Half Baked: The Need for Clarity on the Party Exemption to the Wiretap Act for Private Actors Using Tracking Cookies

Joseph F. Tower IV*

"Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule."[1]

I. INTRODUCTION

Consumer privacy has been a growing concern among policymakers.[2] As technology advances, the ability to aggregate data about consumer choices and user activity increases.[3] The value of consumer data and behavioral profiles has grown substantially over the past twenty years, incentivizing firms to maximize

* Suffolk University Law School, J.D. 2023; Boston College, M.S. 2020; Boston College, B.A. 2015. Thanks to Professor Renée Landers for her help in developing the topic of this Note. Additionally, thank you to the staff of the *Suffolk University Law Review* for their hard work and corrections on my own Note, and for all of their work for this journal. Lastly, special thanks to my wife Lizz, for all of her support and for her sacrifice in listening to my thoughts on browser cookies for over a year. Also thanks to Lizz for coming up with the title of this Note.

1. Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1684 (2021).

2. *See* MARK R. WARNER, POTENTIAL POLICY PROPOSALS FOR REGULATION OF SOCIAL MEDIA AND TECHNOLOGY FIRMS 1, 14-15 (2017) (arguing for increased regulation of technology firms to address consumer privacy protection). Senator Warner argued in the aftermath of the Cambridge Analytica case, which involved the sale of social media information for electioneering, that technology firms abused their access to consumer data to profit and possibly interfere with electoral processes. *See id.* at 1 (noting importance of technology firms but also their capacity for harmful effects in information ecosystem); Iga Kozlowska, *Facebook and Data Privacy in the Age of Cambridge Analytica*, HENRY M. JACKSON SCH. OF INT'L STUD. (Apr. 30, 2018), https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica [https://perma.cc/ZWX8-KMJU] (detailing Cambridge Analytica case study). Recently, the Biden administration emphasized renewed scrutiny of technology firms in an executive order, including protecting consumer privacy. *See* Promoting Competition in the American Economy, Exec. Order No. 14036, 86 Fed. Reg. 36987, 36988 (July 9, 2021) (addressing unfair data collection and surveillance practices damaging consumer privacy); Richard Lawler & Adi Robertson, *Biden Signs Executive Order Targeting Right to Repair, ISPs, Net Neutrality, and More*, THE VERGE (July 9, 2021), https://www.theverge.com/2021/7/9/22569869/biden-executive-order-right-to-repair-isps-net-neutrality [https://perma.cc/2ZXZ-WVRT] (reporting on executive order to improve economic productivity).

3. *See* Asta Zelenkauskaite & Erik P. Bucy, *A Scholarly Divide: Social Media, Big Data, and Unattainable Scholarship* (Apr. 19, 2016), https://firstmonday.org/ojs/index.php/fm/article/view/6358/5511 [https://perma.cc/C46B-DR92] (explaining value from increased growth in data generated by technology in "Big Data"); WARNER, *supra note* 2, at 4-5 (stating data exhibits economies of scale, providing firms with preexisting data sets with advantages). These firms may use cognitive bias to keep users on their sites and engaged with their products. WARNER, *supra* note 2, at 5 (describing platform policy aggressively commercializes psychological research to create addictive user behavior).

their ability to build individualized consumer profiles.[4] Simultaneously, consumers have difficulty understanding the methods and ubiquity of commercial tracking techniques.[5] The ease of consumer tracking—coupled with a lack of consumer knowledge—leaves little room for the informed consent required for effective privacy protection.[6] With varying success among circuit courts, consumer litigants are utilizing the Wiretap Act—part of the Electronic Communications Privacy Act (ECPA)—to prevent big technology companies from tracking user behavior with browser cookies, which are small text files that web browsers place on user hard drives.[7]

---

4. *See* April Falcon Doss, *Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities that Are Inextricably Linked*, 59 DUQ. L. REV. 231, 260-61 (2021) (setting forth private sector's intrusive data collection and aggregation methods). Private sector data collection methods extend not only to consumers of social media but also to employees in the workplace. *See id.* (listing various methods technologies firms use to monitor employees); *see also* JONATHAN I. EZOR, PRIVACY AND DATA PROTECTION IN BUSINESS: LAWS AND PRACTICES 6-8 (2012) (discussing increased profits firms utilizing data have seen due to technology). As costs to collect and aggregate data have decreased, the benefits that come from selling and collating customer data have increased due to improvements in computing power and the advent of machine learning. *See* EZOR, *supra*, at 6-8.

5. *See* WARNER, *supra* note 2, at 3-4 (arguing users unaware of extent businesses track and sell user browsing habits). *But see* Venky Anant et al., *The Consumer-Data Opportunity and the Privacy Imperative*, MCKINSEY & CO. (Apr. 27, 2020), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative [https://perma.cc/K2G7-LFDS] (arguing high-profile breaches resulted in more cautious consumers).

6. *See* WARNER, *supra* note 2, at 16 (advocating for adoption of explicit consent to third-party data collection to ensure consumers have notice); EZOR, *supra* note 4, at 15-16 (explaining Fair Information Practices (FIP) encourage consumer notice and consent). FIP include policy recommendations that are the foundational principles for privacy policies promulgated by the Department of Homeland Security. *See* HUGO TEUFEL III, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM 1-2 (2009) (noting FIP's influence on many laws at both federal and state level). These principles include transparent use of data; individual participation and consent of the use of data; collection of data for a specified purpose; only data needed to accomplish a specified purpose should be collected; the data's use should be limited to those purposes that the user was notified for; the data should be accurate and complete; the data should be secured against loss or unauthorized access; and the appropriate audits should be implemented. *See* EZOR, *supra* note 4, at 16. The principles are designed to help ensure that a program requiring data collection of individual users will address any possible privacy concerns. *See* TEUFEL III, *supra*, at 3 (noting importance of principles protecting individuals' privacy).

7. *See* Emily A. Jordan, Comment, *Sharing More than You Thought: Facebook Cannot Assert the Party Exception to Avoid Liability Under the Wiretap Act*, 62 B.C. L. REV. ELEC. SUPPLEMENT 205, 208, 212-220 (2021) (advocating for Ninth Circuit's interpretation of ECPA while detailing circuit split). The ECPA is the most recent federal statute regulating the interception of communications and consists of three titles: the Wiretap Act, the Pen Register Act, and the Stored Communications Act (SCA). *See* Orin S. Kerr, *The Next Generation Communications Privacy Act,* 162 U. PA. L. REV. 373, 382-83 (2014) (explaining structure of ECPA). Each of these titles regulate privacy protections for computer technologies to prevent unauthorized interceptions. *See id.* at 382 (discussing Congress's decision to pass ECPA based on fact-finding privacy report). The Pen Register Act regulates the installation of monitoring devices on telephone numbers. *See* Electronic Communications Privacy Act § 301, 18 U.S.C. § 3121(a) (stating no person may install or use pen register or trap and trace device); *see also* Kerr, *supra*, at 382-83 (explaining Pen Register Act makes installing monitoring device to record telephone numbers unlawful). The SCA regulates the privacy protection of electronic communication content when the content is at rest, which is a wiretapping concern distinct from previous because phone conversations were not stored in repositories like emails or other digital artifacts. *See* Kerr, *supra*, at 383 (explaining SCA creates statutory privacy rights for consumers' email services); Electronic Communications Privacy Act § 2701(a)

This Note addresses the question of whether users must give consent to third-party advertisers to collect their data through browser cookies.[8] Third-party advertisers argue an exception to the Wiretap Act—known as the party exemption rule—permits the use of cookies to collect users' data without their knowledge.[9] The party exemption rule allows a party to a communication to record or "intercept" that communication as long as they do not do so for a tortious purpose.[10]

In 2020, the Ninth Circuit Court of Appeals revisited the Wiretap Act's party exemption rule as applied to tracking techniques used in internet browsers.[11] In *Davis v. Facebook*, users brought a class action suit against Facebook for its use of browser cookies to track users without their consent.[12] These cookies generated copies of users' browser communications and sent those copies to Facebook's servers.[13] In holding that Facebook's use of surreptitious and simultaneous parallel communications violated the ECPA, the court weighed in on an ongoing debate of how the party exemption rule applies to the use of browser-

(barring unlawful access to stored electronic communications). The Wiretap Act regulates the interception of communications as "point-to-point" occurrences. *See* JULIAN S. MILLSTEIN ET AL., DOING BUSINESS ON THE INTERN-ET § 10.03[c][i] (stating ECPA protects communications traveling through cyberspace). The Wiretap Act has its history in previous statutes regulating the interception of oral and wire communications; the ECPA adds "electronic communications" to the list of communications actors may not intercept unless they fall within delineated exceptions. *See* Kerr, *supra*, at 378-79 (identifying early state and federal statutes forbidding interceptions of telephone calls); *id.* at 382 (discussing interception of computer data transmissions to Wiretap Act to provide new privacy protections); Electronic Communications Privacy Act § 2511 (barring interception and disclosure of electronic communications).

8. *See infra* Part III.B (advocating for updated wiretapping protections for users).

9. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (arguing users intended to send separate communication and advertiser intended recipient).

10. *See* CHARLES DOYLE, CONG. RSCH. SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 12-13 (2012) (defining consent exception); Jordan, *supra* note 7, at 209 (explaining when party exception rule applies).

11. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (holding party exemption does not cover surreptitious duplication akin to interception of communications), *cert. denied*, 141 S. Ct. 1684 (2021). *Davis* deals with the use of "GET" requests, the method in which a website accesses a cookie and named after the command the website follows—GET—to access that cookie from plug-ins that track the browsing habits of Facebook users while they are logged out of their Facebook profiles. *See id.* at 607. Facebook is a social media platform that allows users to build profiles with their own generated content. *See* Facebook, Inc., Annual Report (Form 10-K) 5 (Dec. 31, 2018), https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm [https://perma.cc/6EAH-8HR6]. Users then "friend" other users, linking profiles together so they can browse each other's content. *See id.* Facebook generates revenue from this service by collecting and aggregating user data and then selling advertisements based on consumer profiles generated with Facebook's collected data. *Id.* Internet browsers are applications that run on a user's computer and connect with webservers, providing the user with access to the content hosted on the webserver. *See* Sandra Grauschopf, *Internet Browsers: A Simple Guide to How Browsers Work*, LIVEABOUTDOTCOM (Feb. 21, 2022), https://www.liveabout.com/what-is-internet-browser-892819 [https://perma.cc/PQF5-GAGC] (explaining browser gateway to internet).

12. *See Davis*, 956 F.3d at 596 (stating suit concerns collection of user referrer headers via cookies on browsers, violating user privacy).

13. *See id.* at 607 (noting Facebook's code directs browser to send duplicate GET request to its server).

tracking technologies.[14] The court reasoned that the use of deceitful means to induce a user to create a parallel browser communication violated the intent behind the party exemption rule.[15] Armed with this recent ruling, private parties and state attorneys general filed an increasing number of claims in state courts against entertainment and technology companies utilizing different website tracking methods.[16]

In contrast, in *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, the Third Circuit interpreted the party exemption rule as applicable when a browser sends an intended communication to a webserver, even if the user is deceitfully induced to make that communication.[17] This ruling protects advertisers from liability when using browser cookies to "copy" user internet traffic generated by browsing websites.[18] Despite being faced with the circuit courts' contrasting approaches to the party exemption rule, the Supreme Court denied certiorari on Facebook's appeal of the *Davis* decision, leaving the circuit split unaddressed.[19]

---

14. *See id.* at 607-08 (expanding on reasoning of First and Seventh Circuits); United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (holding contemporaneous duplication of communications constitutes interception under ECPA); Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 22 (1st Cir. 2003) (holding not "two separate communications," but rather one, intercepted communication). Browser-tracking technologies ubiquitously include cookies. *See What Are Cookies?*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/cookies [https://perma.cc/FH7A-JFRS] (defining cookies).

15. *See Davis*, 956 F.3d at 608 (reasoning website-duplicated GET requests stretches definition of intended recipients).

16. *See* Laura A. Mazzuchetti & Alysa Z. Hutnik, *Privacy Litigation Trend: The Latest on Session Replay Lawsuits, and Practical Considerations for Risk Mitigation*, AD L. ACCESS (May 21, 2021), https://www.adlawaccess.com/2021/05/articles/privacy-litigation-trend-the-latest-on-session-replay-lawsuits-and-practical-considerations-for-risk-mitigation [https://perma.cc/L97A-ARVF] (discussing rise of litigants following *Davis*).

17. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 141-42 (3d Cir. 2015) (holding communications sent to intended party even if party deceived communicator); *see also* Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 CARDOZO L. REV. 669, 697 (2012) (discussing third party's duties if first party does not consent to interception).

18. *See In re Google*, 806 F.3d at 143 (holding advertisers can become party to communication by deceit).

19. Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021) (denying certiorari). A class action suit alleged Facebook tracked user browsing habits while those users were logged out of their Facebook accounts. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 596-97 (9th Cir. 2020) (defining class of plaintiffs Facebook tracked until blogger disclosed tracking practices in 2011), *cert. denied*, 141 S. Ct. 1684 (2021). The plaintiffs claimed Facebook utilized "plug-ins" that existed on third-party websites which surreptitiously tracked user behavior including sensitive information; collected the user's identity; collected the webserver's identity; collected the name of the web page and the search terms the user used to find it; and used that behavior to build consumer profiles which Facebook then sold to advertisers. *See id.* at 596 (discussing collection of associated referrer headers and internet protocol addresses). These "plug-ins" tracked user behavior without the knowledge of either the user or the operators of the third-party websites. *See id.* at 602 (stating Facebook's privacy disclosures failed to report continued tracking when users logged out). After these tracking practices had been disclosed, the Federal Trade Commission initiated a lawsuit, which later settled, alleging Facebook had engaged in deceptive trade practices. *See* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises [https://perma.cc/6CRU-H68W] (reporting settlement of Federal Trade Commission

This Note argues that a uniform approach to the application of the Wiretap Act is required to resolve confusion about the use of common technology among social media firms, search engines, and online advertisers so as to protect consumers' reasonable expectations of privacy against abuse.[20] This Note details the historical approaches among the circuits, as well as the legislation defining party exemption.[21] It then analyzes the merits of the circuit courts' competing interpretations to explore practical solutions to interceptions by browser cookies.[22] This Note concludes by offering an interpretation of the party exemption rule that will ensure adaption to changing technology, arguing that explicit user notice and consent prioritizes the legislature's intent to protect private communications from third-party intrusions.[23]

II. HISTORY

A. Wiretapping Legislation and Previous Iterations of the Wiretap Act

Statutes regulating the interception of communications in the United States have their roots in the regulation of the telephone and telegraph.[24] While these devices were advanced at the time and allowed for easy communications over vast distances, they were also unsecure.[25] A person could listen in on conversations by attaching a rod along the telephone wire, giving rise to the name "wiretap."[26] Both governmental and private actors have used wiretaps to access

---

complaint). In the aftermath of *Davis*, private litigants and state attorneys general have sought to expand the interpretation of the Ninth Circuit by filing claims asserting ECPA violations against technology and entertainment companies that use similar tracking methods. *See* Kristin Bryan & Alexis Chandler, *Session Replay Software Litigation: The Hot Data Privacy Litigation Trend Already Reaching the End of the Line*, CONSUMER PRIV. WORLD (July 22, 2021), https://www.consumerprivacyworld.com/2021/07/session-replay-software-litigation-the-hot-data-privacy-litigation-trend-already-reaching-the-end-of-the-line [https://perma.cc/QTV7-R6BC] (discussing likelihood wiretap ligation based on session replay will succeed).

20. *See infra* Part III (arguing benefits of uniform approach to ECPA).

21. *See infra* Part II (outlining jurisprudence interpreting elements of ECPA for private actors).

22. *See infra* Part III (discussing competing arguments of circuit courts in application of party exemption).

23. *See infra* Part IV (advocating for updated application of ECPA party exemption rule).

24. *See* Kerr, *supra* note 7, at 378 (discussing privacy flaws of telephones compared to earlier telegraphs). Early surveillance laws regulated access to telephone lines as these had no security preventing unauthorized access by individuals. *See id.* at 378-79 (analyzing security of communication forms). State legislatures passed the early anti-wiretapping laws soon after the invention of the telephone in the 1880s. *See id.* (noting early responses to concerns about maintaining private communications).

25. *See id.* (explaining states passed privacy laws to address "breaking in" to telephone conversations). The "wiretapper" only needed some simple tools and physical proximity to access a phone call carried in a telephone wire. *See id.* at 378 (showing ability to access "new" communications). Due to the physical requirements for wiretapping a call, legislation often focused on the act of intercepting the call. *See id.* at 378-79 (providing history of tools required to intercept telephone calls).

26. *See id.* (describing means required to tap into telephone wire). A simple tap requires a user to scrape insulation from a telephone wire and then connect a receiver via an extension wire that the user attached with metal clips; at that point, the person is a party to the conversation. *See* Meyer Berger, *Tapping the Wires*, THE NEW YORKER (June 11, 1938), https://www.newyorker.com/magazine/1938/06/18/tapping-the-wires [https://pe-

telephone conversations, prompting many state legislatures to pass their own laws regulating wiretaps.[27]

In *Katz v. United States*,[28] the Supreme Court held that the use of warrantless wiretaps by a government entity constituted an unreasonable search in violation of the Fourth Amendment.[29] *Katz* concerned the investigation of a sports bettor via the wiretapping of a phone booth.[30] The Court held that this warrantless wiretapping constituted an invasion of Katz's right to privacy, stating the Fourth Amendment "protects people, not places."[31] Further, the Court introduced the concept of an individual's "reasonable expectation of privacy," which requires both a personal, subjective expectation of privacy, and an objective, societal recognition of privacy.[32]

At the federal level, Congress took steps to regulate the use of wiretaps.[33] In 1934, Congress passed the Federal Communications Act, and its comments focused on the importance of user privacy.[34] Congress then passed the Wiretap

---

rma.cc/8Y77-RGSC**]** (discussing author's experience with wiretaps).

27. *See* April White, *A Brief History of Surveillance in America, Smithsonian Mag*., (Apr. 2018), https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ [https://perma.cc/U-Q82-543J] (discussing private corporations and private detectives using wiretaps). Private parties used wiretaps since their inception, while government agents began to utilize wiretaps with the beginning of Prohibition. *See id.* (explaining stockbrokers used wiretaps to gain market advantage).

28. 389 U.S. 347 (1967).

29. *See id.* at 359 (holding government wiretapping of phone booth violated Fourth Amendment). *Katz* overruled *Olmstead v. United States*, which had reasoned that telephones are not subject to Fourth Amendment protections because, unlike mail by postage, the communications wires carry cannot be searched. *See id.* at 353; 277 U.S. 438, 464 (1928) (explaining United States does not have custody of telephone messages, unlike mail). The jurisprudence evolved further to interpret the Fourth Amendment as applicable to wiretapping into telephone calls, which constitutes an impermissible search of the communication. *See* Berger v. New York, 388 U.S. 41, 64 (1967) (holding New York electronic eavesdropping statute violated Fourth Amendment). Congress then passed the Omnibus Crime Control and Safe Streets Act in 1968, which included its own Wiretap Act and protected against the interception of telephone calls between parties to a communication. *See* Kerr, *supra* note 7, at 379 (discussing evolution of Communications Act of 1934 to Wiretap Act of 1968); Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 82 Stat. 197, 211-25 (1968) (codified at 18 U.S.C. §§ 2510–2523). This Act required government interceptions of telephone conversations via wiretaps to minimize the amount of intercepted information to only necessary components. *See* Kerr, *supra* note 7, at 379-80 (discussing requirements of government interceptions under 1968 Act).

30. *See Katz*, 389 U.S. at 348 (noting facts of case).

31. *See id.* at 351 (distinguishing between exposing communications to public and seeking to preserve privacy of communications in booth).

32. *See id.* at 361 (Harlan, J., concurring) (outlining two-prong test).

33. *See* Kerr, *supra* note 7, at 374-75 (discussing changes in technology prompting updated statute). The Office of Technology Assessment (OTA) published a report that warned of the growth of email communications, which were not covered under the 1968 Wiretap Act. *See id.* at 380-81 (discussing email's lack of telephone line use, thus not triggering Wiretap Act of 1968); United States v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978) (holding hacker monitoring network traffic does not violate Wiretap Act). Congress addressed these concerns by passing the ECPA, designed to protect electronic data both in storage and in transit. *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (enacting session law).

34. *See* Communications Act, Pub. L. No. 73-418, 48 Stat. 1064 (1934) (passing law).

Act of 1968—the basis for the current wiretapping statute.[35] The Act focused on wire and oral communications between at least two private parties.[36] At that time, however, much of the jurisprudence surrounding wiretaps concentrated on protecting against unauthorized government wiretaps.[37] Wiretaps were primarily a method to conduct criminal investigations rather than a method to intercept private calls.[38] The methods available—either for a private party or the government—to conduct a wiretap of telephones—the most common communication channel—were easily employed, but required physically tapping the phoneline.[39]

While Congress aimed to restrict the interception of wire communications, they also acted to expand protections to communications made through the fast-growing internet.[40] In 1986, Congress passed the ECPA, which revised the Wiretap Act of 1968.[41] The ECPA included provisions protecting data at rest; data that is "in storage" as opposed to being transferred between parties; and metadata—defined as the "routing information" of electronic data.[42] Congress determined that communications "in transit" require separate protections and ultimately passed the updated Wiretap Act.[43] Using the prior Wiretap Act of 1968 as a model, the Wiretap Act of 1986 states that it is illegal to "intentionally intercept [o]r procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[44]

This statute is further limited by the ECPA, which includes the exceptions to liability under the Wiretap Act.[45] One delineated exception is the party

35. Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 82 Stat. 197, 212-13 (1968) (codified as amended at 18 U.S.C. § 2510); *see* Kerr, *supra* note 7, at 379 (discussing history of Wiretap Act).

36. *See* Omnibus Crime Control and Safe Streets Act § 801.

37. *See* Howard J. Kaplan et al., *The History and Law of Wiretapping*, ABA 1, 3-4 (Apr. 20, 2012), https://www.americanbar.org/content/dam/aba/publications/litigation_news/29-1-history-and-law-of-wiretapping.pdf [https://perma.cc/8X8Z-L6VP] (explaining jurisprudence of Supreme Court wiretapping history).

38. *See* Kerr, *supra* note 7, at 379 (outlining history of Fourth Amendment concerns of prior wiretapping statutes).

39. *See* Kaplan et al., *supra* note 37, at 3, 5 (highlighting methods available for wiretapping investigations).

40. *See* Kerr, *supra* note 7, at 380-81 (discussing effect of 1985 OTA report on impact of email).

41. *See id.* at 382-83 (noting passage of ECPA).

42. *See* Electronic Communications Privacy Act § 201, 18 U.S.C. § 2701(a) (creating protections for data at rest in Stored Communications Act); *id.* § 301, 18 U.S.C. 3121(a) (establishing protections against use of pen register in Pen Register Statute). "Data at rest" refers to electronic data that is stored—either on a hard drive, on servers, in the cloud, or some other capacity—instead of data parties communicate at that moment, which is data in transit. *See id.* § 2701(a) (stating actor may not divulge stored data under this statute unless exceptions apply); *see also* Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 274-76 (2013) (noting privacy protection concerns after recipient receives electronic communication). Metadata refers to the information that describes other data, such as author, creation date, or file size. *See* Garry Kranz, *Metadata*, WHATIS.COM (July 2021), https://whatis.techtarget.com/definition/metadata [https://perma.cc/9VQH-RQDM] (providing definition of Metadata).

43. *See* Kerr, *supra* note 7, at 383 (explaining purpose of different standards for protecting data at rest and data in transit).

44. Electronic Communications Privacy Act § 101, 18 U.S.C. § 2511(1)(a).

45. *See* Electronic Communications Privacy Act § 102, 18 U.S.C. § 2511(2) (providing five explicit exceptions to liability under Wiretap Act). These exceptions to liability for interceptions include providers of wire and

exemption, which allows a party to a communication to "intercept" the contents of the communication without incurring any liability under the Wiretap Act so long as one party has given consent.[46] The Wiretap Act defines electronic communication as "[a]ny transfer of signs, signals, writing, images, sounds, data, or intelligence . . . transmitted . . . by a wire, radio, electromagnetic, photoelectronic or photooptical system."[47] Browser communications between computers through the use of cookies fall within the Act's definition of communications.[48]

In implementing the ECPA and the revised Wiretap Act, Congress intended to balance the privacy expectations of individuals and businesses with the realities of technology.[49] In particular, Senator Charles Mathias noted that "inadvertent overhearing" should not be penalized—the Act should only cover intentional acts of interception.[50] Congress cited the alliance of different stakeholders supporting privacy-centric goals, providing carveouts for law enforcement purposes, as one reason why it passed the Act.[51] During the ratification process, senators highlighted the ECPA's goal to "enhance the privacy of Americans and update the provisions of the 1968 wiretap act."[52] In light of these goals, Senator Mathias described the Act as "uncontroversial," and President Reagan signed it into law on October 21, 1986.[53]

---

electronic communications services, authorized law enforcement interceptions, the use of pen registers or trap and trace devices, electronic communications readily accessible to the public, and where a person is party to a communication or has given prior consent to such an interception. *Id.* (delineating situations where interceptors avoid liability).

46. *See id.* § 2511(2)(c)-(d) (listing party exemption rules); DOYLE, *supra* note 10, at 13 (outlining rationale for party exemption rule to Wiretap Act). The Supreme Court held this consent exemption constitutional, reasoning that a speaker on a telephone already "risks the indiscretion of his listeners." *See* DOYLE, *supra* note 10, at 13 (discussing Court's reasoning against Fourth Amendment challenge); *see also* United States v. White, 401 U.S. 745, 751 (1971) (holding party consent to recording satisfies Fourth Amendment). The speaker is in no worse a position due to the other party's indiscretion simply because that other party chose to record or transmit the speaker's statements instead of repeating them verbally. *See* DOYLE, *supra* note 10, at 13; *White*, 401 U.S. at 751 (emphasizing no difference between immediately writing down conversation after consent and recording conversation with consent).

47. Electronic Communications Privacy Act § 101, 18 U.S.C. § 2510(12); *see also* DOYLE, *supra* note 10, at 11-12 (discussing intentionally broad scope of term electronic communications).

48. *See* DOYLE, *supra* note 10, at 11-12 (explaining communications encompassed by amended Act).

49. *See* 132 CONG. REC. 14,451 (1986) (statement of Sen. Charles Mathias) (asserting expectation of privacy when using technology).

50. *See id.* (distinguishing between inadvertent and intentional acts for liability).

51. *See* 132 CONG. REC. 4046 (1986) (statement of Rep. Robert Kastenmeier) (articulating unusual nature of coalition supporting privacy measures of Act).

52. *See* 132 CONG. REC. 14,451 (1986) (statement of Sen. Charles Mathias) (noting House Judiciary Committee passed Act by unanimous vote).

53. *See* 132 CONG. REC. 4045 (1986) (statement of Rep. Robert Kastenmeier) (highlighting wide range of support from business organizations); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); Nicole Ozer, *Online Privacy Law Turns a Quarter of a Century Old Today*, ACLU (Oct. 21, 2011) https://www.aclu.org/news/civil-liberties/online-privacy-law-turns-quarter-century-old-today#:~:text=Today%2C%20the%20Electronic%20Communications%-20Privacy,Reagan%20signed%20ECPA%20into%20law [https://perma.cc/CY3P-6QYF].

B. Browser Communications

Companies use electronic communications to track the behavior of users that visit their websites.[54] Companies often use browser cookies as a unique identifier for individual users.[55] A browser cookie is a small text file that a website places on a user's common directory of their hard drive.[56] The website that a user visits injects a cookie onto the user's browser the moment they connect with that website.[57] When the user revisits that website, the site recognizes the cookie that sat on the user's browser since their last visit to the site, allowing the company to tailor aspects of its website to the recognized user who visits.[58]

There are always at least two parties to the communication when a user visits a website—the user and the webserver itself—which often places at least one cookie on the user's browser.[59] The manner in which a user's web browser sends a message to the desired website to display its contents is called a GET request, which acts as a "digital call and response."[60] Third parties may also

54. *See* Fern L. Kletter, Annotation, *Claims Concerning Use of "Cookies" to Acquire Internet Users' Web Browsing Data Under Federal Law*, 36 A.L.R. Fed. 3d Art. 5 § 2 (2022) (discussing how information cookies show how user interacted with website). Many websites use software that accesses stored cookies on the user's computer, which extrapolates information regarding the user's behavior, including pages they visited, the time they visited these pages, and products they bought. *See id.* (explaining software designed to predict user behavior). From this information, the program can further determine the user's name, their browsing habits, and other user information. *See id.* (showing innocuous information can build profile with personal information).

55. *See id.* (discussing websites use cookies to identify users); Jordan, *supra* note 7, at 210 (detailing evolution of data collection by cookies); *see also* Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, VOX (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy [https://perma.cc/KU67-C4WC] (explaining websites use cookies to monitor users and to provide information about their transactions); Per Fries, *Getting Valid Cookie Consent as Part of Ensuring Compliance in the Collection of Data*, PRECIS (Mar. 2, 2020), https://www.precisdigital.com/blog/getting-valid-cookie-consent-as-part-of-ensuring-compliance-in-the-collection-of-data [perma.cc/H2HQ-JRPA] (raising compliance, consent and jurisdictional concerns when collecting personally identifying information of users). Companies may attach these identifiers to users to market the website to the specific interests of the user. *See* Kletter, *supra* note 54, § 2 (stating operator of website accesses cookie each time user visits website to gather information). Cookies on a user's computer can also help improve the connection between the user's browser and the website by establishing a connection faster while improving the performance of the website. *See What Are Cookies?*, *supra* note 14 (explaining beneficial functions of cookies).

56. *See What Are Cookies?*, *supra* note 14 (defining cookies); Kletter, *supra* note 54, § 2 (noting technical information of cookies).

57. *See What Are Cookies?*, *supra* note 14 (discussing HTTP cookies created upon start of browser connection with website); *see also In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 131 (3d Cir. 2015) (explaining cookie advertising methods Google uses to target ads to users).

58. *See* Kletter, *supra* note 54, § 2 (tailoring websites based on cookies found on user device). The website matches the unique cookie created with a "name-value" that corresponds to saved information from the user's previous sessions. *See What Are Cookies?*, *supra* note 14 (comparing cookies to getting unique tickets at coat checks).

59. *See* Kletter, *supra* note 54, § 1 (emphasizing different actors required to establish connection through web browser).

60. *See* David Koenig, Note, *Cacophony or Concerto?: Analyzing the Applicability of the Wiretap Act's Party Exception for Duplicate GET Requests*, 90 FORDHAM L. REV. 951, 954 (2021) (explaining GET requests).

communicate with the user when that user visits a website.[61] A webserver may host third parties, like advertisers purchasing space on the webserver's page.[62] These third parties often also place cookies on the user's browser when the user visits the webserver.[63] The cookies from the visited webserver are referred to as "first-party cookies" while those cookies from the third parties the website hosts are referred to as "third-party cookies."[64]

Consumers using web browsing services are frequently unaware of the extent to which cookies track their behavior, even if they are generally aware that companies track their behavior.[65] Consumers often do not know background

---

61. *See In re Google*, 806 F.3d at 130 (describing third-party advertiser access to user browser session). Even if the user has enabled a cookie blocker, the third party is able to place cookies on a user's hard drive without their knowledge by exploiting loopholes in the feature. *See id.* at 132 (noting cookie blockers have built-in exceptions allowing third-party cookies access to users); Jordan, *supra* note 7, at 211 (discussing third-party placement of cookies through deceitful means).

62. *See In re Google*, 806 F.3d at 131 (highlighting business model of selling advertising directed toward users visiting website). The process of selling individually tailored webpage advertisements using third-party cookies has become a ubiquitous web service practice. *See id.* (noting cookie-based tracking commonplace).

63. *See* Michal Wlosik & Michael Sweeney, *What's the Difference Between First-Party and Third-Party Cookies?*, CLEARCODE (Nov. 21, 2022), https://clearcode.cc/blog/difference-between-first-party-third-party-cookies [https://perma.cc/Q8QV-5867] (discussing differences between types of cookies). While first- and third-party cookies have no technical differences, they have different purposes. *See id.* (explaining both cookies carry same information). First-party cookies are often considered benign because the host webserver creates them, and they are commonly known to provide services tailored to help the host website perform better. *See id.* (listing beneficial services of first-party cookies). Third-party cookies often have negative connotations, and scholars associate them with privacy violations because unsolicited advertisers often use them to track users. *See* Jordan, *supra* note 7, at 210-12 (noting companies placing third-party cookies on user hard drives surreptitiously). These tracking cookies continue to gather information on users as they visit other websites because cookies are not restricted to only gathering information from the domain that created them; rather, any website that can access the third party's code. *See* Wlosik & Sweeney, *supra* (defining technical process behind third-party cookies). Once the user visits any website that utilizes the same webserver used by the third-party advertiser, the third-party server matches the existing cookie to the identity of the user. *See id.* (discussing ad-retargeting services assigning cookies to users to retarget them on other websites). Both first- and third-party cookies have malicious and beneficial purposes, despite popular industry beliefs. *See id.* (explaining malicious first-party cookies and beneficial third-party cookies).

64. *See supra* note 63 and accompanying text (defining differences between first- and third-party cookies).

65. *See* Kletter, *supra* note 54, § 2 (noting lack of user knowledge and assent to embedded cookies on computer). At the same time, Pew Research Center reported that roughly 72% of Americans believe that advertisers and technology firms track most of what they do online. *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/FVF4-YN9Q] (discussing survey of 4,272 adults regarding government and private data collection). Additionally, the same research states that 81% of Americans think the potential risks of private companies collecting their data outweigh the benefits. *See id.* (reporting Americans have become more conscious of privacy concerns from both private and government actors). These reports highlight that Americans are suspicious of targeted advertising and believe the benefits are limited. *See id.* (explaining Americans find increased targeted advertisements invasive). But, consumers are more willing to allow tracking and data collection if they are aware of a stated purpose. *See id.* (providing scenarios in which consumers would consent to data-tracking policies); John Koetsier, *IDFA Survey: 62% of Consumers Will Not Allow App Tracking in iOS 14*, SINGULAR (Mar. 4, 2021), https://www.singular.net/blog/i-

processes occur when they visit each website—they simply seek to use the webpage's service.[66] Nevertheless, when a "popup" banner appears on users' screens asking them to accept cookies, users usually decline the option to allow cookies on their hard drives because cookies can negatively affect their computers by decreasing performance and introducing malware.[67] Advertisers thus argue users must not actually care about the "loss in privacy" that occurs through third-party tracking, as users would refuse to pay for currently free internet services in order to prevent third parties from tracking them.[68]

C. Simultaneous Communications and Interceptions

An interception that violates the Wiretap Act must involve the acquisition of the communication's content.[69] Under the Act, content is defined as anything that "concerns the substance, purport, or meaning of the communication."[70] In *Smith v. Maryland*,[71] the Supreme Court held that the means of establishing a communication is distinct from the contents of the communication.[72] *Smith*

---

dfa-survey [https://perma.cc/D6QE-JLH3] (stating over 50% of survey respondents would allow tracking if they knew data collection purpose).

66. *See* Kletter, *supra* note 54, § 2 (discussing consent element of websites placing cookies on user hard drives); *see also* Meg Leta Jones & Jenny Lee, *Comparing Consent to Cookies: A Case for Protecting Non-Use*, 53 CORNELL INT'L L.J. 97, 106 (2020) (explaining advertisers' continued tracking of users who "opted-out" of cookie-based tracking).

67. *See* WARNER, *supra* note 2, at 2-3, 16-17 (arguing user's lack of knowledge of web tracking techniques makes consent meaningless); Marilyn Lavin, *Cookies: What Do Consumers Know and What Can They Learn?*, 14 J. TARGETING, MEASUREMENT & ANALYSIS FOR MKTG. 279, 281 (2006) (finding consumers change internet behavior based on perceived likelihood of cookie placement on computers); *see also* Anant et al., *supra* note 5 (noting consumer concerns towards privacy and consumer data use). In recent years, consumers have become more wary of cookies and increasingly use cookie-blocking programs to prevent websites from placing cookies on their hard drives without their knowledge. *See* Lavin, *supra*, at 283 (demonstrating increased use of cookie blockers worldwide). Importantly, numerous cookie blockers differentiate between first- and third-party cookies, allowing many customers to reject third-party cookies while continuing to accept first-party cookies. *See id.* at 284 (showing many cookie blockers marketed to consumers focus on third-party cookies).

68. *See 8 in 10 Americans Say They Value Online Privacy—But Would They Pay to Protect It?*, PANDA MEDIA CTR. (Sept. 11, 2021), https://www.pandasecurity.com/en/mediacenter/security/how-much-is-my-data-worth [https://perma.cc/DX7G-LNUQ] (noting discrepancy between Americans concerned about online privacy and Americans willing to pay for privacy). Security experts consider whether Americans would rather hand over personal information to technology companies if they will not pay for services in lieu of data collection; if not, they may not value data privacy if the alternative is to pay upfront costs to preserve it. *See id.* (noting Americans may misvalue data privacy evidenced by lack of willingness to pay).

69. *See* Electronic Communications Privacy Act § 101, 18 U.S.C. § 2510(8); *id.* § 2511(1)(c)-(e).

70. Electronic Communications Privacy Act § 101, 18 U.S.C. § 2510(8); *see In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 136 (3d Cir. 2015) (discussing difference between intercepted content and noncontent in electronic communications).

71. 442 U.S. 735 (1979).

72. *See id.* at 743 (reasoning content of phone conversation private unlike number person dialed). The Court applied a two-factor test to determine if a wiretapped conversation constituted an impermissible seizure: whether the person making the comments had an actual expectation of privacy, and whether the expectation of privacy is one that society recognizes as reasonable. *See id.* at 740 (outlining inquiry to determine whether legit-

concerned the warrantless use of a pen register—a device that records all telephone numbers called from a particular phone—in a criminal investigation of a robbery.[73] The Court held that the Fourth Amendment only protects the content of the communication, thereby allowing authorities to use pen registers in investigations without a warrant.[74] The ECPA update to the Wiretap Act similarly differentiated between the signaling information—as detailed in the Pen Register Act of the ECPA—and content of communications—as detailed in the Wiretap Act of the ECPA.[75] The line between content governed by the Pen Register Act and the Wiretap Act for locational information as defined by *Smith* has evolved to a case-specific inquiry into whether the role of the location-identifying portion of a communication is protected content, unprotected metadata, or both.[76]

By their nature, electronic communications are easily duplicated and recorded when the sender uses those services.[77] In a telephone conversation, a wiretapper listens to an ongoing conversation by accessing the "stream" of signals between two conversers, gaining real-time access to the communications.[78] This access

---

imate expectation of privacy exists); *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (creating test for expectation of privacy for wiretapping).

73. *See Smith*, 442 U.S. at 737 (stating police placed register on Smith's telephone line to confirm threatening calls to victim). Telephone companies routinely used pen registers as a part of their business model; users must convey their telephone numbers so that those companies can route their calls. *See id.* at 742 (recognizing reasonable telephone users aware of lack of phone number privacy).

74. *See id.* at 743 (reasoning Smith's conduct may keep contents of conversation private, but not number dialed). As consumers voluntarily turn over their numbers to telephone companies—third parties to the conversation—they should not expect that information to be private. *See id.* at 742-45 (concluding society would not recognize reasonable expectation of privacy for dialed numbers).

75. *See In re Google*, 806 F.3d at 136 (highlighting statutory distinction between content and noncontent identical to *Smith* holding); H.R. REP. NO. 107-236, at 53 (2001) (confirming intent to legislate *Smith* ruling).

76. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 136-37 (3d Cir. 2015) (discussing when location identifier in URL becomes substance of communication instead of communication's routing function). This case-specific distinction need not separate these communications conclusively into the content category or the metadata category; they may serve both functions. *See id.* at 137 (discussing opinion from Foreign Intelligence Surveillance Court). Often, electronic metadata can be more sensitive than the contents of the communications themselves, requiring courts to apply the protections of the Wiretap Act to the metadata as well as the contents of the communications. *See* Graf v. Zynga Game Network, Inc. (*In re* Zynga Priv. Litig.), 750 F.3d 1098, 1108-09 (9th Cir. 2014) (holding URLs content if reproduce words from search query); *see also* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (noting capture of URLs, despite having metadata characteristics, could fail *Katz* privacy test for wiretaps); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1029-30 (2010) (stating difficulty in differentiating between content and noncontent in context of URLs and search queries).

77. *See* Davis v. Facebook, Inc. (*In re* Facebook Inc. Internet Tracking Litig.), 956 F.3d 589, 607 (9th Cir. 2020) (discussing duplication of GET requests by cookies copying referrer header to Facebook server), *cert. denied*, 141 S. Ct. 1684 (2021); *In re Google*, 806 F.3d at 140 (stating websites would duplicate GET requests from users and send to third party); United States v. Szymuszkiewicz, 622 F.3d 701, 704 (7th Cir. 2010) (explaining duplication and forwarding of emails through packet switching); Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 22 (1st Cir. 2003) (arguing strict interpretation of interception eschewing duplicated communications via cookies defeats purpose of Wiretap Act).

78. *See supra* note 26 and accompanying text (discussing mechanics of wiretapping telephone conversations by breaking into phone line).

to a communication is different than the commonly available methods of electronic wiretaps because the third-party wiretapper may obtain a copy of the electronic communication between the parties by inducing the original sender to send that copy to the third party.[79] Thus, the third-party wiretapper may not access the communication between the intended parties at all, but instead access a separate copy of the communication.[80]

In these instances, an analysis of whether the Wiretap Act applies to an interception may focus on the data transferred in the communication rather than which of the two identical communications was intercepted.[81] For instance, if a user browsing a website sends a communication—information such as their URL and IP address—to the webserver by visiting the site, a third-party advertiser that placed a cookie on the user's hard drive may send a "request" to the user to send an additional copy of that communication with their URL and IP address to the third party.[82] Privacy advocates note that an interception of a copy of the communication may defeat the Wiretap Act's purpose of preventing outside parties from accessing the contents of a communication because a copy the user did not intend to make could be accessed.[83]

D. Scope of Consent to Communications Interception

The party exemption rule to the Wiretap Act is premised on the communicator giving consent to an interception of the communication.[84] It is often referred to

79. *See In re Google*, 806 F.3d at 140, 143 (explaining duplication of GET requests when visiting web page to populate content).

80. *See id.* at 141 (noting user web browsers communicate directly with Google servers independent of communications with desired webserver); *see also* Koenig, *supra* note 60, at 956 (asserting duplicate communication separate and requires own analysis to determine if interceptor party).

81. *See* Koenig, *supra* note 60, at 957 (arguing analysis for duplicated communications should focus on data transmitted instead of communication itself).

82. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 140 (3d Cir. 2015) (noting web browser's instruction to send second GET request for advertising purposes).

83. *See* Jordan, *supra* note 7, at 223 (arguing Wiretap Act intended to prevent "eavesdropping" on conversations). The congressional purpose of the Wiretap Act was to safeguard the privacy of communications. *See* S. REP. NO. 90-1097, at 2233, 2236-37 (1968) (stating Act should safeguard right to privacy).

84. *See* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 21 (1st Cir. 2003) (discussing lack of client consent to interception of consumer data based on use of product). A party's consent may extend to all, some, or none of the intercepted communications, necessitating that courts review the dimensions of the consent to determine whether the interception has exceeded those boundaries. *See* Griggs-Ryan v. Smith, 904 F.2d 112, 119 (1st Cir. 1990) (explaining parameter of consent circumscribed depends on specific facts). The scope of consent is focused on whether the party had notice of the interception, rather than the party's subjective knowledge of the interception. *See id.* at 119 (disagreeing lack of subjective knowledge meant lack of implied consent to recording). Additionally, courts have interpreted the word "intercept" in the Wiretap Act broadly, as the conventional definition, "to seize or interrupt in progress or before arrival," is so narrow that any electronic recording outside the scope of consent may be allowable under the Wiretap Act. *See In re Google*, 806 F.3d at 144 (rejecting Google's contention they did not "intercept" communications); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (noting "intercept" meaning contemplated by Wiretap Act broader than ordinary definition).

as the consent exemption, in that one of the parties to the communication has consented to an interception of that communication.[85] The interception is valid if it is within the scope of what a party has consented to—the interception cannot exceed the bounds of the consented to transmission.[86] Courts have determined that a party must give actual consent, explicitly or implicitly, to the interception.[87] Implied consent to an interception is permissible only when the party should have knowledge of the interception based on the surrounding circumstances.[88] Courts that permit implied consent to interceptions often focus their inquiries on whether the party has notice of the interception, rather than whether the party is subjectively aware of the interception.[89]

The scope of who should consent to an interception of a communication is partly a question of who the Wiretap Act recognizes as a party to a communication, and thus whom may give consent to the interception.[90] At the state level, some legislatures have passed wiretapping legislation narrowing the contours of the party exemption rule by requiring all parties to a communication to consent

85. *See* DOYLE, *supra* note 10, at 12-14 (outlining ECPA party exemption synonymous with "consent exception").

86. *See supra* note 84 and accompanying text (discussing limited scope of consent and circumstantial inquiry into scope).

87. *See Blumofe*, 329 F.3d at 19 (stating conditions for implied consent though constructive consent insufficient); Williams v. Poulos, 11 F.3d 271, 281-82 (1st Cir. 1993) (explaining consent, either express or implied, determined by surrounding circumstances); *Griggs-Ryan*, 904 F.2d at 119 (holding implied permission for recording); United States v. Verdin-Garcia, 516 F.3d 884, 894-95 (10th Cir. 2008) (determining consent implied from prison phone use). A court will only recognize implied consent—meaning without actual notice—if the surrounding circumstances can show convincingly that the party knew about and consented to the interception. *See Griggs-Ryan*, 904 F.2d at 119 (showing Griggs-Ryan impliedly consented to recording because Smith told her what to expect).

88. *See Blumofe*, 329 F.3d at 20 (stating surrounding circumstances must convincingly show party knew of interception).

89. *See Williams*, 11 F.3d at 281-82 (acknowledging Poulos informed of monitoring of call thus had at least minimal knowledge).

90. *See* Koenig, *supra* note 60, at 956 (noting eavesdroppers not included within scope of parties whom may give consent to interception).

to its interception.[91] These rules, like the federal Wiretap Act, apply to electronic communications as well as telephonic communications.[92]

Some courts recognize party status in the recipients to a communication or in other individuals through affirmative acts of a defendant.[93] Affirmative acts of a defendant often refer to participation in a conversation.[94] Alternatively, affirmative acts can intimate an active service a defendant provides to another party as a "known participant" to a communication.[95] Party status as a recipient to a communication allows an entity to whom a conversation is directed to be a party—just as the Wiretap Act envisioned.[96] In order for a communication to be subject to the Wiretap Act, there must be at least one sender and one recipient to the

91. *See* DOYLE, *supra* note 10, at 80 (charting state consent exceptions to wiretapping statutes). Currently, there are fourteen states that have some version of "all party consent" exemptions to their own wiretapping statutes—analogues to the federal Wiretap Act. *See* CAL. PENAL CODE § 632 (Deering 2023); CONN. GEN. STAT. § 52-570d. (2022); FLA. STAT. § 934.03 (2022); 720 ILL. COMP. STAT. §§ 5/14-2 to -3 (2022); MD. CODE. ANN., CTS. & JUD. PROC. § 10-402 (LexisNexis 2023); MASS. GEN. LAWS ch. 272, § 99 (2022); MICH. COMP. LAWS § 750.539c (2022); MONT. CODE ANN. § 45-8-213 (2020); N.H. REV. STAT. ANN. § 570-A:2 (2022); OR. REV. STAT. § 165.540 (2022); 18 PA. CONS. STAT. § 5704 (2022); WASH. REV. CODE § 9.73.030 (2022); Lane v. Allstate Ins. Co., 969 P.2d 938, 941 (Nev. 1998) (interpreting Nevada statute to require all party consent). Importantly, these state exemptions only apply to their own wiretapping laws and not the federal Wiretap Act. *See* DOYLE, *supra* note 10, at 13-14 (discussing state analogues to Wiretap Act applying only to their respective state statutes). They do, however, provide alternatives to the federal model allowing only one party to a communication to *intercept* and record a communication without the consent of the other parties to the communication. *See id.* (stating Wiretap Act compliance does not exempt one from state liability).

92. *See* PENAL § 631 (prohibiting recording of confidential communications by telephone or other device except radio); § 934.03(2)(d) (requiring consent to intercept contents of wireless communications between electronic devices); § 5/14-2 (forbidding interception of electronic communications without all parties' consent); § 750.540 (mandating all parties' consent to read or copy contents of messages sent between electronic devices); § 45-8-213(1) (disallowing recording of electronic communication without consent of all parties); § 9.73.030-(1)(a) (proscribing unlawful recording by telephone, telegraph, radio, or other device). California has created its own data privacy regime that may legislate areas the federal Wiretap Act currently covers. *See* Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, 33 BERKELEY TECH. L.J. 131, 163 (2018) (highlighting differences between California statutory requirements for operating in state and Wiretap Act requirements).

93. *See* Koenig, *supra* note 60, at 962 (arguing affirmative acts path to become party to conversation).

94. *See* Caro v. Weintraub, 618 F.3d 94, 97-98 (2d Cir. 2010) (stating affirmative acts like conversing at kitchen table may grant defendant party status). Congressional intent supports the idea that affirmative acts may confer party status to a defendant. *See* S. REP. NO. 90-1097, at 2236 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112 (asserting "party" should mean person participating in conversation). This definition of "party" is contrasted with a possible "unseen auditor" that may intercept communications. *See* United States v. Eady, 648 F. App'x 188, 192 (3d Cir. 2016) (reasoning Congress intended to restrict party status to those taking part in conversations); *see also* S. REP. 90-1097, at 2154 (recognizing "unseen auditor" impacts privacy of active participants in conversation).

95. *See* Zak v. Bose Corp., No. 17-CV-02928, 2019 U.S. Dist. LEXIS 54871, at *9 (N.D. Ill. Mar. 31, 2019) (concluding information intentionally routed to app for functionality, indicating app known participant in communication); *see also* Koenig, *supra* note 60, at 962 (discussing affirmative acts first method to become party to conversation).

96. *See In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 274 (3d Cir. 2016) (stating communications on Viacom's website makes Viacom party to those communications); United States v. Szymuszkiewicz, 622 F.3d 701, 705 (7th Cir. 2010) (defining communication consisting of sender and recipient); *see also* Koenig, *supra* note 60, at 964 (arguing "recipient status" second possible path to becoming party to conservation).

communication.[97] The sender must have intended to send the communication for the recipient to become a party.[98]

Other courts, however, have focused their inquiries not only on whether a sender intended to make communications, but also whether the communication reached the intended recipient.[99] These inquiries distinguish intended recipients—those who should receive the benefit of the party exemption rule—from unintended recipients.[100] The behavior of the actual recipient of the communication can indicate whether they are the intended recipient.[101] For instance, manufactured recipients use techniques that purposefully cause the user to send a communication to them, leading some courts to hold that the sender lacks the requisite intent to communicate for the defendant to be a party.[102] While surreptitious listeners invisibly listen to a communication, that alone does not vitiate their status as parties to a communication.[103] Courts that recognize this status have also held a defendant is a surreptitious listener only if they intrude on a communication that would exist without the defendant's participation.[104]

The *In re Google Inc.* opinion discusses whether the Wiretap Act party exemption protects communications made by deceptive methods.[105] The essential issue is whether the communication is intended, and if so, whether the communicating party is fully informed of the identity of the party receiving the

97. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (acknowledging, tautologically, every communication involves at least two parties).

98. *See id.* at 143 (focusing analysis on voluntariness of communication, not certainty of identity of intended recipient). *But see* Koenig, *supra* note 60, at 964 (favoring communications to identifiable intended recipients for party exemption); Jordan, *supra* note 7, at 223 (stating unknown third-party interception of communication contrary to legislative intent).

99. *See* Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1042 (N.D. Cal. 2014) (rejecting party status when finding Apple not intended recipient of messages); Koenig, *supra* note 6060, at 965 (noting intentionality factor in determining party status).

100. *See* Koenig, *supra* note 60, at 965 (noting unintended recipients often do not qualify for party exemption rule to Wiretap Act). *Compare* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (holding receiving communication sufficient for party status), *with Backhaut*, 74 F. Supp. 3d at 1042 (requiring finding Apple intended recipient of communication).

101. *See* Koenig, *supra* note 60, at 968 (distinguishing between manufactured recipients and surreptitious listeners).

102. *See* White v. Samsung Elecs. Am., Inc., No. 17-1775, 2019 WL 8886485, at *6 (D.N.J. Aug. 21, 2019) (discussing "smart" televisions requiring transmission of viewing preferences due to intentional software design); Koenig, *supra* note 60, at 968-69 (arguing behavior another model to render recipient ineligible for party exemption); *see also* Allen v. Quicken Loans Inc., No. 17-12352, 2018 WL 5874088, at *5 (D.N.J. Nov. 9, 2018) (stating website's design to transmit user data required for functionality).

103. *See Allen*, 2018 WL 5874088, at *5 (finding lack of user knowledge of interception does not prevent Quicken from claiming party status); *see also* Koenig, *supra* note 60, at 969-70 (opining not every surreptitious interception makes defendants ineligible for party status).

104. *Compare White*, 2019 WL 8886485, at *6 (determining no party status when surreptitiously intercepting communications), *with Allen*, 2018 WL 5874088, at *5 (providing Quicken intended recipient despite surreptitious actions because those actions facilitate intended communications).

105. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 132 (3d Cir. 2015) (discussing defendant surreptitiously exploiting loopholes in internet browser cookie blockers).

communication.[106] In *United States v. Pasha*,[107] the Seventh Circuit distinguished communications a party makes to an intended recipient whose identity is unknown from communications made to a known recipient.[108] In determining whether the party exemption applies, courts consider whether the communicator intends to make those communications to the other party, not whether the communicator knows with whom they are communicating.[109]

E. Notice of Other Party's Presence

A communication between two parties requires not only that there be a sender and a recipient, but also that the sender is aware of the presence of the recipient.[110] While courts have held that the sender may be unaware of the identity of the recipient, they have also recognized that Congress intended the Wiretap Act to prevent "unseen auditors" from having access to a communication.[111] Knowledge of the other party's presence in a communication helps to provide purpose to the communication and notice to the communicator that its contents may be recorded.[112]

---

106. *See id.* at 143 (addressing argument of circumvention of cookie blocker should vitiate defendant's party status).

107. 332 F.2d 193 (7th Cir. 1964).

108. *See id.* at 198 (holding no interception when unaware defendant dials law enforcement instead of other defendant); *see also In re Google*, 806 F.3d at 144 (relying on *Pasha*). The *Pasha* court drew the distinction between reaching out to a wrong or unintended party and a party that has overheard a communication between two parties, indicating a narrower definition of interception. *See Pasha*, 332 F.2d at 198 (stating active surreptitious overhearing of conversation not equivalent to facts of case). Further, the *Pasha* court indicated impersonation of the intended receiver is not synonymous with interception as considered by the federal wiretap statute at the time. *See id.* (acknowledging little difference between law enforcement answering "yes" and explicitly impersonating intended receivers). Additionally, the Fifth and Sixth Circuits have found the *Pasha* interpretation of impersonating an intended receiver applicable to the federal wiretap acts in force at the time. *See* Clemons v. Waller, 82 Fed. App'x 436, 442 (6th Cir. 2003) (arguing Congress-intended impersonation of intended receiver does not preclude party status by citing *Pasha*); United States v. Campagnuolo, 592 F.2d 852, 863 (5th Cir. 1979) (stating Congress likely intended to reaffirm result in *Pasha* through passing 1968 Wiretap Act).

109. *See Pasha*, 332 F.2d at 198 (explaining Pasha's belief he spoke with other defendants over telephone); Billeci v. United States, 184 F.2d 394, 397 (D.C. Cir. 1950) (discussing appellants' lack of knowledge of identity of person taking bets over telephone). While the identity of a participant may not be dispositive in determining whether a defendant is a party to a communication, the Wiretap Act does require that the defendant's presence is known to the other participants. *See* United States v. Eady, 648 Fed. App'x 188, 192 (3d Cir. 2016) (noting jury instructions correctly state defendant not participant in conversation unless presence known); *see also Pasha*, 332 F.2d at 198 (contrasting lack of knowledge of identity with outside third-party eavesdropping on conversation).

110. *See In re Google*, 806 F.3d at 143 (stating communication involves at least one sender and one recipient).

111. *See supra* note 94 and accompanying text (differentiating between participants in conversation to unseen auditors listening in).

112. *See* Koenig, *supra* note 60, at 963 (noting recipient's active participation in conversation can confer party status).

The party exemption rule's rationale is that it is logical to assume that the other party may divulge the contents of a communication to outsiders.[113] Thus the party exemption rule follows the logic that if one party can transcribe and gossip about the contents of a telephone conversation at the end of a telephone call, then that party should not be held liable for recording that same conversation.[114] If either party to a telephone conversation records that telephone conversation, they are effectively "intercepting" their own communications, despite there being another party involved in the conversation.[115] Without the knowledge that there is another party to a communication, the communicator has no notice that the contents of that communication may be intercepted.[116]

F. Circuit Split Between Third Circuit and First and Ninth Circuits

The First Circuit addressed the use of cookies to assist in third-party user tracking in *In re Pharmatrak, Inc*.[117] *In re Pharmatrak, Inc.* dealt with pharmaceutical companies that invited users to their websites to learn about their drugs and obtain rebates.[118] Pharmatrak was a company that provided a database service to pharmaceutical companies and collected user personally identifiable information (PII) through cookies to make intra-industry comparisons, despite providing assurances to the pharmaceutical companies and the webusers that Pharmatrak did not collect PII.[119] While Pharmatrak argued companies using its services had consented to this PII-tracking policy by contracting with Pharmatrak, the court reasoned that the party exemption rule cannot be invoked through the "casually inferred consent" of a party to a communication.[120] Additionally, the users themselves certainly did not consent to the interception, as the

113. *See* DOYLE, *supra* note 10, at 13 (explaining argument in favor of consent interception when speaker risks indiscretion of listeners); *see also* United States v. White, 401 U.S. 745, 751 (1971) (discerning no difference between writing down speaker's statements and recording those statements).

114. *See* DOYLE, *supra* note 10, at 13 (asserting recording in real time and transcribing contents of conversation later functionally same).

115. *See* Rauvin Johl, *Reassessing Wiretap and Eavesdropping Statutes: Making One-Party Consent the Default*, 12 HARV. L. & POL'Y REV. 177, 181-82 (2018) (arguing eavesdropping interceptions often imply involvement of third party).

116. *See* CTR. FOR DEMOCRACY & TECH., AN OVERVIEW OF THE FEDERAL WIRETAP ACT, ELECTRONIC COMMUNICATIONS PRIVACY ACT, AND STATE TWO-PARTY CONSENT LAWS OF RELEVANCE TO THE NEBUAD SYSTEM AND OTHER USES OF INTERNET TRAFFIC CONTENT FROM ISPS FOR BEHAVIORAL ADVERTISING 9-10 (2008), https://cdt.org/wp-content/uploads/privacy/20080708ISPtraffic.pdf [https://perma.cc/ZA7L-QFSJ] (stating implied consent may require explicit notice of monitoring, not only knowledge of capacity).

117. *See* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 14 (1st Cir. 2003) (noting use of "persistent cookie" to track users visiting webpages monitored by NETcompare).

118. *See id.* at 12 (explaining purpose of Pharmatrak service to assist pharmaceutical companies by comparing website traffic within industry).

119. *See id.* (stating companies urged they did not want users' PII).

120. *See id.* at 19-20 (reasoning consent implied only when surrounding circumstances show party knew about interception).

websites gave no indication that a third party—Pharmatrak—was collecting their PII.[121]

The Third Circuit later decided that third-party browser cookie GET requests could receive the benefit of the party exemption rule, relying on a series of articles exposing the practice of secretly placing cookies to track user web browsing in the aftermath of revelations that technology companies were evading users' cookie blockers.[122] In *In re Google Inc.*, the world's most-used search engine allowed third-party advertisers to place cookies onto the hard drives of users.[123] Many users enabled "cookie blockers" to prevent third-party advertisers from tracking their activity with browser cookies, but Google designed third-party cookies that bypassed these cookie blockers, frustrating the intent of users.[124] These third-party cookies continued to send duplicates of users' communications with their intended website servers to third-party advertisers without the users' knowledge.[125] The court held that users intended to communicate with the third-party advertisers by interacting with the host website through their web traffic.[126] The court also held that the Wiretap Act's party exemption rule turns on whether the user intended to communicate with the other party, despite the fact that many

121. *See Blumofe*, 329 F.3d at 21 (showing websites gave no indication to users informing use meant third parties would collect PII).

122. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 141 (3d Cir. 2015) (discussing use of cookies to track user activity for advertisers without user knowledge). *In re Google Inc.* has its roots in an article that Stanford graduate student Jonathan Mayer published in 2012. *See* Jonathan Mayer, *Safari Trackers*, CTR. FOR INTERNET AND SOC'Y (Feb. 17, 2012), http://cyberlaw.stanford.edu/blog/2012/02/safari-trackers [perma.cc/K4QX-B36U] (identifying tracking cookies circumvent Safari web browser cookie blockers); *see also In re Google*, 806 F.3d at 132 (highlighting Mayer article). Similarly, blogger Nik Cubrilovic published an article in 2011 highlighting Facebook's harvesting of user data and tracking their browsing of other websites with cookies that users were unaware of. *See* Nik Cubrilovic, *Facebook Re-Enables Controversial Tracking Cookie*, NIK CUBRILOVIC (May 5, 2022), https://nikcub.me/posts/facebook-re-enables-controversial-tracking-cookie [https://perma.cc/K8GT-FJLD] (revealing Facebook cookie tracks users after logging out of user accounts); *see also* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 596-97 (9th Cir. 2020) (highlighting Cubrilovic blog), *cert. denied*, 141 S. Ct. 1684 (2021). These articles revealed that a number of technology companies, including the *In re Google Inc.* and *Davis* defendants, had discovered methods to avoid common cookie blockers and had used those methods to continue to harvest additional data from their users. *See Davis*, 956 F.3d at 596-97 (stating blog prompted FCC investigation and lawsuit); *In re Google*, 806 F.3d at 132 (pointing out article prompted lawsuit).

123. *See In re Google*, 806 F.3d at 130 (discussing technical elements involved in placing third-party cookies on user hard drives for advertising purposes).

124. *See id.* at 131 (noting web browsers designed built-in features to prevent installation of cookies by third-party servers). As cookies have become more ubiquitous, so have cookie blockers. *See id.* (explaining prevalence of "default opt-out" cookie blockers).

125. *See id.* at 132 (detailing how Google's code sent hidden forms to trigger cookie blocker loopholes without consumer knowledge).

126. *See id.* at 141 (stating users sent transmissions directly to third-party servers rather than sending through first-party website).

users did not know the other party receiving the web traffic was a third-party advertiser using third-party cookies.[127]

The Ninth Circuit, however, reached the opposite conclusion.[128] In *Davis*, a class action suit alleged Facebook violated the Wiretap Act by surreptitiously collecting duplicate communications from users through the use of duplicate GET requests that Facebook's cookies generated from users' hard drives.[129] The Ninth Circuit rejected Facebook's argument that it was a party to those communications.[130] The court reasoned the Third Circuit had erred in its interpretation of the Wiretap Act in the *In re Google Inc.* case and instead held that the surreptitious nature of establishing the communication would frustrate the congressional intent of the Wiretap Act.[131]

III. ANALYSIS

A. Nonconsensual Duplication of GET Requests Does Not Constitute a Separate Communication

The Ninth Circuit's interpretation more accurately reflects the congressional purpose of the Wiretap Act than the Third Circuit's.[132] In *Davis*, the Ninth Circuit posited that, as the Wiretap Act does not define the term "party" in its exemption, the circuit courts must construe this definition themselves.[133] Each of the Wiretap Act cases relied upon by the Ninth Circuit concerned whether the establishment of a duplicated communication between a user and a third party should be protected due to the third party's status as a "party" to the communication.[134] The Third Circuit, alone, affords third parties an exempt status in such a duplicated communication, indicating that it is out of step with much of the

127. *See In re Google*, 806 F.3d at 143 (asserting party takes part in conversation, regardless of whether intended recipient procured conversation through fraud).

128. *Compare* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (holding simultaneous and unknown duplication and communication of GET requests do not establish party status), *cert. denied*, 141 S. Ct. 1684 (2021), *with In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (holding defendants intended recipients of duplicated GET requests and thus established party status to communication).

129. *See Davis*, 956 F.3d at 596 (explaining use of plug-ins to trigger cookies to send user website history to Facebook servers).

130. *See id.* at 608 (concluding Wiretap Act party exemption does not apply).

131. *See id.* at 609 (applying interpretation of First and Seventh Circuits to duplicate GET requests).

132. *See* Jordan, *supra* note 7, at 224-25 (arguing entrance into conversation by deceit eviscerates purpose of Wiretap Act).

133. *See Davis*, 956 F.3d at 607 (discussing circuit split to define "party").

134. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 607 (9th Cir. 2020) (outlining other circuit approaches), *cert. denied*, 141 S. Ct. 1684 (2021); *see also* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (stating secret forwarding of email does not confer party status); Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 22 (1st Cir. 2003) (holding surreptitiously duplicated cookie transmission cannot create party status).

jurisprudence on this issue.[135] The third party's placement of the cookie is done surreptitiously when the user visits a website.[136] Once the third party has placed a cookie on the user's hard drive, it can remain there indefinitely, continuing to gather information about the user's activities.[137] The user often does not know the cookie is sending this information, and, in many cases, the user has enabled cookie blockers to prevent third parties from placing these cookies in the first place.[138] In *Davis*, the users had logged out of their Facebook accounts when visiting other websites, and Facebook's promulgated privacy policy stated it would not track users who had logged out.[139] Despite this, Facebook plugins continued to generate GET requests of logged out users, sending a duplication of the communication between the user and the first-party website directly to Facebook.[140] Similarly, in *In re Google Inc.*, the users had enabled cookie blockers specifically to prevent the placement of third-party cookies on their hard drives.[141] Despite this, Google crafted methods to circumvent these cookie blockers in order to place third-party cookies.[142]

As the third parties are not "party" to exempt communications, the communications are not protected because the user has no knowledge they are occurring.[143] A "communication" that only one party is aware of is not the sort of communication the Wiretap Act protects.[144] A communication requires both a sender, who intends to the send the communication, and a recipient.[145] The Third Circuit states that the user "intends" to send the duplicated GET request containing third-party cookie triggers because the user intends to make a communication with that same content—they simply fail to realize the identity of the recipient.[146]

135. *See* Jordan, *supra* note 7, at 207 (arguing Ninth Circuit's holding deepens Third Circuit's minority position).

136. *See supra* note 63 and accompanying text (explaining creation of third-party cookies when user visits first-party websites).

137. *See* Jones & Lee, *supra* note 66, at 99 n.16 (noting cookies collect information without customer knowledge and require manual deletion from computers).

138. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 132 (3d Cir. 2015) (discussing exploits of cookie blockers).

139. *See Davis*, 956 F.3d at 596, 602 (highlighting Facebook privacy policy contradicts practices).

140. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 596 (9th Cir. 2020) (alleging plug-ins trigger duplicated GET request), *cert. denied*, 141 S. Ct. 1684 (2021).

141. *See In re Google*, 806 F.3d at 131 (noting cookie blockers enabled to prevent third-party cookie placement).

142. *See id.* at 132 (describing circumvention of cookie blockers).

143. *See supra* note 109 and accompanying text (explaining how knowledge of other party's existence can come through active participation in conversation).

144. *See supra* note 94 and accompanying text (discussing "unseen auditors" ineligible for party exemption).

145. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (emphasizing two parties required for communication).

146. *See id.* at 143 (stating users sent GET requests voluntarily, even though induced by deceit).

The court assumes this inducement to send a GET request is tantamount to an intent to communicate.[147]

The Third Circuit's holding, however, does not reflect the caselaw's understanding of the intent to communicate, or the common user's understanding of whom they intend to communicate with.[148] In *In re Google Inc.*, the court relied on *Pasha*'s holding that the communicator does not need to know the identity of the party they are communicating with to establish a communication.[149] The Third Circuit concluded that the plaintiffs voluntarily transmitted GET requests thinking that they were communicating with the first-party website.[150] These duplicated communications, however, are dissimilar to the protected telephone conversations in *Pasha*.[151] In a telephone conversation, a third party does not "induce" the sender to make a duplicated phone call to another number beyond the one originally dialed.[152] The *Pasha* court further stressed that there was no "tampering with the established means of communication," and "the officer was the immediate party to the call."[153] This contrasts with the facts of *In re Google Inc.*, in which the third parties "tampered" with the users' hard drives by surreptitiously placing browser cookies to create the transmission at issue.[154] The Third Circuit failed to discuss the difference between browser cookies and telephones when comparing the facts to *Pasha*.[155]

Further, the Third Circuit's holding does not reflect the congressional intent of the Wiretap Act.[156] Congress intended to exclude "unseen auditors" of communications from the Act's definition.[157] This exclusion helps protect the parties' reasonable expectation of privacy by ensuring that *only* the intended

147. *See id.* (emphasizing voluntariness of communication).

148. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (joining other circuit interpretations because interpretations more consistent with congressional intent), *cert. denied*, 141 S. Ct. 1684 (2021).

149. *See In re Google*, 806 F.3d at 143-44 (suggesting Congress implied one who impersonates intended receiver party to communication); United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (holding impersonation on phone call not Wiretap Act violation).

150. *See In re Google*, 806 F.3d at 143 (arguing voluntary nature of transmission dispositive rather than deceit involved in transmission).

151. *Compare In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 141 (3d Cir. 2015) (showing secondary copy of cookie transmission occurs alongside intended transmission), *with Pasha*, 332 F.2d at 198 (holding defendant intentionally dialed recipient telephone number).

152. *See Pasha*, 332 F.2d at 198 (determining defendant voluntarily called recipient number).

153. *See id.* (noting officer did not tamper with telephone line).

154. *See In re Google*, 806 F.3d at 141 (stating Google cookie, which allows Google to identify users, placed by circumventing user privacy settings).

155. *See id.* at 144 (focusing *Pasha* analysis on holding stating impersonation of intended receiver party to communication).

156. *Compare* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (asserting Congress intended to prevent acquisition of messages by unseen auditors), *cert. denied*, 141 S. Ct. 1684 (2021), *with In re Google*, 806 F.3d at 144 (explaining Congress, by referencing *Pasha*, intended to include parties gaining entrance into communication by deceit).

157. *See Davis*, 956 F.3d at 608 (discussing unseen auditors in congressional record).

recipients have access to the contents of the communication.[158] Allowing a third party to break into a communication and trigger a new unintended communication defeats the statute's privacy-centric purpose.[159] The rationale behind the party consent exemption is that the sender of a communication already risks the indiscretion of the receiver.[160] When speaking on a telephone, the other party may divulge the contents of the speaker's communications orally to third parties, or the other party may record the communication and distribute it.[161] In either instance, the speaker can generally converse freely with the expectation the communication will remain private if they trust the other party.[162] It is typically the speaker's knowledge of the other party's existence that puts them on notice the communication may be intercepted.[163] The Third Circuit's rule that any communication, regardless of the sender's intent to send it, can be intercepted by an unknown party authorizes the very unseen auditors that the Wiretap Act intends to protect against.[164]

B. User Consent Ensures Notice of Browser Communication

In order to ensure the user has the requisite intent to communicate with the third-party advertiser through browser cookies, the third party should obtain the user's consent to place a browser cookie on their hard drive.[165] The Wiretap Act party exemption requires only that one party consents to an interception.[166] Browser cookies, however, can create additional communications unbeknownst to the user.[167] This is unlike a oral conversation, where both parties are actively aware and participating in ongoing communication.[168] By receiving the user's

158. *See id.* (emphasis added) (prohibiting entity from engaging in unauthorized duplication and forwarding of unknowing user information).

159. *See* Jordan, *supra* note 7, at 224-25 (stating Ninth Circuit decision upholds purpose of Wiretap Act).

160. *See* DOYLE, *supra* note 10, at 13 (noting argument in favor of consent interceptions).

161. *See id.* (risking "indiscretion of his listeners").

162. *See id.*

163. *See, e.g.*, United States v. Verdin-Garcia, 516 F.3d 884, 894-95 (10th Cir. 2008) (discussing notice given when stating prison telephone conversations not private due to knowledge of monitoring); Griggs-Ryan v. Smith, 904 F.2d 112, 114-15 (1st Cir. 1990) (stating landlord told tenant she recorded all incoming phone calls on communal line). When talking on a telephone, the speaker generally knows that there is a listener on the other end, but an unsophisticated user visiting a website may not understand the role that cookies play in creating new communications. *See supra* note 67 (considering user knowledge of cookies).

164. *See* Jordan, *supra* note 7, at 224-25 (allowing third parties to fraudulently access communication would not protect data against commonplace intrusions).

165. *See supra* note 87 and accompanying text (distinguishing between actual and constructive consent to interception).

166. *See* Electronic Communications Privacy Act § 102, 18 U.S.C. § 2511(2)(d) (requiring one party to consent to interception).

167. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 596 (9th Cir. 2020) (describing second and separate GET request undetectable by user), *cert. denied*, 141 S. Ct. 1684 (2021).

168. *See* Caro v. Weintraub, 618 F.3d 94, 97-98 (2d Cir. 2010) (noting active participation in kitchen conversation provides notice of party's presence).

consent for duplicated GET requests, a third party can ensure the user is aware a communication is occurring and that the third party may record portions of that communication.[169]

User consent may be either explicit or implicit in order to achieve the policy goal of the Wiretap Act party exemption rule.[170] Explicit consent ensures the user is aware another communication is occurring and of the purpose behind that communication.[171] For browser cookies, the third party seeking to place the cookie on a user's hard drive need only have the user's affirmative consent to accept the cookie when visiting a website.[172] It is not a difficult technical feat to provide a banner that requests the user's consent to this interception.[173] Armed with this consent, the third-party advertiser may continue to use these browser cookies to track the behavior of consenting users, and those users will have adequate notice that protects their privacy interests, which are central to the Wiretap Act.[174]

Implicit consent may similarly achieve the policy goal of the Wiretap Act party exemption rule by ensuring users have actual notice that third parties may place cookies on their hard drives when accessing websites.[175] Just as a telephone call containing a warning that a call may be recorded can provide the appropriate notice, websites can furnish similar warnings that their sites host third-party advertisers and their cookies may share user information.[176] This notice helps to address the privacy concerns raised in *Davis* and *In re Google Inc.* regarding the surreptitious tracking of user behavior by duplication of GET requests.[177]

169. *See* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 21 (1st Cir. 2003) (emphasizing in cookie tracking cases deficient notice always defeats claims of consent); Griggs-Ryan v. Smith, 904 F.2d 112, 118 (1st Cir. 1990) (considering relation between express notice and consent).

170. *See Blumofe*, 329 F.3d at 19, 24 (stating actual consent required, either explicit or implied).

171. *See* WARNER, *supra* note 2, at 16 (arguing explicit consent to third-party data collection ensures notice).

172. *See Blumofe*, 329 F.3d at 21 (rejecting argument users consent to interception simply by visiting website).

173. *See* Fries, *supra* note 55 (discussing European requirements to provide banner notification of cookie data collection on websites).

174. *See* Jones & Lee, *supra* note 66, at 121-23 (pointing out types of cookies which could require user's consent while preserving cookie functionality); Jordan, *supra* note 7, at 224-25 (affirming privacy interests central to Wiretap Act).

175. *See* Fries, *supra* note 55 (discussing use of banners to provide notice of cookie data collection).

176. *See id.* (advising importance of providing notice of data collection).

177. *See* Davis v. Facebook, Inc. *(In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (worrying court allowing most common methods of intrusion would cause exception swallowing rule), *cert. denied*, 141 S. Ct. 1684 (2021); *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (noting court troubled by various interception deceits).

IV. CONCLUSION

A persistent circuit split on the scope of the Wiretap Act as applied to browser cookies is unacceptable; it leaves both users and advertisers uncertain about the legality of these interceptions. Users are unable to trust that their web browsing will not be intercepted by technology firms, even if those firms explicitly state that they do not use cookies to do so. Additionally, advertisers equipped with commonly used cookies cannot collect data about their consumers without fear of liability. Without federal uniformity, the outcome of a suit on internet advertising practices is dependent on the circuit in which a prospective plaintiff files suit.

Prioritizing the consent of the user when determining which party's consent should control for browser cookie interceptions provides certainty for all parties in a communication and ensures the user is aware of an interception. It is the simplest mechanism to follow the statute, regardless of which circuit's interpretation is "correct." Emphasizing consent also follows the legislative intent to protect the privacy of communications, and it is sensible policy that a user should have notice their browser is making additional communications with third parties.

The solution of providing notice to the user by requiring affirmative consent has gained traction in other jurisdictions. California, for example, requires by statute that users affirmatively consent to the placement of any cookies that intercept browser communications. While this requirement is a step in the right direction, federal law should make clear that the Wiretap Act party exception should prioritize the user's consent over a third-party auditor's consent.