, transmitting duplicate user data via

* J.D. Candidate, 2022, Fordham University School of Law; B.A., 2015, University of Washington. Thank you to my friends and family for their support—to whom I wish long, happy, safe, and peaceful lives. My sincere appreciation to the editors and staff of the *Fordham Law Review* for their guidance, encouragement, and expertise.

a second communication is an effective—and sometimes necessary—method of interception for electronic communications on the internet. In that case, duplicate GET requests may indicate interception. This requires courts to analyze shared data, not individual GET requests. Second, equating a direct recipient of a duplicate GET request with an intended recipient lacks judicial support and cannot properly decide party status. Third, users enter URLs or click hyperlinks to navigate the internet. This identifies the websites that users visit as the intended recipients of user data, not digital advertisers. As such, advertisers are best categorized as unintended recipients and therefore ineligible for the Wiretap Act's party exception.

INTRODUCTION

In 1994, one of the first digital advertisements appeared on the internet.[1] Since then, digital advertisers have tailored digital advertising to internet users' individual identities.[2] This process requires vast amounts of user data; data brokers collect thousands of data points on millions of consumers.[3] That user data can be used to tailor digital advertising "based on everything from users' sexual orientations to their moods."[4] The user data necessary for tailored digital advertising has been allegedly collected from emails,[5] the mobile applications that children use,[6] and household appliances like smart televisions.[7]

1. *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr [https://perma.cc/6DJ9-GMZC] (last visited Sept. 17, 2021).

2. Stuart A. Thompson, Opinion, *These Ads Think They Know You*, N.Y. TIMES (Apr. 30, 2019), https://www.nytimes.com/interactive/2019/04/30/opinion/privacy-targeted-advertising.html [https://perma.cc/DW6T-YHU3].

3. *See* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/67SF-PKTN] ("Acxiom maintains its own database on about 190 million individuals and 126 million households in the United States.").

4. Gilad Edelman, *Why Don't We Just Ban Targeted Advertising?*, WIRED (Mar. 22, 2020, 7:00 AM), https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising [https://perma.cc/M6PY-5FQY].

5. Claire Cain Miller, *Google Accused of Wiretapping in Gmail Scans*, N.Y. TIMES (Oct. 1, 2013), https://www.nytimes.com/2013/10/02/technology/google-accused-of-wiretapping-in-gmail-scans.html [https://perma.cc/T9HG-L94K].

6. McDonald v. Kiloo APS, 385 F. Supp. 3d 1022, 1029–30 (N.D. Cal. 2019) (describing allegations that the defendants tracked and collected children's personal data from mobile devices).

7. *In re* Vizio, Inc., Consumer Priv. Litig., 238 F. Supp. 3d 1204, 1212 (C.D. Cal. 2017) ("Plaintiffs allege that, unbeknownst to them, Vizio's Smart TVs . . . collect and report consumers' content viewing histories.").

The process of collecting user data can begin with something as simple as an internet user browsing the internet.[8] In its essential form, the internet is built on a series of technical conversations.[9] A typical internet user accesses internet shopping, social media, news, and a myriad of digital content by visiting websites served to a user via GET requests.[10]

The GET request is a digital call and response; an internet user's web browser calls out to the user's intended destination—a particular website.[11] The website responds to the user's GET request by displaying the website's content.[12] The user and website communicate digitally and, in the process, exchange data.[13]

For example, a user visits *The New York Times* online.[14] The user enters *The New York Times*'s URL into a web browser.[15] This generates a GET request that is sent to *The New York Times*.[16] *The New York Times* responds by providing access to the website.[17]

At the same time, additional conversations can be created because of the code that Facebook, Google, and other digital advertisers embed in the websites that users visit.[18] The code creates a secondary GET request directing a user's web browser to contact the digital advertisers.[19] Notably, this secondary GET request ("duplicate GET request") is a duplicate of the first GET request insofar as the secondary request shares user data with the

8. Daniel B. Garrie & Rebecca Wong, *Demystifying Clickstream Data: A European and U.S. Perspective*, 20 EMORY INT'L L. REV. 563, 565–66 (2006) (describing user data collected by visiting websites).

9. Notwithstanding this Note's simplification, accessing a website is more complicated. The process may generate forty-eight technical inquiries. Dan Luu, *What Happens When You Load a URL?*, https://www.danluu.com/navigate-url [https://perma.cc/G64R-9BJ6] (last visited Sept. 17, 2021).

10. *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 268 (3d Cir. 2016) ("When a person uses a web browser to access a website, the browser sends a 'GET' request to the server.").

11. *See generally Client-Server Overview*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Client-Server_overview [https://perma.cc/8WVR-J7Z9] (last visited Sept.17, 2021) ("You can make a simple GET request by clicking on a link . . . . [The response] contains the actual [website] HTML returned by the request.").

12. *Id.*

13. *See* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *3 (N.D. Ill. Mar. 5, 2018) (finding identifiable data in URLs); *see also infra* notes 26–29 and accompanying text (outlining the identifiable data in GET requests, including the aforementioned URLs).

14. Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001) (explaining step-by-step how a user would access nytimes.com via a GET request sent between a user and the website).

15. *See id.*

16. *See id.*

17. *See id.*

18. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596 (9th Cir. 2020) (explaining that Facebook embeds a "like" button containing Facebook code on affiliated websites).

19. *Chance*, 165 F. Supp. 2d at 1156 (explaining that the initial communication between a user and a website can generate an additional communication used to contact a digital advertiser).

first request.[20] This duplicate GET request not only delivers digital advertisements but also transmits the duplicate user data to the advertisers.[21]

In the example, *The New York Times* responds to a user's original GET request with access to its homepage, and an advertiser's embedded code also directs a user's web browser to contact advertisers using a duplicate GET request.[22] The digital advertisers fill advertising space on *The New York Times*'s website.[23] This duplicate GET request calls out to advertisers and the advertisers respond by serving digital advertisements.[24]

For an advertiser, user data is important because it can be monetized.[25] The duplicate GET request transmits the URL a user entered.[26] This identifies users' web browsing histories.[27] A duplicate GET request can also include user data identifying the search terms a user queried in order to locate the website[28] or referral information identifying the last webpage a user visited.[29] Because duplicate GET requests contain the same user data as the GET request between users and websites, advertisers can see user data they

20. *See In re Facebook*, 956 F.3d at 607 ("Facebook's code directs the user's browser to copy the referer [sic] header from the GET request and then send a separate but identical GET request and its associated referer [sic] header to Facebook's server."); *see also* Brown v. Google L.L.C., No. 20-CV-03664, 2021 WL 949372, at *1 n.1 (N.D. Cal. Mar. 12, 2021) (referring to these secondary GET requests as "duplicate GET requests" and noting that *In re Facebook* and *In re Google* also included duplicate GET requests).

21. *Id.* at 596.

22. *See* Russell A. Miller, *The Legal Fate of Internet Ad-Blocking*, 24 B.U. J. SCI. & TECH. L. 299, 313 (2018) ("The user's browser responds to these secondary get-requests by calling for . . . subsidiary content, such as advertising."); *Chance*, 165 F. Supp. 2d at 1156.

23. *Chance*, 165 F. Supp. 2d at 1156.

24. *Id.* ("This communication instructs Avenue A's server to send the computer a banner advertisement to fill the blank space on the nytimes.com home page.").

25. *See In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 266 (3d Cir. 2016) (noting that data powers "trackers, cookies, and algorithms designed to capture and monetize the information").

26. *See* Orin Kerr, *Websurfing and the Wiretap Act*, WASH. POST (June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act [https://perma.cc/U9J4-NBT6] (providing legal commentary on pending GET request litigation and considering the Wiretap Act implications—if any—of a technical process that concededly leads to the "disclosure of URLs to . . . third party sites.").

27. United States v. Forrester, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (concluding that URLs reveals users' internet activity).

28. Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *3 (N.D. Ill. Mar. 5, 2018) ("[I]f a user searches for 'The Few, The Proud' on Google, the resulting URL contains 'the+few+the+proud' . . . ."); *Client-Server Overview*, *supra* note 11 (providing an illustrative GET request that includes queried search terms "client+server+overview" within the GET request).

29. Burak Guzel, *HTTP Headers for Dummies*, ENVATOTUTS+ (May 12, 2021), https://code.tutsplus.com/tutorials/http-headers-for-dummies--net-8039 [https://perma.cc/6AFS-63WS] ("The remainder of the request contains . . . various information about the . . . request . . . . [I]f there was a referring [URL], that would have been in the [request] too.").

might not otherwise have access to.[30] Advertisers can store and identify this duplicate user data.[31]

Internet users argue that the code generating a duplicate GET request intercepts communications between internet users and the websites that the internet users visit.[32] This redirects a cacophony of user data to the advertisers.[33] Advertisers respond that the internet users' GET requests sent to websites generate a concerto of exempt GET requests intended for the digital advertisers.[34] These additional GET requests are necessary in order to assemble websites built on the advertisers' content.[35]

If internet users are correct, digital advertisers may have accessed a communication between users and websites as an eavesdropper.[36] If that is so, advertisers are one step closer to wiretap liability.[37] If advertisers are correct, a duplicate GET request creates an entirely new communication between users and advertisers.[38] As a consequence, the new communication would be exempt and the duplicate user data legally insignificant.[39]

From a statutory perspective, internet users and advertisers disagree about whether the Wiretap Act's party exception should apply to the duplicate GET requests that the digital advertisers generate.[40] According to the Wiretap Act's party exception, eavesdroppers are liable for interception while parties to a communication are not.[41] Circuit courts disagree regarding whether the

30. *Id.*; *see also Forrester*, 512 F.3d at 511 n.6 ("[Capturing] URLs would also divulge the particular articles . . . viewed."); *In re* Application of U.S. for A Pen Reg., 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

31. *In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001) (establishing that cookies can retain GET data).

32. *See generally* Brief for Plaintiffs-Appellants at 44–48, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020) (No. 17-17486), 2018 WL 313496, at *44–48 (arguing in favor of a prima facie claim of unlawful wiretap interception in GET litigation).

33. *See id.*

34. Answering Brief of Defendant-Appellee Google, Inc. at 5–6, *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125 (3d Cir. 2015) (No. 13-4300), 2014 WL 1413954, at *5–6. ("[S]ending of [information contained within a GET request] is inherent to the Internet browsing process . . . .").

35. Websites are assembled from content found elsewhere on the internet; GET requests assemble the content in one place. *Id.*

36. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020) (reserving judgment on the other elements of a successful wiretap claim but declining to exempt the defendant from interception liability as a matter of law).

37. *See* 18 U.S.C. § 2511(1)(a) (prohibiting the intentional interception of "any . . . electronic communication").

38. *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (finding that an intended recipient of a duplicate communication becomes a party to that communication and cannot be liable for a Wiretap Act violation).

39. *Id.*

40. *See* 18 U.S.C. § 2511(2)(d); *In re Google Inc.*, 806 F.3d at 143 (assessing whether the Wiretap Act's party exception applies where a defendant allegedly intercepted data via GET request).

41. Warden v. Kahn, 160 Cal. Rptr. 473, 475 (Ct. App. 1979) (finding wiretap interception liability for eavesdroppers but not for parties); *In re Facebook*, 956 F.3d at 607 (confirming that *Warden* properly interprets party exception applicability to eavesdroppers in the context of federal law because the state exception in *Warden* is equivalent to the federal exception).

party exception applies to duplicate GET requests.[42] Advertisers and users are left asking if duplicate GET requests are evidence of unlawful interception or legally exempt.[43]

This Note focuses on the party exception to the Wiretap Act[44] and analyzes whether a digital advertiser who receives a duplicate GET request containing the same data as another GET request is potentially liable under the Wiretap Act or legally exempt under the Wiretap Act's statutory party exception.[45]

Part I examines the emergence of wiretap surveillance, the legislative history of federal wiretap protections, and the extension of those protections to electronic communications. Part I further considers a prima facie Wiretap Act claim and the statutory liability exceptions available to wiretap defendants.

Part II provides an in-depth analysis of the party exception to the Wiretap Act. It describes a typical party analysis by identifying two paths to party status—affirmative acts and recipient status. It also considers two other factors that can influence a typical party analysis—a recipient's behavior and how a court defines the scope of a protected communication.

Part III examines the circuit split on duplicate GET requests and the party exception. First, it considers the Third Circuit's decision concluding that the party exception applied. Then, it highlights First and Seventh Circuit decisions that established doctrine for a contrary approach. Finally, it reviews the Ninth Circuit's analysis of duplicate GET requests in a decision in which the court held that the party exception did not apply.

Part IV contends that advertisers that receive duplicate GET requests are ineligible for the party exception. It argues that when a duplicate GET request contains the same user data as another GET request, the shared data should be the focus of a court's party analysis. Then, Part IV suggests that direct receipt of a GET request cannot properly decide party status. Part IV concludes that when a duplicate GET request's data is analyzed, advertisers are ineligible for a party exception.

I. A BRIEF HISTORY OF WIRETAPPING AND WIRETAP PROTECTIONS

Part I.A details the origins of wiretapping and the legislative response prohibiting the practice of wiretapping. Part I.B examines the extension of wiretap protections to electronic communications. Part I.C identifies the statutory elements of a wiretap violation. Part I.D highlights statutory exceptions to wiretap liability, including the party exception.

---

42. *Compare In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020) (finding that the party exception did not apply to GET request litigation), *with In re Google Inc.*, 806 F.3d at 145 (finding the party exception did apply). *See generally* Brianna Vollman, *Cookie Monster: Facebook Sued Under Wiretap Act*, U. CIN. L. REV. (June 2, 2020), https://uclawreview.org/2020/06/02/cookie-monster-facebook-sued-under-wiretap-act [https://perma.cc/3UKJ-3B7P] (outlining the circuit split regarding GET request litigation detailed in this Note).

43. *See supra* note 42 and accompanying text.

44. *See supra* notes 40–42 and accompanying text.

45. *See supra* notes 36–42 and accompanying text.

A. Emergence of Wiretapping and the Legislative Response

When the telegraph was invented in 1844, it allowed parties to send and receive messages across long distances.[46] Soon thereafter, telegrams were routinely intercepted by splicing telegraph wires and intercepting the messages contained within.[47]

State law enforcement began wiretapping telegrams and telephones in order to aid in criminal investigations; the process of intercepting these communications became a useful alternative to paying criminal informants.[48] By 1938, government and private wiretapping had proliferated, and public outcry had grown, but federal law did not prohibit wiretap interception.[49] In these early days of wiretap interception, disclosing information obtained by wiretap was prohibited, but wiretap interception itself was not.[50] The U.S. Supreme Court clarified the legality of wiretapping in *Katz v. United States*.[51] *Katz* prohibited government wiretaps when the wiretap would violate Fourth Amendment protections against unlawful searches and seizures.[52]

In quick order, Congress enacted the first substantive federal protections against private wiretapping in the Omnibus Crime Control and Safe Streets Act of 1968[53] ("Omnibus Act"). In addition to outlining procedures for government wiretapping that complied with the *Katz* ruling, the Omnibus Act prohibited private actors from intercepting "any wire . . . communication."[54] The Omnibus Act treated private surveillance differently than government surveillance and found that private surveillance had "little [legal] justification."[55] Accordingly, the Omnibus Act implemented a "blanket prohibition" outlawing private wiretapping—thus protecting wire and oral communications.[56]

---

46. Alex Markels, *Timeline: Wiretaps' Use and Abuse*, NPR (Dec. 20, 2005, 12:00 AM), https://www.npr.org/templates/story/story.php?storyId=5061834 [https://perma.cc/3H43-VXLD].

47. Hereinafter, "wiretapping" is used to refer to the process of interception. Michael Pollak, *A Short History of Wiretapping*, N.Y. TIMES (Feb. 28, 2015), https://www.nytimes.com/2015/03/01/nyregion/a-short-history-of-wiretapping.html [https://perma.cc/E36D-29QD] (describing the interception of telegrams by wiretap).

48. Meyer Berger, *Tapping the Wires*, NEW YORKER (June 18, 1938), https://www.newyorker.com/magazine/1938/06/18/tapping-the-wires [https://perma.cc/7S8E-PS2Q].

49. *Id.* ("[L]awyers . . . have worked hard for federal legislation against wire-tapping, but their efforts have always failed.").

50. Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103–04 (codified as amended at 47 U.S.C. § 605) (prohibiting the disclosure of wiretapped communications).

51. 389 U.S. 347 (1967).

52. *See id.* at 353.

53. Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of the U.S.C.).

54. *Id.* § 2511, 82 Stat. at 213.

55. S. REP. NO. 90-1097, at 69 (1968) ("Virtually all concede that the use of wiretapping . . . by private unauthorized hands has little justification where communications are intercepted without the consent of one of the participants.").

56. *Id.* at 91.

That said, the "blanket prohibition" included caveats. The Omnibus Act introduced important statutory exceptions—including the party exception—that remain in effect today.[57] The party exception provided that, "[i]t shall not be unlawful . . . for a person . . . to intercept a wire or oral communication where such person is a party to the communication."[58]

B. Updating Wiretap Protections for Modern Technologies

Despite these newfound statutory protections, the Omnibus Act did not account for the development of technologies that changed how people communicate with one another. The Omnibus Act was concerned with oral conversations that were intercepted using recording devices[59] and oftentimes transmitted greater distances using telephone lines[60] and via radio communications.[61] By 1986, new technology enabled wireless telephone conversations via cellular technology and non-oral electronic communication via the internet's transmission of data.[62] The fledgling internet allowed companies to transmit company data digitally and enabled individuals to communicate using email.[63] Neither form of communication was protected by existing federal law.[64]

Acknowledging this gap in federal wiretap protections, Congress enacted the Electronic Communications Privacy Act[65] ("Wiretap Act"). The Wiretap Act amended the Omnibus Act to clarify and expand "privacy protections and standards" by addressing modern technologies.[66] The Wiretap Act included federal protections for electronic communications.[67] The party exception reappeared in the Wiretap Act. Intercepting an "electronic communication where such person is a party to the communication" was legally exempt according to the Wiretap Act.[68] The Wiretap Act's legislative

57. *See* 18 U.S.C. § 2511(2)(d).

58. Omnibus Crime Control and Safe Streets of 1968, Pub. L. No. 90-351, § 2511, 82 Stat. 197, 214.

59. S. REP. NO. 90-1097, at 94–95 (detailing congressional concern with disguised devices used to intercept oral communications).

60. *Id.* at 92 (highlighting the statute's prohibition of wiretap interception leveraging the use of telephone line surveillance).

61. *Id.* (detailing the statute's equivalent prohibition of wiretap interception leveraging the use of radio communications).

62. S. REP. NO. 99-541, at 2 ("Today we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing.").

63. *Id.* at 8.

64. *Id.* at 5 (conceding that no federal law protected modern telecommunications like the internet from wiretap interception).

65. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

66. S. REP. NO. 99-541, at 1.

67. 18 U.S.C. § 2511(1)(a); *see also In re* Matter of Search Warrant for [redacted].com, 248 F. Supp. 3d 970, 974 (C.D. Cal. 2017) (surveying the legislative purpose of the Wiretap Act).

68. H.R. REP. NO. 99-647, at 85 (1986).

history reveals that Congress remained concerned with unauthorized private persons accessing "communications to which they were not a party."[69]

C. Outlining a Prima Facie Wiretap Act Claim

This Note analyzes whether the Wiretap Act's party exception applies to a duplicate GET request received by advertisers when that duplicate request shares data with GET request sent between users and websites.[70] For clarity, this Note first considers the elements of a prima facie Wiretap Act claim.

The Wiretap Act prohibits the intentional interception of an electronic communication.[71] In order to plead a successful wiretap claim, a plaintiff must allege that the defendant "(1) intentionally (2) intercepted . . . (3) the contents of (4) an electronic communication, (5) using a device."[72]

Interception is intentional when the defendant had knowledge of the interception or it was the defendant's conscious objective to intercept the communication.[73] Interception is unintentional when the defendant intercepts a communication by mistake or by accident.[74] The circuit split discussed in this Note addresses digital advertisers allegedly embedding code on websites; that code ultimately generates the duplicate GET requests.[75] This indicates intentional conduct, whether or not wiretap liability exists.

Interception also requires the acquisition of a communication's contents.[76] Content is defined as the "information concerning the substance, purport, or meaning of that communication."[77] Acquiring a GET request can meet this requirement when it contains URL data identifying a user's queried search terms[78] or the particular web page users visit.[79]

---

69. *Id.* at 19.

70. *See supra* notes 32–45 and accompanying text.

71. 18 U.S.C. § 2511(1)(a).

72. White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *5 (D.N.J. Aug. 21, 2019).

73. *In re* Pharmatrak, Inc., 329 F.3d 9, 23 (1st Cir. 2003) ("An 'intentional' state of mind . . . [can mean] the result of one's conduct if such conduct or result is one's conscious objective." (quoting S. REP. NO. 99-541, at 23 (1986))); Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014) (holding that Apple's knowledge qualified as intent).

74. *Backhaut*, 74 F. Supp. 3d at 1044 ("Interceptions that are the product of inadvertence or mistake are insufficient . . . .").

75. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596 (9th Cir. 2020) ("Facebook facilitated [the tracking of users] by embedding third-party plug-ins on . . . web pages.).

76. Zak v. Bose Corp., No. 17-CV-02928, 2020 WL 2762552, at *2 (N.D. Ill. May 27, 2020) (outlining prima facie elements).

77. DIRECTV, Inc. v. Boonstra, 302 F. Supp. 2d 822, 827 (W.D. Mich. 2004) (quoting 18 U.S.C. § 2510(8)).

78. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 139 (3d Cir. 2015) (considering the content element in GET request litigation and concluding "we are persuaded that—at a minimum—some queried URLs qualify").

79. *Id.* at 138; United States v. Forrester, 512 F.3d 500, 511 n.6 (9th Cir. 2008) ("A URL . . . identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity."); *see supra* notes 26–29 and accompanying text (confirming that GET requests can contain these URLs).

An "electronic communication" is "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."[80] The data exchanged between users and websites qualifies.[81] The Third and Ninth Circuits did not question a GET request's status as an electronic communication.[82] Accordingly, this Note does not question a GET request's status as an electronic communication.

Finally, a communication must be intercepted using "a device."[83] The Third Circuit was unable to identify a device that could intercept the user data of a GET request sent between users and websites.[84] Other courts recognize that the device is a second communication that contains duplicate data or—at a minimum—that the web servers facilitating a second communication qualify as the device.[85] This Note agrees: a duplicate GET request powered by the defendant's web servers is the device.[86]

D. Statutory Exceptions to Wiretap Act Liability

A prima facie wiretap claim must also account for the Wiretap Act's statutory exceptions. This includes exceptions for law enforcement[87] and interception as an incident in the ordinary course of business.[88] Notably, consent to interception can exempt the accused from liability.[89] If an internet user communicates with a website and the website consents to an advertiser intercepting the communication, an advertiser is free from liability.[90] For that reason, consent can exempt an advertiser from liability.[91]

---

80. 18 U.S.C. § 2510(12).

81. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

82. *See generally In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020); *In re Google Inc.*, 806 F.3d 125.

83. 18 U.S.C. § 2510(4).

84. *See In re Google*, 806 F.3d at 141–42.

85. *See In re* Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003) ("[I]t is clear that Pharmatrak relied on devices such as its web servers to capture information from users."); *see also* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *6 n.5 (N.D. Ill. 2018) (concluding that the defendant has employed an "artifice" to receive the allegedly intercepted communications).

86. *See infra* Part IV.A.

87. 18 U.S.C. § 2511(2)(c).

88. *Id.* § 2511(2)(a)(i). Incidentally, a federal district court in the Northern District of California rejected an ordinary course of business exception for a wiretap claim involving GET requests. Brown v. Google L.L.C., No. 20-CV-03664, 2021 WL 949372, at *15 (N.D. Cal. Mar. 12, 2021) ("Sending a duplicate GET request to Google neither facilitates nor is incidental [to] the communication that Plaintiffs allege was intercepted—in this case, the communication between the user's computer and the website.").

89. *In re Pharmatrak*, 329 F.3d at 19–20.

90. 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful . . . where one of the parties to the communication has given prior consent . . . unless such communication is intercepted for the purpose of committing any criminal or tortious act . . . .").

91. *See generally In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (exempting liability with consent).

Consent is not foolproof. An eavesdropper may fail to get consent from the websites that users visit.[92] If an eavesdropper asks for consent, they may fail to adequately disclose the extent of data collection, rendering consent invalid.[93] Each statutory exception is analyzed on its own merit.[94] Circuit courts still disagree on whether the party exception applies to duplicate GET requests.[95] As a result, party exception applicability remains relevant and is thus this Note's focus. According to that exception, a person who intercepts an "electronic communication where such person is a party to the communication" is exempt from Wiretap Act liability as a matter of law.[96]

II. NAVIGATING THE WIRETAP ACT'S PARTY EXCEPTION ANALYSIS

Part II outlines how courts conduct a party exception analysis. Part II.A identifies two ways a defendant can become an exempt party. This includes affirmative acts in Part II.A.1 or recipient status in Part II.A.2. Part II.B distinguishes between intended and unintended recipients using two analytical methods. Part II.B.1 analyzes manifestations of sender intent. Part II.B.2 analyzes a communication's intended destination. Part II.C highlights how a recipient's behavior can also distinguish between intended and unintended recipients. This recipient behavior includes manufactured recipients, discussed in Part II.C.1, and surreptitious listeners, discussed in Part II.C.2. Part II.D examines how the scope of a communication affects party status.

A. Identifying Parties: Affirmative Acts and Recipients

The parties to a communication are exempt from liability under the Wiretap Act.[97] Digital advertisers can become an exempt party through affirmative acts[98] or recipient status.[99]

1. Path One: Affirmative Acts May Indicate Party Status

The Second Circuit held in *Caro v. Weintraub*[100] that a defendant's affirmative acts can grant exempt party status under the Wiretap Act.[101]

92. *See In re Pharmatrak*, 329 F.3d at 20.

93. Brown v. Google L.L.C., No. 20-CV-03664, 2021 WL 949372, at *11 (N.D. Cal. Mar. 12, 2021) ("[E]ven assuming that Google has established that websites generally consented to the interception of their communications with users, Google does not demonstrate that websites consented to . . . interception of communications with users who were in private browsing mode.").

94. *See* Ali v. Douglas Cable Commc'ns, 929 F. Supp. 1362, 1376–77 (D. Kan. 1996) (analyzing two statutory exceptions distinctly).

95. *See supra* notes 36–42 and accompanying text.

96. 18 U.S.C. § 2511(2)(d).

97. *Id*. ("It shall not be unlawful . . . where such person is a party to the communication . . . .").

98. *See infra* Part II.A.1.

99. *See infra* Part II.A.2.

100. 618 F.3d 94 (2d Cir. 2010).

101. *See id.* at 97–98.

Caro involved a conversation across a kitchen table.[102] The defendant engaged in conversation and recorded the exchange with his phone.[103] The *Caro* court had to decide whether the recording was wiretap interception or exempt because the defendant was a party to the conversation.[104]

In order to identify the parties, the court in *Caro* analyzed the defendant's behavior. The court held that the defendant was a party because of his affirmative acts: namely, participation in the conversation.[105] By participating in the conversation, the defendant was deemed an exempt party.[106] This is consistent with the legislative history for wiretap laws.[107] By this metric, participation can accord exempt party status.[108]

The reach of affirmative acts extends well beyond the kitchen table. In *Zak v. Bose*,[109] the court considered a mobile application that allowed users to play music and view information about the users' selected songs.[110] By design, the Bose application responded to users' song requests in order to play the songs and display the information expected.[111] In *Zak*, active participation became the cornerstone of a party status analysis.[112] By virtue of the Bose application's functionality, the court concluded that Bose was a "known participant" in the communication, and this established Bose as an exempt party.[113]

Participation in a communication may also be framed in terms of sender and recipient.[114] In *United States v. Szymuszkiewicz*,[115] the Seventh Circuit analyzed email transmissions by describing the movement of email communications as those that were sent from "sender to recipient."[116] This terminology enabled the court to conclude, on other grounds, that the defendant was best characterized as neither. Instead, the defendant was a

---

102. *Id.* at 96.

103. *Id.*

104. *Id.* at 97–98 (reviewing de novo the district court's ruling that the defendant was a party to the conversation at issue).

105. *Id.* at 98 (noting that the defendant "spoke up a few times urging [Caro] to continue" and determining that "[t]hose facts [we]re sufficient to establish that David was a party to the conversation").

106. *Id.* at 97 ("[A] party to the conversation is one who takes part in the conversation . . . .").

107. *See* S. REP. NO. 90-1097, at 94 (1968) ("'[P]arty' would mean the person actually participating in the communication.").

108. *See id.*

109. No. 17-CV-02928, 2019 WL 1437909 (N.D. Ill. Mar. 31, 2019).

110. *Id.* at *1.

111. *Id.*

112. *Id.* at *3 ("[T]he relevant inquiry is whether the defendant is a participant in the conversation, as opposed to a non-participant that uses other means to gain access . . . .").

113. *Id.* at *3–4. (finding that receiving and displaying user media was the primary function of the application and this established that the defendant was eligible for party status).

114. *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (supporting this framework by identifying paradigmatic parties as "the speaker and/or sender, and at least one intended recipient").

115. 622 F.3d 701 (7th Cir. 2010).

116. *Id.* at 705 (analyzing defendant's defense on other grounds by framing a communication as between a sender and a recipient).

"spy," who accessed "nonpublic" emails and was thus subject to the Wiretap Act's unlawful interception liability.[117]

2. Path Two: Recipients May Qualify for Party Status

The *Szymuszkiewicz* analysis identified two parties to a communication: the sender and the recipient of an email.[118] Recipient status is the second path to becoming a party. In this view, a party also includes the person to whom, or the entity at which, a conversation is directed.[119] Protected communications will always include at least one sender and one recipient.[120] Without at least one identifiable sender and recipient, there might not be a protected communication at all.[121]

People v. Herrington,[122] an Illinois state court case, is illustrative in this regard: in a simple conversation, words are spoken by one person and directed toward another.[123] *Herrington* held that the person on the receiving end of a conversation can record without liability.[124] For example, an internet user might visit *The New York Times*'s online website.[125] Via transmission of electronic data, the internet user's computer is speaking and directing this conversation to the website.[126] Thus, the website becomes an exempt party because the website is the recipient of the user's communication.[127]

In re Nickelodeon Consumer Privacy Litigation[128] and *Allen v. Quicken Loans Inc.*[129] confirm that in the sphere of electronic communications, the websites that users intend to communicate with are prime examples of exempt recipients. By navigating to the Nickelodeon website owned by

117. *See id.* at 705, 707 (implying that the defendant qualifies as neither sender nor recipient by straying from the sender and recipient terminology to label the defendant as a "spy" and concluding that the defendant had accessed "nonpublic" emails).

118. *See supra* notes 116–17 and accompanying text.

119. *See* People v. Herrington, 645 N.E.2d 957, 958–59 (Ill. 1994).

120. *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (concluding that a communication will always include at least one sender and one recipient).

121. *See* Jurgens v. Build.com, Inc., No. 4:17-CV-00783, 2017 WL 5277679, at *6 (E.D. Mo. Nov. 13, 2017) (noting that if a plaintiff cannot identify an alleged communication's recipient, then no communication exists at all for Wiretap Act protection).

122. 645 N.E.2d 957 (Ill. 1994).

123. *See id.* at 958–59; *see also* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *3 (N.D. Ill. Mar. 5, 2018) (affirming that *Herrington*'s Illinois state law interpretation of party status "comports with the meaning of party under the Wiretap Act" and with the Third Circuit's interpretation.).

124. *Id.* at 959 (holding that a party can record a conversation where the recording was of a conversation the party would otherwise hear by virtue of having the conversation at all).

125. *See supra* notes 22–24 and accompanying text.

126. *See supra* notes 22–24 and accompanying text.

127. *See In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) (finding that the websites users visit are parties to the digital communications sent from these users).

128. 827 F.3d 262 (3d Cir. 2016).

129. No. 17-12352, 2018 WL 5874088 (D.N.J. Nov. 9, 2018).

Viacom, users made Viacom a party to the electronic communication.[130] Likewise, the plaintiff in *Allen* admitted that an allegedly intercepted electronic communication took place on Quicken's website; this admission established that Quicken was a party to the communication.[131]

In sum, defendants can claim party status via affirmative acts including participation as the sender or recipient of a communication.[132] Claiming recipient status may be the preferred path for digital advertisers generating duplicate GET requests and directing this data toward themselves.[133] Advertisers may argue that they are the recipients of users' GET requests and recipients are exempt parties per the party exception.[134]

B. Distinguishing Between Intended and Unintended Recipients

However, not all recipients qualify as parties. Intended recipients qualify for party status, but unintended recipients do not.[135] Therefore, it becomes important to determine whether digital advertisers are intended or unintended recipients.[136]

The person someone intends to talk to is an intended recipient.[137] A mobile application a user intends to engage with qualifies, too.[138] So do the websites a user intends to visit.[139] Despite the various examples of intended recipients, courts may disagree over how to identify an intended recipient. Some courts focus on manifestations of sender intent.[140] Other courts ask whether a communication reached its intended destination.[141] Part IV

130. *See In re Nickelodeon Consumer*, 827 F.3d at 267, 274 (establishing that the communications occurred on "Viacom's websites" and then deciding outright that Viacom was a party).

131. *See Allen*, 2018 WL 5874088, at *4 ("[A]ll relevant communications occurred on Quicken's Website, making Quicken the intended recipient (and a party) to the communications.").

132. *See* Caro v. Weintraub, 618 F.3d 94, 97–98 (2d Cir. 2010); *see also Allen*, 2018 WL 5874088, at *4 (agreeing that defendants were eligible for a party exception).

133. *See* Answering Brief of Defendant-Appellee at 5–6, *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125 (3d Cir. 2015) (No. 13-4300), 2014 WL 1413954, *5–6.

134. *Id.* at *35–36.

135. *Compare* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (holding that the defendant was a party to the communication because it "merely received the information transferred to it"), *with* Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1042–43 (N.D. Cal. 2014) (denying a motion to dismiss where a complaint alleged messages were not addressed to Apple).

136. *Compare In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020), *with In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125 (3d Cir. 2015).

137. *See* People v. Herrington, 645 N.E.2d 957, 959 (Ill. 1994) (quoting Bender v. Board of Fire & Police Comm'rs, 539 N.E. 2d 234, 236 (Ill. App. Ct. 1989) (affirming that when a statement is "made or directed" toward someone, that person becomes an exempt party).

138. *See supra* notes 109–13 and accompanying text.

139. *See In re* DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 513–14 (S.D.N.Y. 2001) (concluding, as a preliminary matter, that the websites associated with an advertiser are parties to a communication capable of consenting to advertiser interception).

140. *See infra* notes 142–57, 170–73 and accompanying text.

141. *See infra* notes 158–69 and accompanying text.

analyzes data in an advertiser's duplicate GET request using both approaches, so both approaches are considered here.

1. Analyzing Manifestations of Sender Intent

A federal district court in the Northern District of Illinois, in *Vasil v. Kiip, Inc.*,[142] identified the intended recipient by crediting manifestations of sender intent on a motion to dismiss. While the *Vasil* federal wiretap claim failed on other grounds, the recipient analysis was applied to an Illinois state law claim that defined parties identically to the federal Wiretap Act's definition of an exempt party.[143] The court asked who the sender of a communication intended to communicate with—if anyone—and then asked if that plaintiff-sender intent included the defendant.[144] At the dismissal stage, it was enough that the plaintiff-senders of the communication alleged that they intended to communicate with no one at all.[145] Hence, the senders could not have intended to communicate with *Vasil*'s defendant, and party status failed.[146]

Likewise, in *Backhaut v. Apple*,[147] a federal district court in the Northern District of California found it telling that the senders' intended recipients were clearly identified.[148] Senders addressed text messages to particular recipients, none of whom included Apple.[149] In *Lopez v. Apple, Inc.*,[150] the court, also in the Northern District of California, considered whether Apple was an intended recipient of users' audio communications.[151] Allegedly, user audio was inadvertently sent to Apple via Apple's Siri virtual assistant.[152] Though the claim failed on other grounds, the court, by assessing the senders' manifestations of intent, rejected Apple's defense that it was an exempt intended recipient.[153]

First, on a motion to dismiss, the court credited users' allegations that they did not intend to communicate with Apple.[154] Second, the court inferred the senders' intent: conversations between users and their doctors, business

142. No. 16-CV-09937, 2018 WL 1156328 (N.D. Ill. Mar. 5, 2018).

143. *Id.* at *6. (defining parties under Illinois state law to match the definition as it appears within the Wiretap Act).

144. *See id.*

145. *See id.* ("[P]laintiffs never intended, the complaint alleges, to communicate information to Kiip (or anyone else) when not using the Runkeeper app, so Kiip could not have been a party to a communication of data . . . that Kiip engineered . . . .").

146. *See id.*

147. 74 F. Supp. 3d 1033 (N.D. Cal. 2014).

148. *See id.* at 1043 (crediting plaintiff's allegation that text messages "not addressed or directed to Apple" was sufficient for a viable wiretap claim on a motion to dismiss).

149. *Id.*

150. No. 19-04577, 2021 WL 823122 (N.D. Cal. Feb. 10, 2021).

151. *Id.* at *4 ("Apple argues . . . that it has not 'intercepted' communications because it was the intended recipient.").

152. *Id.* at *1.

153. *Id.* at *4–5.

154. *Id.* at *4 ("Plaintiffs allege that they did not intend Apple to receive their private communications, but that Apple 'captured' such communications using the software in their devices. That sufficiently alleges interception.").

associates, and sexual partners were intended for "doctors, business partners and sexual partners respectively—not Apple."[155]

In *Vasil*, *Backhaut*, and *Lopez*, the courts declined to extend intended recipient status to defendants where the senders of the communications did not intend for the defendants to receive the allegedly intercepted communications.[156] At the dismissal stage, alleged sender intent was enough to defeat party status.[157]

2. Analyzing a Communication's Intended Destination

In contrast, other courts focus on a communication's intended destination.[158] In the Seventh Circuit's influential *United States v. Pasha*[159] decision, callers intended to communicate with the criminal defendants by dialing a particular telephone.[160] The phone call reached the telephone, but law enforcement—not the criminal defendants—answered the call.[161] The court held that law enforcement had not tampered with the underlying communication because the call reached its intended destination: the telephone.[162] Law enforcement must tamper with a call on its way to an intended telephone in order to become an unintended recipient liable for interception.[163]

In *Jurgens v. Build.com, Inc.*,[164] an Eastern District of Montana case, Plaintiff Jurgens admitted that an electronic communication was stored on a computer waiting to be transmitted to the defendant's server.[165] The court held that the defendant must be an intended recipient.[166] It did not matter whether Jurgens intended to actually transmit the communication.[167] According to *Pasha*, a court should reject liability where defendants merely

155. *Id.*

156. *Vasil*, 2018 WL 1156328, at *6 (finding no support for the defendant's argument that "a direct, but unintended, recipient of a communication automatically becomes a party"); *Backhaut*, 74 F. Supp. 3d at 1043 (finding plaintiffs had alleged a prima facie claim because messages were not addressed to defendant).

157. *See supra* notes 142–56 and accompanying text.

158. *See* United States v. Pasha, 332 F.2d 193, 197–98 (7th Cir. 1964) (quoting State v. Carbone, 183 A.2d 1, 26 (N.J. 1962)).

159. 332 F.2d 193 (7th Cir. 1964).

160. *See id.* at 196–98.

161. *See id.* at 196.

162. *See id.* at 198 ("[T]he conversations between the callers and the agent cannot be said to have been intercepted. Interception connotes a situation in which by surreptitious means a third party overhears a telephone conversation . . . .").

163. *See Carbone*, 183 A.2d at 4–5.

164. No. 17-CV-00783, 2017 WL 5277679 (E.D. Mo. Nov. 13, 2017).

165. *See id.* at *5 (highlighting plaintiff's admission that the communication at issue was for the "eventual 'transmittal to Defendant'" (quoting Second Amended Complaint at 5, Jurgens v. Build.com, Inc., No. 4:17-CV-00783 (E.D. Mo. Nov. 13, 2017))).

166. *See id.* (concluding that said admission ended liability because an "intended recipient of such transmission is a party").

167. *See id.*

answer a telephone[168] rather than tamper with a communication on the way to its intended destination.[169]

In *State v. Roden*,[170] Washington state's supreme court considered the *Pasha* approach and offered a persuasive rebuttal to *Pasha* in modern times. *Roden* declined to extend the intended destination approach to text messages.[171] According to *Roden*, text messages are similar to physical mail where the mail's addressee is clearly identifiable.[172] The sender of a text message has an expectation that the text message will reach an intended destination which includes an intended recipient.[173] Like *Vasil* and *Backhaut*, the intended-recipient status hinged on an identifiable intended recipient—not the destination alone.[174]

C. Recipient Behavior May Also Affect Party Status

As discussed in Part II.B, courts have distinguished between intended and unintended recipients by analyzing manifestations of sender intent or analyzing whether a communication reached its intended destination uninterrupted.[175] Some courts also subcategorize recipients based on the recipient's behavior; two subcategories include manufactured recipients[176] and surreptitious listeners.[177]

1. Manufactured Recipients

Communications can begin when someone decides to speak,[178] dials a telephone,[179] sends an email,[180] or visits a website.[181] Although this chain of events is sufficient, the recipients of data can also direct a sender to initiate the communication.[182] This Note refers to these recipients as manufactured recipients.

---

168. *See* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (alluding to, but not citing, the *Pasha* line of thinking by describing an identical and "untenable" hypothetical where "one who picks up a telephone" is subjected to liability).

169. *See* State v. Carbone, 183 A.2d 1, 4 (N.J. 1962) (providing the foundation for *Pasha*'s paradigmatic view of interception).

170. 321 P.3d 1183 (Wash. 2014).

171. *See id.* (declining to extend *Pasha* to text messages).

172. *Id.* ("The sender addresses mail to a particular individual and reasonably expects the communication to be routed to and received by the addressee.").

173. *See id.*

174. *See supra* Part II.B.1.

175. *See supra* Parts II.B.1, II.B.2.

176. *See infra* Part II.C.1.

177. *See infra* Part II.C.2.

178. *See* People v. Herrington, 645 N.E.2d 957, 958–59 (Ill. 1994).

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

180. *See* United States v. Szymuszkiewicz, 622 F.3d 701, 707 (7th Cir. 2010).

181. *See In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 274 (3d Cir. 2016); *see also* Allen v. Quicken Loans Inc., No. 17-12352, 2018 WL 5874088, at *4 (D.N.J. Nov. 9, 2018).

182. *See infra* notes 183–92 and accompanying text.

For some courts, manufactured recipients are ineligible for the party exception. In *In re iPhone Application Litigation*,[183] a federal district court in the Northern District of California considered a plaintiff-class's allegation that user data collected on iPhones and transmitted to Apple was unlawfully intercepted.[184] Apple invoked the party exception because iPhones were intentionally designed to transmit user data to Apple.[185] Apple argued that because user data was intentionally sent to Apple, Apple was an intended recipient and therefore an exempt party.[186]

On a motion to dismiss, the court rejected this argument.[187] Apple's intentional software design was the very thing that allegedly enabled the interception.[188] Apple could not point to "accused conduct" as evidence that it was an intended recipient eligible for a party exception.[189] Likewise, in *White v. Samsung Electronics America, Inc.*,[190] New Jersey's federal district court rejected the party exception—where televisions transmitted users' viewing habits—based on the defendant's intentional software design.[191] This intentional software design supported alleged wiretap interception and could not create an intended recipient on a motion to dismiss.[192]

2. Surreptitious Listeners

Courts have recognized a second subcategory of recipients ineligible for the party exception: surreptitious listeners.[193] *Pasha* imagined unlawful interception as the hypothetical conversation between two parties overheard surreptitiously by a third entity.[194] Interpreting this dicta, the federal district court in New Jersey, in *United States v. Eady*,[195] held that a person invisibly listening to a conversation was ineligible for the party exception.[196] However, not every surreptitious act creates a surreptitious listener ineligible for the party exception.[197] In *Allen*, the invisible transfer of user data by

183. 844 F. Supp. 2d 1040 (N.D. Cal. 2012).
184. *Id.* at 1050 (describing Apple's alleged collection of geolocation data from users' iPhones).
185. *Id.* at 1062.
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.* ("Apple cannot manufacture a statutory exception through its own accused conduct . . . .").
190. No. 17-1775, 2019 WL 8886485 (D.N.J. Aug. 21, 2019).
191. *Id.* at *6.
192. *Id.*
193. *See White*, 2019 WL 8886485, at *6; Zak v. Bose Corp., No. 17-CV-02928, 2019 WL 1437909, at *3 (N.D. Ill. Mar. 31, 2019); Allen v. Quicken Loans Inc., No. 17-12352, 2018 WL 5874088, at *5 (D.N.J. Nov. 9, 2018); Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *6 n.5 (N.D. Ill. Mar. 5, 2018).
194. *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964).
195. No. 14-277, 2015 WL 1735495 (D.N.J. Apr. 15, 2015).
196. *See id.* at *3.
197. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 144 n.80 (3d Cir. 2015).

Quicken was insignificant.[198] No matter how surreptitious, Quicken was already an intended recipient of the communication and could freely transfer the user data surreptitiously.[199]

For that reason, a surreptitious listener must intrude upon a communication that could exist without the surreptitious listener's participation.[200] This standard is met when a court identifies the sender and intended recipient and then determines that the surreptitious listener fits into neither category.[201]

D. Party Status Also Depends on the Scope of a Communication

For all the work courts do to identify the parties to a communication, sometimes analyzing the right communications is what matters most. In *White v. Samsung Electronics America, Inc.*, the New Jersey federal district court was confronted with two communications each with different identifiable parties.[202] The first communication was between television users and content providers, including video streaming services like Netflix.[203] Here, users requested videos from their televisions by directing the televisions to communicate with the content providers.[204]

In the second communication, Samsung's embedded software in the users' televisions created a transmission between users and Samsung's servers.[205] The second communication allegedly sent Samsung data about the videos users requested from the content providers.[206] Viewed in isolation, Samsung was a party to the second communication sent directly from the users to Samsung.[207]

However, the court rejected this isolated analysis.[208] Taken together, the second communication could be evidence that the first communication between users and content providers was being intercepted and sent to Samsung.[209] The second communication conveyed to Samsung the duplicate data contained in a communication between users and content providers; user viewing habits sent from user to content provider.[210] Party status in a second communication could not protect Samsung if a second communication

198. *See* 2018 WL 5874088, at *5 (concluding that once Quicken was a party to the communication, consent allowed Quicken to facilitate interception even if the behavior was unknown to its users).

199. *Id.*

200. *See* White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *6 (D.N.J. Aug. 21, 2019) (finding party status unavailing where surreptitious software intercepted transmissions between content providers and customers' TVs).

201. *See id.*

202. *See id.* at *5.

203. *See id.* at *1, *5.

204. *See id.*

205. *See id.* at *6.

206. *See id.* at *1.

207. *See id.* at *5.

208. *See id.* at *6.

209. *See id.* at *5.

210. *Id.* at *6 ("Plaintiffs allege that Defendants surreptitiously installed software on their televisions that permitted Defendants to track their communications with streaming services, their cable providers, or other content providers . . . .").

intercepted data in a communication between users and content providers which Samsung was not a party to.[211]

As a result, litigants and courts can determine whether party status in one communication is dispositive or distracting from another communication that should decide liability.[212] Similarly, a federal district court in the Northern District of California, in *In re iPhone Application Litigation*, rejected Apple's focus on communications sent directly from users' iPhones to Apple.[213] Looking at these communications in isolation could suggest that Apple was an intended recipient.[214] Instead, the court widened the scope of its analysis and asked whether Apple was a party to earlier, but related, communications sent between users' iPhones and cellular towers.[215]

III. THIRD AND NINTH CIRCUITS REACH OPPOSITE RESULTS ON THE PARTY EXCEPTION IN REGARD TO DUPLICATE GET REQUESTS

Part III examines how the Third and Ninth Circuits applied the party exception to a duplicate GET request. Part III.A considers the Third Circuit case, *In re Google Inc. Cookie Placement Consumer Privacy*,[216] in which the Third Circuit concluded that the party exception applied to a duplicate GET request.[217] Part III.B highlights decisions in the First, Seventh, and Ninth Circuits, which create a circuit split with the Third Circuit. Part III.B.1 analyzes cases in the First and Seventh Circuits where the courts concluded that two communications containing duplicate data are indicia of wiretap interception.[218] Part III.B.2 reviews the Ninth Circuit decision, *In re Facebook, Inc. Internet Tracking Litigation*,[219] which held that the party exception did not apply to a duplicate GET request.[220]

A. Third Circuit: Digital Advertisers Are Exempt Parties

In 2015, the Third Circuit considered the wiretap liability of digital advertisers, including Google.[221] A class of plaintiffs sued for the alleged

211. *See id.* at *5 ("[W]hile Defendants are parties to the latter communication, it is the former that Plaintiffs allege was unlawfully intercepted. Because Defendants are not a party to that communication, the exception does not apply.").

212. *Compare In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (holding that lack of party status in an identical but standalone communication does not deprive party status in a second communication), *with* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *6 (N.D. Ill. Mar. 5, 2018) (holding that a communication from a user to a recipient was relevant insofar as it intercepted another communication).

213. *See id.* at 1062 (rejecting Apple's isolated focus on a single communication flowing directly between the users' iPhones and Apple's servers).

214. *Id.*

215. *Id.* (finding that the relevant communication flowed from users' iPhones to cellular towers before the alleged interception).

216. 806 F.3d 125 (3d Cir. 2015).

217. *See id.* at 142–43.

218. *See generally* United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010); *In re* Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).

219. 956 F.3d 589 (9th Cir. 2020).

220. *Id.* at 608.

221. *See In re Google*, 806 F.3d at 130, 133.

interception of their electronic communications.[222] The suits were consolidated into *In re Google Inc. Cookie Placement Consumer Privacy Litigation*. The plaintiff-class represented the sort of internet users mentioned throughout this Note.[223] Users visited websites delivered via GET requests.[224] On arrival, websites displayed advertisements.[225] Advertisements were served via a duplicate GET request generated when users reached a website.[226] The request was duplicate insofar as it contained data identical to that found in the original request between user and website.[227] Advertisers retained user data and assigned an identity to track users' online behavior.[228]

On appeal, the internet users challenged the district court's dismissal of the wiretap interception claim.[229] Contrary to the district court,[230] the Third Circuit found that the digital advertiser's wiretap liability turned on whether or not the advertisers were exempt parties.[231] The digital advertisers argued that they were intended recipients of the GET request communication and thus qualified for the party exception.[232]

Like *White v. Samsung Electronics America, Inc.* and *In re iPhone Application Litigation*, the Third Circuit began its party exception analysis by asking which communication controlled the digital advertisers' party status.[233] In the internet users' view, advertisers intercepted communications between users and the websites they visited (e.g., the GET request from users to website).[234] The Third Circuit disagreed, isolating its analysis to the duplicate GET request between users and advertisers.[235]

The court supported its conclusion with three points. First, the duplicate GET request used to serve digital advertisements and collect user data flowed directly from the users' web browsers to the advertisers.[236] This duplicate

222. *See id.*

223. *See generally In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262 (3d Cir. 2016); Allen v. Quicken Loans Inc., No. 17-12352, 2018 WL 5874088 (D.N.J. Nov. 9, 2018).

224. *See In re Google*, 806 F.3d at 130 (describing the GET request delivering a website to users and the subsequent secondary GET request used to deliver digital advertisements to users).

225. *See id.*

226. *See id.* at 130–31.

227. *See id.* at 140–41 (inferring that there was no need to obtain user data from a GET request between users and websites because the same user data was contained within the secondary GET request).

228. *See id.* at 131.

229. *Id.* at 134.

230. *See id.* at 139–40 (finding that the district court erred in finding that GET requests did not contain identifiable content).

231. *See id.*

232. *Id.* at 140.

233. *See id.*; White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *5 (D.N.J. Aug. 21, 2019); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012).

234. *In re Google*, 806 F.3d at 140.

235. *See id.* at 142.

236. *Id.* at 140–41.

GET request was not acquired on its way from users to websites.[237] Second, direct receipt of the duplicate GET request meant that the advertisers had "no need" to capture identical data from the first GET request between the users and the websites.[238] Advertisers had the "information . . . anyway" from the duplicate GET request.[239] Third, the court found that the internet users had not identified a device that could intercept the users' first GET request.[240]

Once the court concluded that the relevant communication flowed directly from the users to advertisers, the court proceeded to identify the parties to that communication.[241] In line with the sender and recipient framework, the court concluded that any communication includes a sender and one or more intended recipients.[242] By making up the second half of the communication, an intended recipient is an exempt party.[243]

Applying this logic, digital advertisers were the intended recipients of the duplicate GET request because the requests were transmitted directly to advertisers.[244] This is similar to the logic applied in *Pasha*.[245] The duplicate GET request was intended to reach the advertisers' servers and it reached that destination uninterrupted.[246] Accordingly, the advertisers were exempt parties.[247] At this point, even if the digital advertisers surreptitiously stored data, they did so as exempt parties.[248]

The fact that Google was a manufactured recipient was also deemed legally insignificant.[249] Google's embedded code "circumvented" a web browser's settings in order to generate the duplicate GET request.[250] The court held that Google's behavior could manufacture recipient status by gaining "entrance to a conversation through a fraud" without limiting Google's access to the party exception once the transmission occurred.[251]

237. *See id.*
238. *See id.*
239. *Id.* at 141.
240. *Id.* at 141–42.
241. *Id.* at 142–43.
242. *Id.* at 143.
243. *See id.* ("[T]he intended recipient of a communication is necessarily one of its parties . . . .").
244. *See id.* at 142.
245. *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (quoting State v. Carbone, 183 A.2d 1, 26 (N.J. 1962)).
246. *See In re Google*, 806 F.3d at 140 (characterizing the GET request as a direct transmission from users to advertisers).
247. *Id.* at 145.
248. *Id.* at 143.
249. *See id.* ("Though we are no doubt troubled by the various deceits alleged in the complaint, we do not agree that a deceit upon the sender affects the presumptive non-liability . . . .").
250. *Id.* at 132.
251. *Id.* at 143.

B. A GET Request Circuit Split: The First, Seventh, and Ninth Circuits Disagree with the Third Circuit

Part III.B.1 examines two First and Seventh Circuit decisions important to the Ninth Circuit's decision in *In re Facebook, Inc. Internet Tracking Litigation*. The First and Seventh Circuit decisions held that two communications containing duplicate data are indicia of wiretap interception. Part III.B.2 considers how the Ninth Circuit relied on this logic, rejected the Third Circuit approach, and concluded that duplicate GET requests are ineligible for a party exception.

1. First and Seventh Circuits: Duplicate Communications Are Indicia of Wiretap Interception

By the time the Third Circuit accorded digital advertisers party status in relation to their duplicate GET requests, the First and Seventh Circuits had already set out doctrine for a contrary approach.[252] In the First Circuit, the court considered whether one communication should be analyzed in isolation even though it contained duplicate data from another communication.[253] Isolated, the communication containing duplicate data could grant defendants status as an exempt party so long as they were intended recipients—just as it would in the Third Circuit.[254]

This is precisely what Pharmatrak argued in the First Circuit's 2003 case, *In re Pharmatrak, Inc.*[255] Pharmatrak sold software to pharmaceutical clients, allowing the clients to track users' behavior on the clients' websites.[256] Unknown to the clients and users alike, Pharmatrak collected user data in a variety of ways.[257] In one instance, Pharmatrak duplicated the data from communications sent from users' web browsers to the client websites.[258] User data was then sent back to Pharmatrak using a second communication.[259] Pharmatrak argued that these were two unique communications: one communication between users and client websites, and a second communication between users and Pharmatrak.[260]

The First Circuit rejected this argument. Notably, the user data captured by Pharmatrak was identical to the data generated in the original communication between users and the clients' websites.[261] The court noted

252. *See generally* United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010); *In re* Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).
253. *See In re Pharmatrak*, 329 F.3d at 22.
254. *See id.*; *see supra* notes 244–47 and accompanying text.
255. 329 F.3d 9 (1st Cir. 2003).
256. *See In re Pharmatrak*, 329 F.3d at 14.
257. *See id.*
258. *Id.* at 22 ("[C]ode automatically duplicated part of the communication between a user and a . . . client and sent this information to a third party . . . .").
259. *Id.*
260. *Id.* ("Pharmatrak argues that there was no interception because 'there were always two separate communications: one between the Web user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak.'").
261. *See id.*

that unauthorized interception under the Wiretap Act did not require acquisition of the "same communication"—only a communication's contents.[262] For the First Circuit, this established wiretap liability.[263] It was enough to intercept a communication's contents even if the contents were transmitted using a second communication.[264]

Subsequently, the Seventh Circuit's decision in *United States v. Szymuszkiewicz* confirmed that wiretap interception could include multiple communications tied together because the communications' contents were duplicate. Szymuszkiewicz allegedly spied on Infusino by tampering with Infusino's email settings so that Infusino's emails were automatically forwarded from Infusino's inbox to Szymuszkiewicz's computer.[265] This meant that there were two communications containing duplicate data: emails Infusino received and duplicate emails forwarded from Infusino to Szymuszkiewicz.[266] According to Szymuszkiewicz, there was no interception because the emails were forwarded once Infusino received them, not while the emails were in transit.[267]

The Seventh Circuit declined to require in-transit interception of the emails Infusino received.[268] The court held that from a technical perspective, in-transit interception was impossible because there was never a single communication while the emails were transmitted to Infusino.[269] Emails are split up into multiple communications and only reassembled once they reach their intended recipient.[270] Szymuszkiewicz could only acquire the emails by duplicating and forwarding the contents.[271] Thus, a second transmission containing the same data as another communication was a necessary element of wiretap interception.[272]

2. Ninth Circuit: Digital Advertisers Are Not Exempt Parties

The Ninth Circuit considered and rejected the Third Circuit's holding.[273] In the Ninth Circuit's view, recipients of a duplicate GET request containing the same data as another GET request were not exempt parties.[274] In *In re*

262. *See id.* ("[C]ircuits . . . do not require that the acquisition somehow constitute the same communication . . . .").
263. *See id.*
264. *See id.*
265. United States v. Szymuszkiewicz, 622 F.3d 701, 703 (7th Cir. 2010).
266. *See id.*
267. *Id.*
268. *Id.* at 705.
269. *Id.* ("'[I]nterception' as 'catching a thing in flight' is sensible enough for football, but for email there is no single 'thing' . . . .") (quoting Brief and Appendix of Defendant-Appellant David S. Szymuszkiewicz at *1, United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010) (No. 10-1347)).
270. *Id.*
271. *Id.* at 706 ("'[I]nterception' of a communication sent in packets must be done by programming a computer to copy the contents it sends along . . . .").
272. *See id.*
273. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020).
274. *Id.* ("[S]imultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability . . . .").

Facebook, Inc. Internet Tracking Litigation, internet users sued Facebook for the alleged interception of the users' GET request data sent to websites.[275]

Facebook embedded plug-ins on websites on the internet.[276] These plug-ins allowed internet users to "like" content on the website.[277] The plug-ins also collected user data including URLs of the websites the users visited, referral information indicating the websites that users last visited, and search query terms.[278] Facebook retained and identified this user data.[279]

At a technical level, Facebook's collection of user data leveraged GET requests.[280] When users visited a website, an initial GET request was generated between the users and the websites containing user data.[281] Simultaneously, the Facebook plug-in generated a duplicate GET request between the users and Facebook.[282] This duplicate contained the same user data that appeared in the GET request sent from users to the websites.[283]

In assessing this fact pattern, the lower court had held that the party exception did not apply.[284] On appeal, the Ninth Circuit reviewed the decisions in *In re Pharmatrak* and *Szymuszkiewicz*.[285] The Ninth Circuit interpreted both cases as punishing surreptitious listeners.[286] The Ninth Circuit also noted that both *In re Pharmatrak* and *Szymuszkiewicz* identified wiretap interception where two communications contained duplicate data shared between more than one communication.[287] There was also duplicate data here.[288] Facebook's GET request contained the same user data as the GET request sent from the internet users to websites that contained Facebook's plug-in.[289]

The Ninth Circuit then concluded that a surreptitious GET request containing duplicate user data from another GET request could not accord party status.[290] The court relied heavily on legislative intent to buttress the First and Seventh Circuits' persuasive decisions.[291] The Ninth Circuit

275. *See id.* at 596.
276. *Id.*
277. *Id.*
278. *Id.*
279. *See id.*
280. *See id.* at 607 ("[C]ode directs the user's browser to copy the referer [sic] header from the GET request and then send a separate but identical GET request . . . to Facebook's server.").
281. *Id.* at 605, 607.
282. *Id.* at 607.
283. *Id.*
284. *In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017).
285. *In re Facebook*, 956 F.3d at 607.
286. *Id.* ("The First and Seventh Circuits have implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to communications . . . .").
287. *Id.*
288. *Id.*
289. *Id.*
290. *Id.* at 608.
291. *Id.* (affirming that the Wiretap Act was intended to protect the privacy of communications and that the legislative history "evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party").

interpreted the Wiretap Act as prohibiting the acquisition of communications by surreptitious listeners hidden from the lawful parties to a communication.[292] Using legislative intent, the Ninth Circuit held that allowing Facebook to invoke the party exception would allow frequent and unknown collection of user data.[293] For the Ninth Circuit, this was an exception that swallowed the rule.[294]

IV. DIGITAL ADVERTISERS ARE UNINTENDED RECIPIENTS AND INELIGIBLE FOR THE PARTY EXCEPTION

Part IV argues that when digital advertisers receive a duplicate GET request, they are unintended recipients ineligible for the party exception. Part IV.A contends that when two GET requests contain duplicate data, the duplicate data should be the focus of a court's party analysis. Part IV.B notes that when two communications contain duplicate data, equating the direct recipient of a GET request with an intended recipient lacks judicial support and cannot properly decide party status. Part IV.C concludes that when the GET requests' duplicate data is analyzed, digital advertisers are unintended recipients of that user data. Part IV.C.1 confirms this by analyzing the manifestations of sender intent. Part IV.C.2 reaches the same conclusion by analyzing the user data's intended destination.

A. Duplicate GET Requests Create a Possibility of Interception

In re Google's facts presented the Third Circuit with two GET requests. One was between users and the websites they visited.[295] The other was between internet users and digital advertisers.[296] These GET requests were duplicate insofar as they shared the same user data.[297] Users in the Third Circuit argued that advertisers intercepted data in the GET request between users and websites.[298] However, the court rejected this theory and instead isolated its wiretap interception analysis to the GET request between users and digital advertisers.[299] Isolating the analysis to only one GET request and its data was improper because it misconstrues how user data is intercepted.

When two communications contain the same user data, courts routinely factor this into their analysis. In *Vasil*, the defendant received a communication that conveyed user data from another communication between users and a mobile application.[300] The defendant in *In re iPhone*

292. *Id.* ("[L]egislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.'").
293. *Id.*
294. *Id.*
295. *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 130 (3d Cir. 2015).
296. *Id.*
297. *See id.* at 140.
298. *Id.*
299. *Id.* at 142.
300. Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *3 (N.D. Ill. Mar. 5, 2018).

received a communication that contained user data from another communication between the users' iPhones and cellular towers.[301] Samsung's communication in *White* conveyed users' television viewing data, all of which was contained in another communication between the users and content providers.[302] The communication in *In re Pharmatrak* conveyed user data that also appeared in another communication between users and websites.[303] Each decision found support for interception and held that the party exception did not apply.[304]

These courts correctly analyzed both duplicate communications and the duplicate data because it is the smoking gun of unlawful interception. *Szymuszkiewicz* recognized that a second communication can be necessary in order to intercept certain user data.[305] Emails are broken up into packets of information and sent using many different communications.[306] In order to intercept an email broken up into packets, a second communication must duplicate and transmit the contents.[307] Other user data is broken up into packets of information.[308] This can include the GET request exchange.[309] Accordingly, the same logic can apply to GET requests. User data in a GET request may be intercepted by duplicating the contents of one GET request and transmitting that data using a second communication. This means that intercepting a GET request may involve the use of a second communication.[310] Intercepting GET requests may appear different than recording an oral conversation[311] or wiretapping a telephone line,[312] but it is still a potential form of interception.[313]

Not every GET request necessarily relies on multiple packets to transmit the initial user data—far from it. The transmission of user data via a GET

---

301. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012).

302. White v. Samsung Elecs. Am., Inc., No. CV 17-1775, 2019 WL 8886485, at *1, *5 (D.N.J. Aug. 21, 2019).

303. *In re* Pharmatrak, Inc., 329 F.3d 9, 14, 22 (1st Cir. 2003).

304. *See supra* notes 300–03 and accompanying text.

305. *See* United States v. Szymuszkiewicz, 622 F.3d 701, 704–05 (7th Cir. 2010).

306. *Id.* at 705.

307. *Id.* at 706 ("The 'interception' of a communication sent in packets must be done by programming a computer to copy the contents it sends along (and reassemble them later) . . . .").

308. *Packets*, NETWORKS LAND (Oct. 21, 2020), http://networks.land/reference/packets/ [https://perma.cc/L6ZT-GSBX] ("Packets are the basic unit of transport for digital communications networks.").

309. Pamela Fox, *Hypertext Transfer Protocol (HTTP)*, KHAN ACADEMY, https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:web-protocols/a/hypertext-transfer-protocol-http [https://perma.cc/3Q77-BTNH] (last visited Sept. 17, 2021).

310. Even if this is not a necessary method for intercepting GET requests, *Szymuszkiewicz* and *In re Pharmatrak* suggest that it is sufficient. *See supra* Part III.B.1. With that in mind, courts should analyze the GET requests together because there is the possibility one GET request intercepts another request's data.

311. *See generally* Caro v. Weintraub, 618 F.3d 94 (2d Cir. 2010).

312. *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (requiring interception while a communication is in transit).

313. *See* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010).

request may only use a single packet.[314] In fact, the total exchange should include as few packets as possible.[315] That said, the response to a GET request may generate many packets to transmit website content.[316]

Even so, cookies identifying user data can increase the size of an initial GET request's data, thus employing additional packets for the transmission.[317] Particular senders, recipients, or pathways between senders and recipients may warrant additional packets.[318] Accordingly, second communications remain an effective method of capturing user data where there is uncertainty as to whether data in the first communication will be found within a single easily intercepted transmission.[319] Furthermore, GET requests may be sent using HTTPS connections, in which case the user data in the GET request is encrypted.[320] At that point, a duplicate GET request may not only be an effective method of interception, but a necessary one.

As a result, the Third Circuit was quick to exclude the GET request between users and websites.[321] The GET request digital advertisers received could contain the data of a GET request between users and websites because that data was intercepted. When user data is shared between two GET requests, this is not evidence that interception is unnecessary;[322] it is evidence that interception may have occurred.[323] The Third Circuit also erred when it did not identify a device "capable of capturing" the GET requests between users and websites.[324] The GET request that advertisers receive is the answer. The duplicate GET request is an "artifice" that not

314. *See* Fox, *supra* note 309 (contemplating an HTTP request, which can include a GET request, contained within a single packet).

315. *See HTTP/2 Frequently Asked Questions*, INTERNET ENG'G TASK FORCE, https://http2.github.io/faq [https://perma.cc/F8Y8-B3ZB] (last visited Sept. 17, 2021) (advocating for the compression of data to reduce the number of requests and speed up websites).

316. *See* Fox, *supra* note 309 ("[E]ach HTTP response [versus the HTTP request] is inside another IP packet—or more typically, multiple packets, since the response data can be quite large.").

317. *An Analysis of Cookie Sizes on the Web*, PAUL CALVANO (July 13, 2020), https://paulcalvano.com/2020-07-13-an-analysis-of-cookie-sizes-on-the-web [https://perma.cc/Z99D-86ZF] (examining how the size of cookies can dictate whether "multiple TCP packets" are used in an HTTP request, including GET requests).

318. *See Maximum Packet Size*, IBM, https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=addresses-maximum-packet-size [https://perma.cc/8DLN-Z3PJ] (last visited Sept. 17, 2021) (describing how a client, server, and network can have varying maximum packet sizes resulting in the use of additional packets if data exceeds the maximum packet size).

319. *See* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (concluding that when packets are in use in the transmission of data, the underlying data must then be copied).

320. *See Introduction to HTTPS*, CIO COUNCIL, https://https.cio.gov/faq [https://perma.cc/7WDA-VM4Z] (last visited Sept. 17, 2021).

321. *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 142 (3d Cir. 2015) (isolating the exception analysis).

322. *Id.* at 140–41 ("[T]here is no need . . . to acquire that information from [other] transmissions . . . [T]he defendants would have the information at issue anyway.").

323. *See In re* Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003); *see also Szymuszkiewicz*, 622 F.3d at 706.

324. *In re Google*, 806 F.3d at 141–42.

only displays digital advertisements but also, by its function, redirects duplicate data between the user and the website.[325]

The Third Circuit should have asked whether the two GET requests were so interrelated that they create the possibility of interception. If so, the court should have assessed whether the advertiser was an intended recipient of that duplicate data. Focusing on the data recognizes that interception can occur when data is duplicated, even if that process requires a second GET request.[326] Otherwise, the court turns a blind eye to a common method of interception: duplicating user data and transmitting it using a second communication.[327] The Wiretap Act's party exception protects parties to a communication.[328] The party exception does not protect novel forms of interception.[329]

The GET request between users and advertisers qualifies as the sort of communication that should be analyzed in terms of duplicate data. First, the GET request that advertisers receive contains duplicate data found in another GET request.[330] A GET request containing duplicate data from another GET request mirrors the communications in *Vasil*, *In re iPhone*, *White*, *In re Pharmatrak*, and *Szymuszkiewicz*, where one communication contained the same data as another communication creating the risk that the data was obtained by interception.[331] As such, two GET requests containing duplicate data should be analyzed in terms of the data's intended recipient because that duplicate data may indicate that it was likewise obtained by interception.[332]

Second, the advertisers' duplicate GET request is automatically generated when the GET request between users and websites is created.[333] This is what *Szymuszkiewicz* interception would expect—affirming the risk that the duplicate data is being intercepted using a second GET request. One communication's content is being intercepted using a second communication; an effective, or even necessary, method of interception for

325. Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *6 n.5 (N.D. Ill. Mar. 5, 2018).

326. *In re Pharmatrak*, 329 F.3d at 22 (concluding that wiretap interception does not require the interception of the same communication and that two duplicate communications are sufficient).

327. *See Szymuszkiewicz*, 622 F.3d at 706.

328. Warden v. Kahn, 160 Cal. Rptr. 473, 475 (Ct. App. 1979); *see supra* note 41 and accompanying text (confirming that *Warden*'s state law interpretation is equivalent to the federal law exception).

329. *Szymuszkiewicz*, 622 F.3d at 706; *Vasil*, 2018 WL 1156328, at *6 (declining to reward tech savvy wiretappers); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) ("Apple cannot manufacture a statutory exception . . . .").

330. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596 (9th Cir. 2020) (explaining that the "like" button "is able to replicate [user data]."); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 140 (3d Cir. 2015).

331. *See supra* notes 300–20 and accompanying text.

332. *See* White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *5 (D.N.J. Aug. 21, 2019).

333. *See In re Google*, 806 F.3d at 130; *see also In re Facebook*, 956 F.3d at 607.

data.[334] When the Third Circuit declined to analyze the intended recipient of the duplicate data, the court ignored an indicium of interception.[335]

B. Direct Receipt of GET Requests Cannot Decide Party Status

After too quickly isolating its analysis, the Third Circuit equated the direct recipient of a duplicate GET request with an intended recipient.[336] This standard is inconsistent with case law and cannot accurately decide party status for GET requests that share data. Case law indicates that the interception of data appears deceptively direct—from user to alleged wrongdoer.

In *Vasil*, the communication flowed directly from the users' phones to Vasil's servers.[337] Although *Vasil* applied Illinois state law, the court noted that the Illinois definition of a party "comports" with the federal definition.[338] The court held that federal law does not equate direct and intended recipients.[339] Likewise, *In re iPhone* involved an intentional transmission sent directly from "mobile devices to Apple's servers."[340] The court declined to apply the party exception.[341] The Third Circuit is not bound by either legal decision. Yet, both courts were confronted with direct recipients and did not find that factor valuable in deciding exempt party status.

It is possible that the Third Circuit has found some value in equating direct receipt with an intended recipient that lower courts have not. That said, New Jersey federal district court's decision in *White* and a subsequent reading of *White* in *New Concepts for Living, Inc. v. Communications Workers Local 1040*[342] may demonstrate the limited value of the standard for electronic communications.

In *White*, the court rejected Samsung's argument that relevant communications "were transmissions from Plaintiffs' Smart TVs to [Samsung's] servers," which—if Samsung had been correct—would imply that the communications were "directly received" by Samsung and exempt according to a direct receipt standard.[343]

Rather, the court in *New Concepts for Living, Inc.* read *White* as describing "allegedly captured transmissions that were not being directly sent to [Samsung]."[344] For this reason, *White* can be viewed as a case of a liable indirect recipient, and *In re Google* can be viewed as a case of a direct

334. *See supra* notes 300–20 and accompanying text.
335. *See supra* notes 300–20 and accompanying text.
336. *In re Google*, 806 F.3d at 140–42.
337. Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *6 (N.D. Ill. Mar. 5, 2018).
338. *Id.*
339. *See id.* at *7.
340. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012).
341. *See id.*
342. No. 19-719, 2021 WL 2201835 (D.N.J. May 28, 2021).
343. *See* White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *5 (D.N.J. Aug. 21, 2019) (rejecting Samsung's characterization, while noting that *In re Google* granted party status where Google "directly received their communications").
344. *See New Concepts for Living, Inc.*, 2021 WL 2201835, at *5.

recipient treated as an intended recipient.[345] The trouble is that both *White* and *In re Google* describe alleged interception by indirect recipients no matter the fact that some underlying communications appear deceptively direct as they move from users to the defendants of each case.

In *White*, Samsung was an indirect recipient because Samsung allegedly monitored communications between users' television and content providers before receiving a second communication from "the Smart TV[s] to [Samsung's] servers."[346] Despite the fact that Samsung was a party "to the latter communication" sent from users to Samsung, Samsung was not a direct recipient so long as the alleged interception began with a communication between the users' televisions and the content providers.[347] Receipt and party status in the second communication was not enough so long as alleged interception began with the first communication.[348]

Yet, the GET request that an alleged wrongdoer typically receives takes an equally attenuated path—deceptively direct—from user to defendant. *Popa v. Harriet Carter Gifts, Inc.*,[349] in the Western District of Pennsylvania, examined the movement of a GET request from user to defendant—Navistone—while relying on *In re Google*'s application of the direct recipient standard for party status.[350] Despite concluding that Navistone was "a direct party" to the GET request received, that communication first relied on a transmission between user and website: "[t]he visitor's browser first sends a GET request to [the website's] server, and that server responds," which only then prompts the additional GET requests transmitted toward Navistone.[351]

In this way, *In re Google* and *Popa* both describe a GET request moving from user to defendant prompted only by virtue of an earlier communication between the user and the website.[352] Like in *White*, however direct a defendant's receipt of a GET request appears, alleged interception begins by relying on an initial communication between two other parties that does not include the defendant. In *White*, Samsung relied on communications

345. *See id.* (distinguishing *White* from *In re Google* by concluding that *White* included "captured transmissions that were not being directly sent to [Samsung]," while *In re Google* "involved direct receipt by those defendants of the relevant communications").

346. *White*, 2019 WL 8886485, at *5.

347. *See id.*

348. *See id.*

349. No. 2:19-CV-450, 2021 WL 2463304 (W.D. Pa. June 17, 2021).

350. *Id*. at *7–8 ("The processes and operations underlying the communications between a user's web browser, Harriet Carter's website server, and Navistone's servers are materially similar to those discussed in *In re Google*."). *Popa* decides a state law claim. However, the court concluded that Pennsylvania law is equivalent to the Wiretap Act. *Id.* at *6.

351. *See id.* at *7–8.

352. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 140 (3d Cir. 2015) (noting that the GET request from a user to a digital advertiser is prompted by an earlier GET request exchange between a user and a website); *see also id.* at *7 (noting visitors send an initial GET request to the website before the server prompts GET requests sent to the defendant).

between users and content providers.[353] In *Popa* and *In re Google*, defendants relied on GET requests between users and websites.[354] Receiving a communication dependent on another transmission—all the while sharing that earlier transmission's data—means that a defendant's communication is the indirect result of a former communication that defendants "are not a party to" and not merely a communication "directly received."[355]

Notwithstanding the trouble identifying bona fide direct receipt of electronic communications reliant on other transmissions, the Third Circuit's interest in direct recipients may arise from *Pasha*'s interpretation of intended recipients. The court cited *Pasha* in an unrelated analysis.[356] In *Pasha*, the court analyzed whether a communication reached its intended destination uninterrupted.[357] This was one way to distinguish intended and unintended recipients.[358] However, the Third Circuit's reasoning suggests that any direct recipient of a communication is an intended recipient.[359] This interpretation appears inconsistent with *Pasha*. The Third Circuit focused on whether a GET request reached its destination directly but did not ask if the GET request had reached its "destined place."[360]

This suggests that the Third Circuit's reasoning either misinterprets *Pasha* or lacks judicial support. If the Third Circuit created a new standard, it cannot properly decide party status for duplicate GET requests. Under this standard, a court would ask if a GET request reached a destination uninterrupted without deciding if the GET request reached an intended destination.[361] If there is only one GET request, and one recipient to analyze, this standard makes sense. Every protected communication includes at least one sender and one recipient.[362] Otherwise, no communication exists to begin with.[363] If a plaintiff can only identify one communication and one recipient, then that recipient must have been intended.[364]

In this situation, identifying a direct recipient is useful because interception requires at least three entities: (1) a lawful sender, (2) an intended recipient, and (3) an unintended recipient that is tampering with the communication.[365]

353. *See* White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *5 (D.N.J. Aug. 21, 2019).

354. *See supra* note 352 and accompanying text.

355. *See White*, 2019 WL 8886485, at *5–6; *see also supra* Part IV.A (describing the possibility of *Szymuszkiewicz* interception where two electronic communications share the same underlying data).

356. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143–44 (3d Cir. 2015).

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

358. *See supra* notes 158–63 and accompanying text.

359. *See In re Google*, 806 F.3d at 142.

360. *Pasha*, 332 F.2d at 198 (quoting Goldman v. United States, 316 U.S. 129, 134 (1942)).

361. *See supra* notes 359–60 and accompanying text.

362. *See supra* note 120 and accompanying text.

363. *See supra* note 121 and accompanying text.

364. *See* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (concluding that the only identifiable recipient was a party when there was no evidence of tampering).

365. *See supra* notes 193–201 and accompanying text.

Here, the unintended recipient tampers with the underlying communication so that it no longer reaches its intended destination uninterrupted.[366] If there is only one possible recipient and one identifiable communication, a direct recipient could not have tampered with the communication.[367] The communication had nowhere else to go.[368] By default, the direct recipient becomes the communication's intended recipient and a lawful party.[369]

For duplicate GET requests, the direct recipient of a single GET request says little. Here, there are two recipients: websites users visit and advertisers.[370] A court must identify the intended recipients of the data because one communication could intercept the data from another communication.[371] In this case, digital advertisers are direct recipients of a GET request, but the GET request may still leverage another GET request by duplicating user data between users and websites.[372]

As a result, the direct recipient of a duplicate GET request is equally consistent with the three-entity requirement of a surreptitious listener.[373] When a user sends a GET request, websites are intended recipients, and advertisers receive a duplicate GET request to eavesdrop on users and websites as the third entity in the exchange.[374] When duplicate GET requests can be evidence of interception, even the direct recipients thereof could be intercepting data.[375] A court must analyze whether advertisers are intended recipients of the duplicate data, not whether advertisers are direct recipients of the suspect data.

C. Digital Advertisers Are Ineligible for the Party Exception

Part IV.C concludes that digital advertisers are unintended recipients of duplicate user data shared by two GET requests. Part IV.C adopts two methods for distinguishing intended and unintended recipients. Part IV.C.1 assesses manifestations of sender intent when internet users communicate

366. *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (quoting Goldman v. United States, 316 U.S. 129, 134 (1942)).

367. Contrast this with a surreptitious listener who intrudes upon a communication between two parties: a sender and an intended recipient. *See supra* notes 200–01 and accompanying text.

368. *See* Jurgens v. Build.com, Inc., No. 17-CV-00783, 2017 WL 5277679, at *5 (E.D. Mo. Nov. 13, 2017) ("[I]f there was an 'electronic communication' here, Defendant was a party to it.").

369. *See id.*

370. *See supra* notes 224–26, 281–83 and accompanying text.

371. *See supra* Part IV.A.

372. *See supra* notes 321–35 and accompanying text.

373. *See supra* notes 193–201 and accompanying text.

374. Once a duplicate communication is seen as an indicium of interception, that may enable a court to conclude that the party exception should not apply. *See supra* notes 300–25 and accompanying text. However, under an intended recipient analysis, a court will still need to confirm that the defendant was not the intended recipient of the duplicate communication's data by going on to assess either manifestations of sender intent or the intended destination. *See supra* Parts II.B.1, II.B.2. But now the analysis must focus on the duplicate data (i.e., the content being allegedly intercepted). *See supra* Part IV.A.

375. *See supra* notes 300–25 and accompanying text.

data in GET requests. Part IV.C.2 considers the intended destination of GET requests' data. Using either approach, advertisers are unintended recipients ineligible for the party exception.

1. Manifestations of Sender Intent and GET Request Data

Internet users manifest the intent to send user data to websites, not to digital advertisers. In *Backhaut* and *Roden* the manifestations of sender intent were explicit.[376] Cellphone users addressed text messages to a particular recipient.[377] In *Roden*, the court accepted a sender's reasonable expectation that a text message would reach the identified recipient, not someone else.[378] The same explicit manifestations of intent appear in GET requests; that intent does not include transmission to digital advertisers.

Here, an internet users' web browsers navigate the internet via GET requests.[379] Internet users make it clear that they want to communicate with a particular website when they enter a website's URL or click on a website's link.[380] But any intent to communicate with advertisers is difficult to locate. Unlike entering a URL or clicking a link, a duplicate GET request is generated automatically in a process invisible to users.[381]

It is illogical to say that users explicitly intend to communicate data with digital advertisers when the transfer of the user data happens without the users' involvement and is hidden from the users' view.[382] Furthermore, when advertisers gain access to data invisibly, they become surreptitious listeners that the Wiretap Act punishes, not exempt parties that the Wiretap Act should absolve.[383]

However, *Vasil* might allow a court to infer an intent to communicate with digital advertisers. The court inferred intent based on how users expect phones to communicate data based on privacy settings.[384] *Roden* was also

376. *See* Backhaut v. Apple, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014); State v. Roden, 321 P.3d 1183, 1189 (Wash. 2014).

377. *See Roden*, 321 P.3d at 1189 ("[S]ending a text is more like mailing a letter. The sender addresses mail to a particular individual and reasonably expects the communication to be routed to and received by the addressee."); *see also Backhaut*, 74 F. Supp. 3d at 1043–44 (concluding that plaintiff's allegations that text messages were not "addressed or directed to Apple" created a viable claim of interception on a motion to dismiss).

378. *See Roden*, 321 P.3d at 1189.

379. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 130 (3d Cir. 2015); *see also In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (9th Cir. 2020) ("When an individual internet user visits a web page, his or her browser sends a message called a 'GET request' . . . .").

380. *See In re Facebook*, 956 F.3d, at 596 (quoting *In re* Zynga Priv. Litig., 750 F.3d 1098, 1101 (9th Cir. 2014)).

381. *See id*. (describing the GET process as "undetectable"); *In re* Pharmatrak, Inc., 329 F.3d at 9, 22 (1st Cir. 2003) (describing Pharmatrak's use of GET requests and then characterizing the process as "code that automatically duplicated part of the communication").

382. *See supra* note 381 and accompanying text.

383. United States v. Eady, No. 14-277, 2015 WL 1735495, at *3 (D.N.J. Apr. 15, 2015).

384. *See* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *3 (N.D. Ill. Mar. 5, 2018) (inferring the possible intended recipients based on the privacy settings a user could select).

interested in the reasonable expectations of a user.[385] Internet users understand that their electronic data is monetized.[386] Advertisers commonly monetize user data.[387] In this way, internet users may reasonably expect to communicate with advertisers when they navigate the internet.

But *Vasil* and *Roden* inferred intent to protect electronic communications, not exempt defendants.[388] A court may disfavor Wiretap Act interpretations that create broad liability exceptions.[389] A user cannot consent to interception simply because the user knows interception is possible.[390] This would limit the Wiretap Act to uninformed plaintiffs. The Wiretap Act does not exempt novel forms of interception.[391] This would limit the Wiretap Act to only the sort of interception a court has seen before. Courts should not limit the Wiretap Act merely because internet users have grown to expect advertisers on the internet. This would limit liability for the pervasive eavesdropper.[392]

If there is any intent to generate a duplicate GET request, it comes from digital advertisers, not internet users. Digital advertisers intend to communicate with internet users when they embed code that will generate the duplicate GET request.[393] But recipient intent is not enough for the party exception.[394] Apple could not invoke the party exception because it designed iPhones to transmit user data to Apple's servers.[395] Samsung could not invoke the party exception because it developed software to transmit user data directly from a user's television to Samsung.[396] Similarly, advertisers should not be able to invoke the party exception because they intentionally manufactured GET requests.

---

385. *See* State v. Roden, 321 P.3d 1183, 1189 (Wash. 2014).

386. *See In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 266 (3d Cir. 2016) (accepting that users understand that their data is not entirely private and that their data is monetized).

387. *See id.*

388. *See Vasil*, 2018 WL 1156328, at *6; *see also Roden*, 321 P.3d at 1189 (concluding that a user's reasonable expectations do not include unaddressed recipients).

389. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020) (disfavoring a statutory interpretation of parties that would allow the "exception to swallow the rule").

390. *See*, *e.g.*, Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the capability of monitoring alone cannot be considered implied consent.").

391. *See supra* note 329 and accompanying text.

392. *In re Facebook*, 956 F.3d at 589, 608 ("The unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion . . . .").

393. *See id.* at 596.

394. *See supra* Part II.C.1.

395. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) ("Apple cannot manufacture a statutory exception through its own accused conduct . . . .").

396. White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *6 (D.N.J. Aug. 21, 2019) ("Plaintiffs allege that Defendants surreptitiously installed software on their televisions that permitted Defendants to track their communications . . . . Defendants' argument that they were parties to these communications is unavailing.").

In sum, users only manifest clear intent to communicate with the websites that the users visit via a URL or hyperlink.[397] A court need not stretch to find some other manifestation of sender intent where the intent is clear. When users clearly intended to communicate with doctors, business associates, or sexual partners, then a court did not search for other exempt parties.[398] Likewise, when websites are unambiguously users' intended recipients via a URL, advertisers receive duplicate GET requests as unintended recipients because websites are the focus of sender intent. As unintended recipients of the data in a GET request, advertisers are ineligible for the party exception.[399]

2. Intended Destinations and GET Request Data

The court in *Pasha* decided whether a communication reached its "destined place" uninterrupted.[400] If so, the recipient was a party.[401] If a telephone call reached its intended telephone, anyone who answered the call was a party.[402] Corporations accessing communications intended for their web servers are parties, too.[403] An unintended recipient tampers with the communication and redirects that communication to an unintended destination in order to gain access.[404] In *Pasha*, the intended destination was explicit because a particular telephone number was dialed.[405] In *Jurgens* and *Crowley*, the intended destinations were implied because the communications had nowhere else to go.[406] These recipients merely accessed communications that were sent to their servers.[407] In *Crowley* this ruled out tampering.[408]

Like *Pasha*'s telephone, the data in an internet user's GET request has an explicit intended destination. The intended destination does not include

397. *See supra* notes 380–83 and accompanying text.

398. *See* Lopez v. Apple, Inc., No. 19-04577, 2021 WL 823122, at *4 (N.D. Cal. Feb. 10, 2021).

399. *See supra* note 135 and accompanying text.

400. United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (quoting Goldman v. United States, 316 U.S. 129, 134 (1942)).

401. *Id.* (concluding that law enforcement had not intercepted the telephone conversations by merely answering the telephone).

402. *Id.* (concluding that answering a telephone was not enough to create liability, while identifying tampering as interception).

403. Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (concluding that the defendant had not engaged in wiretap interception where the defendant "merely received the information transferred" to the defendant onto their server).

404. *See Pasha*, 332 F.2d at 198 ("[T]here was no tampering with the established means of communication." (quoting Goldman v. United States, 316 U.S. 129, 134 (1942))).

405. *See id.* at 196.

406. *See* Jurgens v. Build.com, Inc., No. 17-CV-00783, 2017 WL 5277679, at *5–6 (E.D. Mo. Nov. 13, 2017) (concluding that if there was a communication, then the defendant was a party and that otherwise, there would be no communication); *see also Crowley*, 166 F. Supp. 2d at 1269 ("Amazon merely received the information transferred to it . . . an act without which there would be no transfer. Amazon acted as . . . the second party . . . .").

407. *See supra* note 406 and accompanying text.

408. *See Crowley*, 166 F. Supp. 2d at 1269 (concluding that receiving an email was as benign as answering a telephone).

digital advertisers. Internet users visit a website by entering its URL or clicking on a hyperlink.[409] URLs and hyperlinks include the website's domain name (e.g., "nytimes.com").[410] Each domain name is assigned a unique IP address identifying the location of the website and its content.[411] An IP address is the internet's equivalent of a telephone number.[412] Entering the URL or clicking on a hyperlink generates the GET request containing user data that calls out to that IP address.[413] A website's servers are assigned to the IP address and respond to the GET request with the website's content.[414] Therefore, when users enter a URL or click on a hyperlink, they identify a website as the intended destination.

But unlike *Pasha*, the GET request's data reaches a second destination: the server of a digital advertiser.[415] Nothing in the initial URL or hyperlink identifies digital advertisers' servers as an intended destination. According to *Pasha*, the GET request's data should only reach its intended destination. *Pasha* cannot help advertisers where GET request data reaches an intended destination but also a second unexpected destination.[416]

This result still has all the attributes of an unintended recipient ineligible for the party exception. First, digital advertisers embed the code to generate a duplicate GET request with a second destination.[417] Then, digital advertisers are still acting like a manufactured recipient punished by courts.[418] Second, digital advertisers receive a second GET request with duplicate data. This is still an indicator of *Szymuszkiewicz* interception.[419] Third, digital advertisers engage in this conduct invisibly; courts punish the surreptitious listener.[420]

---

409. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 605, 607 (9th Cir. 2020); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 130 (3d Cir. 2015).

410. *See* Fox, *supra* note 309 ("We typically type nice human-friendly URLs into browsers, like 'khanacademy.org' . . . .").

411. *See id.* ("Those domain names map to IP addresses, the true location of the domain's computers.").

412. *What Is an IP Address?*, GNOME HELP, https://help.gnome.org/users/gnome-help/stable/net-what-is-ip-address.html.en [https://perma.cc/4BCE-N4LH] (last visited Sept. 17, 2021) ("An IP address is similar to [a] phone number . . . . [It] is a unique set of numbers that identifies [a] computer so that it can send and receive data . . . .").

413. *See* Fox, *supra* note 309.

414. *See id.*

415. *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 605, 607 (9th Cir. 2020).

416. *But see* Kerr, *supra* note 26 (concluding that the intended destination case law that exempts an unexpected party merely answering a telephone call is equivalent to "browser info that gets routed to the third party"). This Note argues instead that duplicate GET requests are more akin to a phone call reaching two destinations despite being intended for only one destination. This Note readily concedes Kerr's subsequent argument that the standalone consent exception may exempt many defendants. *See supra* notes 89–91 and accompanying text.

417. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 130 (3d Cir. 2015).

418. *See supra* notes 393–96 and accompanying text.

419. *See supra* notes 321–25 and accompanying text.

420. *See supra* note 383 and accompanying text.

Each of these factors should disqualify advertisers from invoking party status. The intended destination of user data does not rebut this conclusion because the only identifiable intended destination was a website identified by an IP address.[421] That being so, when a duplicate GET request's data is sent to an advertiser's server, the advertiser is an unintended recipient.

Jurgens and *Crowley* offer no support for digital advertisers. There, intended destinations were inferred because there was only one possible recipient.[422] Here, there is already an intended destination and it is the website's servers, not advertisers.[423] With all the indications of interception,[424] and nothing to suggest advertisers' servers were intended,[425] courts can only conclude that advertisers' servers were an unintended destination. Advertisers are thus ineligible for a party exception.

CONCLUSION

User data can be intercepted by duplication and transmission of that data using a second communication.[426] It then follows that duplicate data in a second GET request may indicate interception.[427] Therefore, courts must decide party status by analyzing the user data's intended recipient by assessing manifestations of sender intent or the user data's intended destination.[428] The URLs and hyperlinks users employ to visit websites identify the websites as the intended recipients of user data.[429] The same cannot be said for digital advertisers.[430] Accordingly, digital advertisers are unintended recipients and ineligible for the Wiretap Act's party exception.

If interception on the internet is properly understood, the party exception is unavailable for duplicate GET requests. This Note does not discount the Ninth Circuit's focus on legislative intent to reach the same result.[431] This Note also does not forget the power of consent to otherwise exempt wiretap

421. *See supra* notes 409–14 and accompanying text. Additionally, digital advertisers cannot claim to be part of the destination website and benefit from that intended destination given that advertisers act as "independent parties who [mine] information from other websites" and are not the websites themselves. *See* Graham v. Noom, Inc., No. 20-CV-06903, 2021 WL 1312765, at *5 (N.D. Cal. Apr. 8, 2021) (concluding that *In re Facebook* duplicate GET requests were website-independent, whereas *Graham*'s defendant FullStory was an extension of the website because the user data there was being collected on the website's behalf).

422. *See* Jurgens v. Build.com, Inc., No. 17-CV-00783, 2017 WL 5277679, at *5 (E.D. Mo. Nov. 13, 2017); Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001).

423. *See supra* notes 409–14 and accompanying text.

424. *See supra* notes 417–20 and accompanying text.

425. *See supra* notes 409–14 and accompanying text.

426. *See supra* notes 305–07 and accompanying text.

427. *See supra* notes 308–35 and accompanying text.

428. *See supra* notes 336–75 and accompanying text.

429. *See supra* notes 379–80, 409–14 and accompanying text.

430. *See supra* notes 381–99, 415–25 and accompanying text.

431. *See supra* notes 292–94 and accompanying text.

defendants.[432] Still, examining how data is intercepted on the internet reveals a cacophony of GET requests that are ineligible for the party exception.

432. *See supra* notes 89–91 and accompanying text.