Boston College Law Review

Volume 62
Issue 9 *Electronic Supplement*

Article 13

4-6-2021

Sharing More Than You Thought: Facebook Cannot Assert the Party Exception to Avoid Liability Under the Wiretap Act

Emily A. Jordan
Boston College Law School, emily.jordan.2@bc.edu

SHARING MORE THAN YOU THOUGHT: FACEBOOK CANNOT ASSERT THE PARTY EXCEPTION TO AVOID LIABILITY UNDER THE WIRETAP ACT

Abstract: On April 9, 2020, the United States Court of Appeals for the Ninth Circuit, in *Davis v. Facebook, Inc.* (*In re Facebook*), held that unauthorized third parties receiving simultaneous, direct copies of a party's communication do not fall within the scope of the Party Exception of the Wiretap Act, 18 U.S.C. § 2510–2523. In doing so, the Ninth Circuit, based its holding on the legislative history and purpose of the Wiretap Act and reasoned that the Party Exception requires a narrow construction. Further, it held that to interpret the exception as inclusive of actors like Facebook risks eviscerating the scope of the Wiretap Act entirely. With its decision, the Ninth Circuit joined the First and Seventh Circuits, deepening the circuit split with the Third Circuit over the judicial interpretation of the Wiretap Act. This Comment argues that the Ninth Circuit's understanding of the Act is correct because it protects the integrity of the Wiretap Act and adheres to the legislative intent to broadly protect individuals' privacy.

INTRODUCTION

In 1968, Congress passed the Wiretap Act (the Act) which prohibited the interception of telephonic and wire communications.[1] The evolution of legisla-

[1] *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 379 (2014) (describing that the Wiretap Act (the Act) took the place of the Communications Act of 1934). The Communications Act was the first federal surveillance law, and it regulated wire and radio communications. *See id.* (noting that the Act and the Communications Act both concerned privacy protections); *see also* 47 U.S.C. §§ 151–609 (containing the Communications Act). After Congress enacted the Communications Act, the public's rights under the Fourth Amendment began to conflict with the justice system's need for wiretapping. *See* Catherine R. Gellis, Note, *Copysense and Sensibility—How the Wiretap Act Forbids Universities from Using P2p Monitoring Tools*, 12 B.U. J. SCI. & TECH. L. 340, 343–44 (2006) (stating that the Communications Act could have banned wiretapping, but the courts restricted its scope to physical invasions). This tension culminated in two critical Supreme Court cases, *Olmstead v. United States* in 1928 and *Berger v. New York* in 1967. *See* Olmstead v. United States, 277 U.S. 438, 465 (1928) (holding that governmental wiretapping does not violate the Fourth Amendment as an unlawful search and seizure), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); *see also* Berger v. New York, 388 U.S. 41, 44, 63 (1967) (concluding that a New York wiretapping statute violated the Fourth and Fourteenth Amendments because it allowed for trespassory invasions of private space in reliance on a warrant that lacked probable cause). In 1968, Congress referenced the standards that the Supreme Court outlined in 1967, in *Katz v. United States*, when developing the Act. *See* S. REP. NO. 90-1097, at 66 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 (providing that the case outlined constitutional considerations relevant for electronic communications); *see also* Katz v. United States, 389 U.S. 347, 351

tive interpretation of the Act culminated in 1986 with the Electronics Communication Privacy Act (ECPA), which formally recognized electronic communications as protected communications.[2] The Act places restrictions on the intentional or attempted interception of another person's oral, wire, or electronic communications.[3] The Act includes a Party Exception which states that, if at least one party to the communication provides the third party with consent for

(1967) (providing that the Fourth Amendment right to privacy protects individuals, rather than specific locations, such as a home).

[2] *See* Gellis, *supra* note 1, at 344 (including that the legislature adopted the Electronics Communications Privacy Act (ECPA) before the widespread use of the Internet, so the language of the ECPA does not fully encompass the nature of web communications). The Act resulted from a combination of the Federal Wire Interception Act and the Electronic Surveillance Control Act of 1967. *See* S. REP. NO. 90-1097, *as reprinted in* 1968 U.S.C.C.A.N. 2153 (noting that significant privacy cases of the time prompted Congress to enact the Act). Title III of the Omnibus Crime Control and Safe Streets Act of 1968 is also known as the modern Wiretap Act. *See* Peter J. Guffin, *The Electronic Communications Privacy Act*, *in* DATA SECURITY AND PRIVACY IN MASSACHUSETTS §§ 2, 2.1 (Stephen Y. Chow ed., 2d ed. 2018) (noting that the Omnibus Crime Control and Safe Streets Act was one of the first laws to ascribe privacy protections from the wiretapping of both the government and private entities). Title III controls the rules for obtaining wiretaps, originally pertaining only to "oral" and "wire" communications. *See Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, U.S. DEP'T OF JUST., https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284 [https://perma.cc/8D32-SSK4] (outlining the background of the Act, along with the privacy and civil liberty considerations). Congress limited these transmissions to aural transfers—communications one can hear. 18 U.S.C. § 2510(18). Following the enactment of the ECPA, Congress modified Title III to include electronic communications. *See* U.S. DEP'T OF JUST., *supra* (stating that enacting the ECPA extended the privacy protections afforded to wire and oral communications to contemporary modes of electronic communication). A protected communication under the ECPA is an electronic communication that the legislature deemed protected by privacy rights and, therefore, guarded from unauthorized access or interception. *See* Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 480 n.109 (2012) (first citing S. REP. NO. 99-541, at 1, 11 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555, 3565; then citing H.R. REP. NO. 99-647, at 18–19, 34 (1986)) (describing the legislative intent to extend privacy protections to electronic communications to adapt privacy rights to the changing technologies and modes of communication.

[3] *See* 18 U.S.C. § 2510–2523 (protecting privacy by barring the (attempted) unauthorized interception and use of communications); Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 18 (1st Cir. 2003) (noting that post-ECPA, the Act explicitly provides claimants with a legal right to sue entities that purposefully intercept or attempt to intercept their communications). The ECPA includes attempted interceptions within its conception of "interception." *See* 18 U.S.C. §§ 2510(4), 2511(1)(a) (defining "intercept" as the use of some device for the attainment of another individual's wire, spoken, or electronic transmission). The Act defines a "wire communication" as any communication made, partially or in full, using wire, cable, or similar methods of transmission, which someone manages for the purpose of interstate or foreign conveyance. *Id.* § 2510(1). An "oral communication" is any statement made with an expectation of privacy, meaning with the expectation that a third party will not intercept the communication. *Id.* § 2510(2). The Act defines "electronic, mechanical, or other device" as any non-telephonic and non-hearing assistive device used to intercept a communication that is not used in the ordinary course of business. *Id.* § 2510(5). An "electronic communication" is any transmission of information conveyed, in part or full, through technology that involves interstate commerce; the statute does not consider oral or wire communications, communications sent through paging devices, communications sent from tracking devices, or communications transferring electronic funds to be electronic communications. *Id.* § 2510(12).

the interception, the acquisition does not violate the Act.[4] The objective of the ECPA, particularly Tile I, containing the Act, is to protect the privacy of communications, both electronic and non-electronic.[5]

In 2020, in *Davis v. Facebook, Inc.* (*In re Facebook*), the United States Court of Appeals for the Ninth Circuit held that a third party's acquisition of an electronic communication and its content without a party's consent constituted an illegal interception under the Act.[6] In so holding, the Ninth Circuit joined the Seventh and the First Circuits.[7] In 2003, the First Circuit determined that the Party Exception does not protect interceptions of electronic communications that copy the contents of the communication during transmission when there is no party consent.[8] The Seventh Circuit held similarly.[9] Conversely, in 2015, the Third Circuit determined that an entity may gain party membership to a communication through deceit, so long as they receive a direct transmission of the communication.[10] The Ninth Circuit's holding in *In re Facebook* deepened the Third Circuit's minority position.[11]

---

[4] *See* § 2511(2)(d) (providing, however, that even if a party gives consent to an interception, the interception violates the Act if the purpose of the interception is tortious or criminal).

[5] *See* S. REP. NO. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (stating that the purpose of the ECPA is to protect privacy in the face of advancing technology). The prevailing objective of both Acts today is to protect privacy, despite Congress's initial intention of ushering in a new technological era with the ECPA. *See In re Pharmatrak*, 329 F.3d at 18 (noting that the chief objective of the Act is to protect individual's privacy in communications); *see also* 18 U.S.C. §§ 2510–2523 (containing the ECPA in its entirety). The ECPA includes a provision defining the types of communications to which it applies. *See* 18 U.S.C. § 2510(1)–(2), (12) (defining wire communications as those made using wire, cable, or a similar means, defining oral communications as those made verbally, and defining electronic communication as those made using technology).

[6] *See* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (rejecting a broad construction of the party exception that would have enabled the defendants to copy the transmitted communications without user consent).

[7] *See id.* at 607 (first citing *In re Pharmatrak*, 329 F.3d at 22; then citing United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010)) (noting that the First and Seventh Circuits implicitly determined that the unauthorized, secretive duplication of a communication by a non-party violates the Wiretap Act).

[8] *See In re Pharmatrak*, 329 F.3d at 19–20 (citing Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998)) (maintaining that the court can only infer the requisite consent if the party whose communications the third party is intercepting has actual notice of the interception, unless the situation "convincingly" demonstrates that the first party had awareness of and consented to the interception). The court also highlighted the importance of "contemporaneity" to the interception. *See id.* at 22 (noting that the "contemporaneous acquisition" of the communications by Pharmatrak weighed strongly in favor of that acquisition constituting an unlawful interception). Contemporaneity in the context of the Act means that the third party duplicates the contents of the communication simultaneous to the communication's transmission. *See id.* (adding that depending on how narrow a construction of the Act a court employs, the contemporaneity of an interception becomes more important).

[9] *See Szymuszkiewicz*, 622 F.3d at 705 (concluding that the purpose of the Act is to protect private communication from unintended recipients and that the defendant's contemporaneous receipt of the communication constituted an interception).

[10] *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 144 (3d Cir. 2015) (determining that Congress intentionally designed the Act to permit an entity to gain member-

Part I of this Comment gives an overview of the Act, provides background on the pertinent data tracking methods, and outlines the history of *In re Facebook*.[12] Part II discusses the circuit split between the Seventh and First Circuits and the Third circuit regarding the Party Exception to the Act.[13] Lastly, Part III argues that the Ninth Circuit's holding in *In re Facebook*, in which it joined the majority, is a practical and correct interpretation of the Party Exception given the legislative history and intent of 18 U.S.C. § 2511.[14]

I. The Wiretap Act and Electronic Communications

In 2020, in *Davis v. Facebook, Inc.* (*In re Facebook*), the United States Court of Appeals for the Ninth Circuit held that the Party Exception of the Wiretap Act does not apply to an unknown third party's instantaneous replication of electronic communications.[15] Section A of this Part provides an overview of the Party Exception to the Act.[16] Section B discusses cookies as a primary mechanism for data tracking and the legal implications of such tracking.[17] Section C briefly reviews the circuit split concerning the Party Exception and introduces the facts and procedural history of *In re Facebook*.[18]

---

ship to a communication through fraudulent means). When the court described the defendants as gaining access to the communication through deceit, the court was referring to the defendants' use of cookies—internet data storage files—to compel the users' computers to directly send them the users' browsing searches. *See id.* at 142 (concluding that, although plaintiffs did not intend for the defendants to be parties, they were, nonetheless); Michal Wlosik & Michael Sweeney, *What's the Difference Between First-Party and Third-Party Cookies?*, CLEARCODE (2018), https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/ [https://perma.cc/U2L9-MX6L] (discussing cookies). The court interpreted the "parties" to a transmission broadly to include internet advertising companies who placed cookies on web-users' browsers. *See In re Google Cookie*, 806 F.3d at 143 (noting that the defendants became parties to the communication because their placement of cookies onto the plaintiffs' computers resulted in the communication's direct transmission to the defendants). In so doing, the Third Circuit determined that the third party did not "intercept" the communications because the party's browser directly communicated with the defendants. *See id.* at 144 (maintaining that the conduct does not constitute wiretapping simply because it was deceitful).

[11] *See In re Facebook, Inc.*, 956 F.3d at 608 (rejecting the Third Circuit's conception of the Party Exception as counter to the legislative intent of the Act).

[12] *See infra* notes 15–43 and accompanying text.

[13] *See infra* notes 44–78 and accompanying text.

[14] *See infra* notes 79–95 and accompanying text.

[15] *See* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (determining that the Party Exception was not appropriate or practical to apply to the facts at hand based on the legislative history and Congressional intent of the Act).

[16] *See infra* notes 19–23 and accompanying text.

[17] *See infra* notes 24–30 and accompanying text.

[18] *See infra* notes 31–43 and accompanying text.

A. The Party Exception to the Wiretap Act and the Role of Deceit

The ECPA codifies the Act and contains four main exceptions that remove liability for entities that fall within their scope.[19] One of these exceptions is the Party Exception.[20] The Party Exception applies to instances where a party gives consent to a third party to intercept a communication.[21] The critical concern under the Party Exception is whether a party consents to an interception—if there was no authorization, an entity's acquisition of a transmission violates

---

[19] *See* Guffin, *supra* note 2, §§ 2.1, 2.3.2 (detailing the Act's exceptions and their relevant statutory provisions). Because the ECPA has stayed mostly stagnant since Congress enacted it in 1986, courts and Congress have worked together to shape the current landscape of electronic surveillance and privacy law. *See id.* § 2.1 (explaining how courts have worked with legislature to establish a body of law that can withstand technological evolution).

[20] *See* 18 U.S.C. § 2511(2)(c) (providing that the Party Exception removes liability for unauthorized interceptions of communications if one of the parties provided consent). In addition to the Party Exception, there are three other primary exceptions. *Criminal Resource Manual 1001–1099*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/jm/criminal-resource-manual-1053-exceptions-prohibitions-interceptions-providers-wire-or [https://perma.cc/BH78-2BE2] (Jan. 21, 2020). The maintenance exception is for service provider employees and allows for these employees to intercept a transmission if they act in the scope of their employment or to protect the rights of their employer. 18 U.S.C. § 2511(2)(a)(i). Another exception allows a service provider to disclose the contents of a transmission if they receive consent from a first party, if § 2511(2)(a) or § 2517 permit; if it is a necessary intermediary; if it was authorized to finish the transmission; or if it accidentally acquired a communication appearing to relate to a crime. *Id.* § 2511(3)(b). Lastly, the ordinary course of business exception removes liability for businesses to monitor communications that occur using certain types of telephonic mechanisms while conducting ordinary business. *Id.* § 2510(5)(a)(ii).

[21] *See* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 19 (1st Cir. 2003) (citing 18 U.S.C. § 2511(2)(d)) (noting that the Party Exception is not applicable in instances where a third party gains consent or authorization for an interception but uses the interception for illegal purposes). According to the court in *In re Pharmatrak*, the first party must give actual assent for a third party to intercept the communication under the Party Exception. *See id.* (noting that constructive consent is not sufficient under the Act); Levinson, *supra* note 2, at 495 (providing that either express or implicit assent is sufficient, but in any case, the individual must be on actual notice that a third party will intercept or monitor their information). Actual assent means that a party to the communication provides consent to the interception in a manner that is not constructive, meaning that the party's knowledge and manifested approval of the interception must be the foundation of the consent. *See* Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (detailing the consent standard for the Act). Prior to *In re Pharmatrak*, there was a disagreement about which party bore the burden of demonstrating consent. *See* 329 F.3d at 19 (noting that some cases suggested that the burden was on the party pursuing the exception, and others suggested that the burden was on the party seeking to show the violation). The First Circuit stated that for the consent exception, the burden is on the entity attempting to invoke the exception, rather than the party claiming the violation. *See id.* (clarifying a hazy body of case law). *Compare* United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) (placing the burden of demonstrating the consent exception on the party seeking its application), *abrogated by* United States v. Watts, 519 U.S. 148 (1997), *with* Williams v. Poulos, 11 F.3d 271, 284 (1st Cir. 1993) (suggesting that the burden is on the party trying to show a violation of the exception). Although a party may consent to an interception, the interception may still violate the Act if it intercepts more than the consented-to portion of the communication. *See In re Pharmatrak*, 329 F.3d at 19 (noting that courts must inquire into the bounds of the consent to determine if the interception exceeded the authorized scope).

the Act.[22] As the Act's primary purpose is to preserve privacy, any unauthorized acquisition of communications inherently violates the Act's objective.[23]

B. Cookies and Data Tracking

Cookies are text files containing a small amount of information about the user, such as the user's browsing history.[24] Under the Act, Internet users can bring a claim against a website for placing cookies on the user's browser to collect their search contents without their consent.[25] Although certain data collection using cookies is a common practice, a webpage may violate the Act if it uses cookies to track users' search histories.[26] Web browsing platforms, such as

---

[22] *See* Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 CARDOZO L. REV. 669, 697 (2012) (positing that where the first party does not provide consent, the Act focuses on whether the third party intruded on the first party's privacy). The circuit split over who constitutes a party and is thereby capable of intercepting an electronic transmission highlights the ambiguous nature of this factor of the Act. *Compare* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (concluding that the defendant violated the Act by receiving direct copies of his coworker's emails without being a party to the communication), *and In re Pharmatrak*, 329 F.3d at 22 (determining that the defendants violated the Act because, through interception, they received duplicate, identical transmissions to the ones their users sent), *with In re* Google Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 142 (3d Cir. 2015) (holding that the defendants were a party to the communication because the plaintiffs' computers sent direct copies of the communications to the defendants).

[23] *See* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (discussing the legislative intent of the Act as protecting the privacy of communications from unauthorized third parties).

[24] *See In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 926 (N.D. Cal. 2015) (providing a detailed background on cookies and how Facebook creates and uses these text files). A cookie text file stores content such as social media logins and passwords or online shopping data and saves the information for when users visit the websites. *In re Pharmatrak, Inc.*, 329 F.3d at 14. Websites save cookies on users' hard drives when they visit the website. *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 (2018) (providing that once the site places the cookie on the user's hard drive, it reads the cookie data whenever the user visits the site). Once the website saves the cookie to the user's hard drive, it can collect personal data on the user when they visit the site. *See id.* (noting that the cookie gathers data by tracking website visits and products purchased). Cookies allow web platforms to include customizable and social features, such as "like" buttons, for sharing content and interacting with others. Defendant Facebook, Inc.'s Motion to Dismiss Plaintiffs' Corrected First Amended Consolidated Class Action Complaint (Fed. R. Civ. P. 12(b)(1) & 12(b)(6)) at 3–4, *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922 (N.D. Cal. 2015) (No. 12-md-02314), 2012 WL 3343173, at *3–4 (describing Facebook's use of cookies as facilitating social media usage compared to the plaintiffs' allegations that the cookies tracked their data, even when they were logged-out of their Facebook account).

[25] *See* Kletter, *supra* note 24, § 2 (addressing how the Act permits claims about a defendants' use of cookie placement to intercept communications so long as the plaintiff demonstrates that the defendant so acted).

[26] *See id.* §§ 9–10 (maintaining that, although the judicial interpretation of interception is jurisdiction and context dependent, it is based on whether the third party uses the cookies for an intentional interception of a communication). Websites create first-party cookies when a user visits their page, and they enable the website to retain certain information like login information and settings preferences. *See* Wlosik & Sweeney, *supra* note 10 (discussing the difference between first-party and third-

Internet Explorer, offer cookie-blocking features that prevent third-party cookies.[27] A webpage can circumvent cookie-blockers by taking advantage of loopholes in the feature without the knowledge or consent of the users.[28] In these situations, the browser directly sends the transmission to the third party, who, therefore, gains party membership through deceitful means.[29] In these situa-

---

party cookies). This is common practice and not frequently contested. *See id.* (maintaining that first-party cookies help websites tailor users' experiences based on past actions). Websites other than the site the user is visiting, however, can also create third-party cookies, which they use to track users' search activity and produce targeted advertisements. *See id.* (discussing the placement of cookies on the website, which then sends information back to the third party to produce an ad). These cookies trail users from site to site to compile a comprehensive Internet profile of the users. *See* Jeffrey R. Schoenberger, *Don't Be a Cookie Monster*, 108 ILL. BAR J. 42, 42 (2020) (raising privacy considerations that arise from cookies tracking website users). When such actions constitute an interception, they likely violate the Act. *See* Kletter, *supra* note 24, § 2 (stating that parties to the communication are exempt).

[27] *See In re Google Cookie*, 806 F.3d at 132 (noting that the use of cookie-blockers is a common and understood practice among cyber companies, such as Google). Cookie-blockers are standard software that browsers may employ to prevent third-party cookies from accessing user data. Wlosik & Sweeney, *supra* note 10.

[28] *See In re Google Cookie*, 806 F.3d at 132 (detailing that the actions that webpages take to exploit the exception result in the exact type of cookie placement that the cookie-blockers should prevent). In 2012, a Stanford student discovered, and subsequently exposed, that webpages could circumvent cookie-blockers by relying on the exception for third parties that have submitted a specified form. *Id.*; *see also* Jonathan Mayer, *Safari Trackers*, WEB POL'Y BLOG (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/ [https://perma.cc/2UXC-ANT3] (containing the student's published research). Platforms, such as Google, had embedded code in the browser that commanded the browser to automatically send the form to Google when users visited sites that contained embedded Google advertisements. *See In re Google Cookie*, 806 F.3d at 132 (providing that, by engaging in this conduct, entities were able to set tracking cookies onto users' browsers regardless of the protective measures of cookie-blockers); Mayer, *supra* (finding three other platforms, in addition to Google, evaded browser cookie-blockers). Relying on these loopholes, webpages can place third-party cookies on users' browsers without the browser detecting an invasion. *See In re Google Cookie*, 806 F.3d at 132 (providing that by sending a hidden form using embedded text, the platform falls into the cookie-blocker exception and can track user activity without detection). A GET request is one method by which a web platform, such as Facebook, receives cookie data. *See Using HTTP Cookies*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies [https://perma.cc/D2BE-255X] (Sept. 28, 2020) (stating that it is through cookies, for example, that websites retain user log-in information). A GET request is a message that the browser transmits to a web page server, such as Facebook, which contains the information that the user searched for and a URL associated with the user. *In re Facebook, Inc.*, 956 F.3d at 607. Although this transmission is typically only between the intended webpage and the user's computer, webpages that contain embedded code to circumvent cookie-blockers will send a distinct communication with identical content to the third party. *See id.* (recognizing that it is through the acquisition of the GET request content that websites compile a profile of the user).

[29] *See In re Google Cookie*, 806 F.3d at 142 (discussing specifically the plaintiffs' direct transference of the GET request to the defendants as indicative of them being a party). The Third Circuit determined that when there is a direct transmission of a communication from a browser to an entity, that entity is a party to the communication. *See id.* at 143 (noting that there need only be one intended party, but there can be more). Because the browser intentionally transmitted the message to the defendants, they were the GET requests' intended destinations, so the defendants did not violate the Act by intercepting the users' transmission. *See id.* (providing that parties to a communication do not violate the Act when they intercept that communication). Thus, the entity gained party membership

tions, some argue that the browser's transmission of cookie data to unauthorized third parties violates the Act because these outside parties intercepted, or attempted to intercept, users' electronic communications.[30]

C. The Circuit Split and In re Facebook*: The Ninth Circuit Joins the Majority*

The Party Exception places unauthorized interceptions of communications outside the scope of the Act when the third party receives consent.[31] Although this exception is present in major electronic communication laws, there is not a consensus among circuits about how to interpret the Party Exception.[32] A circuit split exists regarding whether the Party Exception extends to discrete third parties that, concurrently with the transmission, duplicate communications between two parties.[33]

In 2020, in *In re Facebook*, the Ninth Circuit joined the majority of circuit courts in holding that the Party Exception of the Act does not extend to entities that secretly obtain access to communications between two parties.[34] In *In re*

---

through deceit by circumventing web browsing features. *See id.* (determining that entering a communication through fraudulent means is permissible under the Act).

[30] *See* Kletter, *supra* note 24, § 2 (observing that some courts recognize the claim that cookie placement constitutes an interception under the Act, whereas others have determined that the cookie's data collection was not an interception because a party gathered it).

[31] *Compare* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (determining that a third party's unauthorized interception of a communication violated the Act), *and* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 20 (1st Cir. 2003) (explaining that the Party Exception requires the consent of at least one party, and, without consent, a third party is not a party to the communication), *with In re Google Cookie*, 806 F.3d at 143 (reasoning that a third party is a party to a communication when it directly receives a copy of a communication).

[32] *See In re Facebook, Inc.*, 956 F.3d at 607 (detailing the circuit split arising from this exception due to the Act's failure to define the term "party," leaving it to judicial interpretation). Both the Act and the California Invasion of Privacy Act contain a Party Exception. *See id.* (noting that courts use the same mode of analysis for both); *see, e.g.*, William v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993) (stating that the third party did not have consent to intercept the first party's communication and thus violated the federal and Maine wiretap acts); Warden v. Kahn, 99 Cal. App. 3d 805, 812 (Ct. App. 1979) (prohibiting eavesdropping on communications without party consent under the California Invasion of Privacy Act).

[33] *See In re Facebook, Inc.*, 956 F.3d at 607 (acknowledging that the First and Seventh Circuits have both tacitly determined that unauthorized parties that furtively copy communications between two first-parties are not participants of the communication within the bounds of the Act); *Szymuszkiewicz*, 622 F.3d at 705 (holding that the unauthorized, simultaneous sending of a user's email transmissions to a third party constituted an interception under the Act); *In re Pharmatrak*, 329 F.3d at 22 (concluding that because the plaintiffs did not provide the defendants with consent to receive the communication, they intercepted the transmission in violation of the Act). *But see In re Google Cookie*, 806 F.3d at 143 (finding that the statute does not exclude entities from being parties to a communication when they gain access through deceit).

[34] *See In re Facebook, Inc.*, 956 F.3d at 608 (providing that websites containing embedded Facebook software violated the act when they directly sent Facebook a copy of the users' browsing searches in a separate transmission). The majority relied on cases involving the "surreptitious" duplication of a first party's communication through deceitful means, such as through cookie placement and chang-

Facebook, a class-action suit, the plaintiff-appellants alleged that the defendant, Facebook, monitored the outside Internet searches of users while they were logged-out of the site.[35]

Facebook, Inc. operates a social network entitled "facebook.com," and each of the plaintiffs were members of this network.[36] The plaintiffs maintained that Facebook's use of third-party cookies to produce personalized advertisements constituted an unauthorized interception under the Act.[37] The plaintiffs initially asserted eleven claims against Facebook, Inc., but the U.S. District Court for the Northern District of California dismissed all of the claims and granted leave to amend for six.[38] The district court granted the defendant's motions to dismiss the amended complaints after two sets of motions.[39] The plaintiffs appealed to the Ninth Circuit, which reviewed the claim

---

ing computer settings. *See id.* at 607 (detailing the majority position that legislative design and intention of the Act prohibit such interceptions).

[35] *See In re* Facebook Internet Tracking Litig., 290 F. Supp. 3d 916, 918 (N.D. Cal. 2017) (noting that the plaintiffs alleged that Facebook's monitoring violated the website's stated privacy policy), *aff'd in part, rev'd in part and remanded sub nom. In re Facebook, Inc.*, 956 F.3d 589. A class action suit is one where the court permits a single individual or small group of persons to represent a larger group's interests; the court consolidates the group based on efficiency or the interests of the parties. *See Class Action*, BLACK'S LAW DICTIONARY (11th ed. 2019) (explaining further that although not every interested party is present in court, the present parties represent the interests of the group). Federal procedure requires that, to establish a class action, the class must share questions of legal or factual issues and be large enough such that independent lawsuits would be inefficient. *See id.* (citing FED. R. CIV. P. 23) (recognizing that a class action suit arose out of a need to address the interests of a large group of plaintiffs without flooding the courts with individual cases). The parties must bring claims representative of the larger group, and they must safeguard the class's concerns. *See id.* (citing FED. R. CIV. P. 23) (explaining that these two features, combined with sharing questions of issues and being a sufficient size, make up the four requirements for a class action suit).

[36] *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 926 (N.D. Cal. 2015).

[37] *See In re Facebook, Inc.*, 956 F.3d at 596, 607 (providing that an entity intercepts a communication when it gains access to the transmission without obtaining party consent to be a member). According to the plaintiffs, Facebook used both first-party cookies and third-party cookies. *See In re Facebook, Inc.*, 140 F. Supp. 3d at 926–27 (stating that Facebook acquires users' data by conditioning site membership on users permitting Facebook to place cookies on their computer); *see also supra* note 26 and accompanying text (defining first and third-party cookies).

[38] *See In re Facebook, Inc.*, 140 F. Supp. 3d at 929, 937 (detailing each of the plaintiffs' claims and the court's resolution of each). The district court determined that the plaintiffs had standing for their Wiretap Act, Stored Communications Act, and California Invasion of Privacy Act claims but dismissed them with leave to amend for failure to state a claim. *See id.* at 934 (noting that this statutory standing means that the plaintiffs alleged a sufficiently specific injury under the statutes). The court also dismissed, with leave to amend, the plaintiffs' claims under California's Unfair Competition Law, California's Consumer Legal Remedies Act, and the California Computer Crime Law for lack of standing. *See id.* at 933 (determining that the plaintiffs did not allege a sufficiently specific injury under the statutes). The court dismissed without leave to amend the plaintiffs' Computer Fraud and Abuse Act claim. *Id.* at 937. This was the first round of motions to dismiss. *See In re Facebook*, 290 F. Supp. 3d at 918 (stating that there were two rounds of motions to dismiss preceding the case's current status in the district court).

[39] *See In re Facebook*, 290 F. Supp. 3d at 918 (noting that it was reviewing only the plaintiffs' breach of contract and duty of good faith and fair dealing claims). Upon the plaintiffs' first amended

under the Act *de novo*.[40] The Ninth Circuit found Facebook liable for violating the Act by intercepting users' communications.[41] This is because none of the parties consented to Facebook's acquisition, and Facebook was not an intended recipient of the communication.[42] The court relied on precedential interpretations of the ECPA and the Act's legislative history when reaching its ultimate determination that the Party Exception is not inclusive of unauthorized third-party acquisitions of communications.[43]

II. Interpretation of the Party Exception Leads to a Circuit Split

A circuit split exists regarding the judicial interpretation of the Party Exception of the Act.[44] The majority, comprised of the First and Seventh Circuits, determined that the Party Exception does not apply to unauthorized third parties.[45] The minority, comprised of the Third Circuit, held that entities that re-

---

complaint, the defendant again filed motions to dismiss, and the district court dismissed with prejudice most of the plaintiffs' claims. *See In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 848 (N.D. Cal. 2017) (dismissing the plaintiffs' claims including the claim under the Act). The court granted the plaintiffs leave to amend their breach of contract claim and their breach of duty of good faith and fair dealings claim; on that amended complaint, Facebook again filed a motion to dismiss, which was granted. *See In re Facebook*, 290 F. Supp. 3d at 918, 923 (dismissing plaintiffs' claims without leave to amend and ordering the clerk to close the case).

[40] *See In re Facebook, Inc.*, 956 F.3d at 596–97 (evaluating the plaintiffs' standing and previous dismissals for failure to state a claim). A *de novo* review is the court's power to review a legal issue without deference to the lower court's determination. *See Review*, Black's Law Dictionary, *supra* note 35 (discussing *de novo* review in the context of administrative action).

[41] *See In re Facebook, Inc.*, 956 F.3d at 608 (aligning with the First and Seventh Circuits' stances on unauthorized interceptions).

[42] *See id.* (maintaining that if the court were to permit Facebook to engage in this type of surreptitious acquisition of logged-out user communications, it would result in an overly expansive Party Exception). The Ninth Circuit viewed only the Facebook users and their searched-for webpage as parties to the communication. *See id.* at 607 (noting that traditionally, the GET request communication occurs only between these two parties, but on browsers with the Facebook cookies, the browser sends a separate, identical transmission to Facebook).

[43] *See id.* at 608 (citing Joffe v. Google, 746 F.3d 920, 931 (9th Cir. 2013)) (highlighting that the chief goal of the ECPA is to preserve transmission privacy). ECPA precedent suggests that the Act serves chiefly to guard the privacy rights afforded to electronic communications. *See, e.g.*, *Joffe*, 746 F.3d at 931 (maintaining that Congress intended the Act to protect against unconsented-to interceptions). The court also referenced the legislative history of the Omnibus Crime Control and Safe Streets Act of 1968, which Congress designed to prevent an unauthorized third party from intercepting personal information. *In re Facebook, Inc.*, 956 F.3d at 608 (citing S. Rep. No. 90-1097, at 67 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2154).

[44] *See In re* Google Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (providing the minority interpretation of the Party Exception); United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010) (contributing to the majority stance); Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 18 (1st Cir. 2003) (forming the majority position on the Party Exception).

[45] *See* 18 U.S.C. § 2511(2)(d) (providing that where at least one of the parties to a transmission provides prior consent to an interception, the intercepting third party is not in violation of the Act, unless their interception is to facilitate an illegal purpose); *Szymuszkiewicz*, 622 F.3d at 706 (holding

ceive duplicate, identical copies of a communication through deceitful means are, nonetheless, parties to the transmission.[46] The Ninth Circuit joined the majority in 2020 in *In re Facebook*.[47] Section A of this Part discusses the majority view of the Party Exception related to unauthorized third parties.[48] Section B addresses the Third Circuit's minority perspective that an unknown third party is a party to a communication when it receives a direct copy of the transmission.[49] Section C explains the Ninth Circuit's holding in *In re Facebook*.[50]

A. The Majority View on the Party Exception: Exclusion of Unauthorized Third Parties

Courts disagree on the proper interpretation of the Party Exception under the Act.[51] The difference in interpretation arises because the Act does not contain a definition of the word "party."[52] As such, courts vary on how to treat entities that receive copies of transmissions without a first party's knowledge.[53]

---

that the contemporaneous duplication of an electronic communication constituted an interception under the Act); *In re Pharmatrak*, 329 F.3d at 13 (determining that entities that gain access to a communication through the unauthorized use of software are not parties to a communication under the Act and are thus unlawful interceptors of the transmission).

[46] *See In re Google Cookie*, 806 F.3d at 143 (holding that although the third-party entities were not the plaintiffs' intended recipients, they were parties to the communication because the user's browser sent them a duplicate, identical copy of the communication that it sent to the desired party). The court noted that due to the nature of the Act, the legislature reasonably anticipated that entities may gain participation in a communication through deceitful means. *See id.* at 143 n.76 (citing *Wiretapping*, BLACK'S LAW DICTIONARY (10th ed. 2014)) (concluding that wiretapping is eavesdropping using technology).

[47] *See* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (discussing the circuit split regarding the Party Exception's application); *see also In re Pharmatrak*, 329 F.3d at 22 (forming the basis of the majority view that the Party Exception does not apply); *Szymuszkiewicz*, 622 F.3d at 706 (supporting the majority view). *But see In re Google Cookie*, 806 F.3d at 143–44 (comprising the minority view that the Party Exception applies).

[48] *See infra* notes 51–64 and accompanying text.

[49] *See infra* notes 65–73 and accompanying text.

[50] *See infra* notes 74–78 and accompanying text.

[51] *See In re Facebook*, 956 F.3d at 607–08 (outlining the circuit split between the majority, the First and Seventh Circuits, and the minority, the Third Circuit, about the interpretation of the Party Exception of the Act); *In re Google Cookie*, 806 F.3d at 142–43 (holding that the defendants, who gained access to the communication through the placement of tracking cookies, were parties to the communication); *Szymuszkiewicz*, 622 F.3d at 706 (establishing that the defendant's contemporaneous duplication of the plaintiff's communication constituted an interception and violated the Act); *In re Pharmatrak*, 329 F.3d at 22 (determining that the defendants' contemporaneous duplication of the plaintiffs' communication was an interception, thereby violating the Act).

[52] *See* 18 U.S.C. § 2510 (lacking a definition for "party"). Due to the absence of a "party" definition in the Act, courts interpret the term in the context of the cases they address, which results in variable understandings of the term. *See In re Facebook, Inc.*, 956 F.3d at 607 (noting that the circuit split at issue in *In re Facebook* was a result of the variable treatment of the term "party").

[53] *Compare Szymuszkiewicz*, 622 F.3d at 707 (holding that the defendant violated the Act because he acquired the plaintiff's email communications simultaneous to their transmission without authorization, making those acquisitions unlawful interceptions by a non-party), *and In re Pharmatrak*, 329 F.3d at 20–21 (concluding that the defendants violated the Act because they intercepted the communi-

Courts rely on the legislative intent, legislative history, and case law to define the term so they can determine whether an entity is a party to a communication, rather than an unauthorized third party.[54]

In 2003, in *In re Pharmatrak*, the First Circuit determined that an entity that secretively gains access to communications without the prior consent from a party to intercept the transmission violates the Act.[55] The court held that the plaintiffs did not consent to the collection of personally identifiable information by using Pharmatrak.[56] The court determined that because the defendants obtained the same URL transmission as the one the plaintiffs sent to the pharmaceutical company, the defendants acquired the identical private information, simultaneous to the primary communication.[57] Although the defend-

---

cation simultaneous to its transmission without the consent of the plaintiffs), *with In re Google Inc. Cookie*, 806 F.3d at 143–44 (holding that nothing in the statutory language stops entities from gaining party membership through fraud and deceit, such as through the use of embedded browser cookies).

[54] *See In re Facebook, Inc.*, 956 F.3d at 608 (establishing its sources for the basis of its interpretation and pointing to other circuits' similar reliance on these materials).

[55] *See* 329 F.3d at 19 (detailing the consent requirement for third-party acquisition of a communication). The court outlined five elements of an interception under the Act: the defendant must (1) intentionally (2) intercept (3) the substance of (4) a party's electronic communication (5) using some device or mechanism. *Id.* at 18; *see also* 18 U.S.C. § 2510(4) (defining "intercept" as the use of some means to attain an entity's communications). The Act itself expansively defines what constitutes an "electronic communication" and bars any interception of such communications without consent. *See In re Pharmatrak*, 329 F.3d at 18 (citing 18 U.S.C. § 2510(4)) (providing a broad list of the types of transmissions the Act covers, such as data, pictures, or intellectual property that a person sends by electronic means). In 1986, the ECPA used an expansive construction of "transmissions" to extend the Act's protections to the new computer and telephonic means of communication. *See* Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995) (noting that Congress intended for the ECPA to provide the same protections to electronic transmissions as the Act afforded to oral and wire communications). The flexible definition that the ECPA adopted encompasses any communication made in part or in whole by electronic means that implicates commerce. *In re Pharmatrak*, 329 F.3d at 18 (citing 18 U.S.C. § 2510(12)).

[56] *See In re Pharmatrak*, 329 F.3d at 21 (determining that there was no issue of implied consent because Pharmatrak intentionally collected data in a secretive manner). The court ascertained that the clients received guarantees from the defendant that the webpage did not engage in the gathering of personal data. *See id.* at 20 (noting additionally that the clients specifically conditioned their use of Pharmatrak's software on the company not gathering such information). Pharmatrak is a web-based company that provides a service to compare pharmaceutical companies, and it was through this service that the defendant collected users' personal data. *See id.* at 12 (adding that pharmaceutical companies expressly requested that Pharmatrak not engage in this data collection). The court identified three areas of concern that supported its finding: (1) an inference that the parties consented to this interception is incongruent with the legislative purpose of the Act, (2) this interpretation would undermine efforts of a party to seek privacy protections for their electronic communications, and (3) it would result in unreasonable conclusions. *See id.* at 20 (detailing the court's interpretation of the Party Exception and the protections the Act affords to communications).

[57] *Id.* at 22 (emphasizing that the acquisition of the same URL string was indicative of a duplication of an identical communication to the plaintiffs). In concluding this point, the court added that, although the communication was facially separate, because it occurred simultaneously and was identical in content to that of the plaintiffs, it satisfied the most stringent timing requirements. *See id.* (noting that a narrow construction of "interception" would require an automatic duplication of communications as the user sent them).

ants argued that their conduct should not constitute an interception under the Act, the court rejected this argument because the defendants acquired the contents of the communication simultaneous to its transmission and without party authorization.[58] As such, it was inconsequential that the defendants gained the information through a separate transmission; the acquisition was a concurrent duplication of the intended communication, which constituted an interception under the Act.[59]

In 2010, in *United States v. Szymuszkiewicz*, the Seventh Circuit interpreted the Party Exception as not applying to intentional and contemporaneous interceptions, which instead constitute a violation of the Act, regardless of which device actually copies the data.[60] In this case, the defendant modified a co-worker's email settings to forward them to his computer, where he kept them in a folder on his email account.[61] The defendant alleged that because his co-worker's computer sent him the emails directly, he did not intercept the

---

[58] *See id.* (noting that "contemporaneous" means that the defendant acquired the communication at the same time as the transmission, not that the defendant acquired the exact same communication as the transmission); Reply Brief of Pharmatrak & Glocal in Further Support of Their Motion for Summary Judgment Regarding Plaintiffs' Claim Under 18 U.S.C. § 2511 and Separately for Lack of Article III Standing at 4, *In re* Pharmatrak, Inc. Priv. Litig., 292 F. Supp. 2d 263 (D. Mass. 2003) (No. CIV.A.00–11672), 2003 WL 24272672, at *4. (outlining the defendant's arguments as they pertain to the interception). The defendants argued that they did not intercept the communication because it was a distinct transmission from the communication between the user and the pharmaceutical company. *See In re Pharmatrak*, 329 F.3d at 22 (focusing on the separateness of the transmissions, not their simultaneous and identical nature). The court rejected this argument and established that a third party's interception of a communication does not require that the acquisition be part of the same communication, only that it occur contemporaneous to the transmission. *See id.* (discussing what constitutes "contemporaneous" in regard to an interception under the Act).

[59] *See In re Pharmatrak*, 329 F.3d at 22 (noting that the defendant's argument that there were two separate communications failed because under the Act, an interception only requires that the third party contemporaneously acquire content identical to the first party communication).

[60] *See* United States v. Szymuszkiewicz, 622 F.3d 701, 704–05 (7th Cir. 2010) (placing the focus of the violation not on the physical method of interception, but rather the timing). This interpretation was in line with the First Circuit's holding in *In re Pharmatrak*. *See* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 607 (9th Cir. 2020) (stating that the First and Seventh Circuits comprise the majority in the circuit split over the Party Exception); *see also In re Pharmatrak*, 329 F.3d at 22 (finding that the contemporaneous duplication of a communication violates the Act). The court noted that it is inconsequential which computer *actually* duplicated the transmission because computers communicate by breaking down the transmission into message "packets" that move across a group of computers. *Szymuszkiewicz*, 622 F.3d at 704–05. The packet travels on its own and the receiving computer reassembles the packet upon arrival. *See id.* (providing that the individual packets contain portions of the message and the instructions for arriving at the intended destination). At the end, the computer can reassemble the communication to form the complete message. *See id.* (detailing that the computer reassembles the packets to form the message regardless of the order in which the computer received the packets and if any information was resent or sent across a different route).

[61] *See Szymuszkiewicz*, 622 F.3d at 703 (suggesting that the defendant likely modified his co-worker's email settings while his co-worker was away from her desk).

communications and thus did not violate the Act.[62] The court rejected this argument, maintaining that it did not matter that his co-worker's computer forwarded him the emails.[63] The Seventh Circuit honed in on a clear explanation of "interception," placing emphasis on the simultaneity of the interception rather than the means of acquisition.[64]

B. The Third Circuit Minority Perspective—Deceitful Acquisition Falls into the Party Exception

Unlike the First and Seventh Circuits, the Third Circuit, in *In re Google Cookie*, determined that when an entity receives a direct copy of a users' communication, that entity becomes an intended destination for the users' transmission.[65] The court concluded that the Party Exception includes entities that

---

[62] *See id.* (noting that the defendant argued that the court should have charged him under the Stored Communications Act instead of the Act because although he received the communication directly, he stored it illegitimately). The defendant argued that, because he was a party to the communication, he fell within the Party Exception. *See id.* (summarizing the defendant's argument that he sometimes operated as acting manager and legitimately received emails intended for his co-worker). The defendant also maintained that he did not intercept the transmissions because the system forwarded him the emails *after* they reached his co-worker's inbox. *See id.* (maintaining that an interception requires an acquisition of the communication *as it is sent* to the intended party). The court rejected this argument. *See id.* at 703, 705 (denying the defendant's contention that he did not "catch [the communication] in flight").

[63] *See id.* at 706 (dismissing the defendant's argument that his co-worker's computer acted as a conduit to facilitate the messages' delivery). The court provided that the central purpose of the Act is to protect the privacy of communications, including email transmissions. *See id.* (outlining the Act and its key provisions of preserving the privacy of electronic communications and preventing unauthorized interceptions). The court noted that the focus of the Act is on whether an unauthorized party intercepted the communication "contemporaneous" to its transmission. *See id.* at 705 (maintaining that the timing of the interception is what caused the court to categorize the violation under the Act rather than the Stored Communications Act).

[64] *See id.* at 706 (explaining that contemporaneous interceptions do not require intercepting the communication in the middle of its transmission but, instead, acquiring the transmission at the same time as the intended party or intercepting it at a time prior to the communication entering storage). The court recognized that electronic communications are data packets that browsers transmit through various methods that are, ultimately, irrelevant under the statute. *See id.* at 704 (providing that the means of transmission and order of reception are irrelevant because the computers put the communication back together upon receipt). The Act is concerned with the simultaneity of duplication, rather than the interception of the message in the middle of its transmission. *See id.* at 706 (noting that to understand "contemporaneous" to mean intercepting a transmission in the middle of its sending is to misunderstand the word).

[65] *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015) (determining that the users' computers directly sent the GET requests to the defendants, making them one of the users' intentional destinations and, therefore, members of the communication). The communication at issue was the transmission of the users' GET requests to intended websites, with the websites sending an identical copy of the GET request to the defendants. *See id.* at 140 (noting that the sender and the intended recipients are the parties to the communication). The Third Circuit's determination directly contrasts with the Seventh Circuit's holding in *Szymuszkiewicz*. *See* 622 F.3d at 703, 706 (holding that unauthorized parties who duplicated communications violated the Act and did not fall within the scope of the Party Exception). *But see In re Google Cookie*, 806 F.3d at 143 (con-

gain their access to the transmission though deceit.[66] The defendants placed third-party cookies on the users' computers.[67] This induced the browser to directly send the defendants copies of users' transmissions, believing it was a first party participant in the communication.[68] The plaintiffs asserted that the defendants' conduct violated the Act because they were third parties intercepting the communication.[69] The court, however, found that the language of the statute does not suggest that entities may not use fraud to become parties to a communication.[70]

---

flicting with the Seventh Circuit's holding by finding that unauthorized entities were parties to the communication upon receipt of a direct transmission).

[66] *See In re Google Cookie*, 806 F.3d at 143 (noting that these cookie-setting entities tricked the users' browsers into viewing them as first-party participants in the communication). The court reached its conclusion by assessing the relationship between the statute's definition of parties to a communication as compared to its definition of interceptions. *See id.* at 144 n.80 (indicating that the Act's definition of "intercept" does not preclude the defendants' use of deceitful practices to become a party to the communication).

[67] *See id.* at 141 (noting that the defendants placed the cookies on the users' browsers and received duplications of their transmissions without the users' knowledge). A cookie text file stores content such as social media logins and passwords or online shopping data and saves the information for when users visit the websites. Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 14 (1st Cir. 2003).

[68] *See In re Google Cookie*, 806 F.3d at 132 (stating that the defendants' placement of cookies on the users' browsers allowed the defendants to evade the privacy preferences on the users' computers that should have blocked their placement of third-party cookies). These cookies caused the browser to send the defendants copies of the users' search history for the defendants to produce targeted advertisements in the users' browser. *See id.* at 131 (describing that the tracking cookies provided the defendants with specific search terms and web activity unique to the users).

[69] *See id.* at 143 (presenting the plaintiffs' argument that although their GET request was directly sent to the defendants, it was sent due to the defendants' deceitful skirting of the cookie-blockers). In addition to the plaintiffs' complaint that the defendants violated the Act, they presented two other central arguments to the Third Circuit: (1) the court should not have heard the defendants' argument that they were a party to the communication because the district court did not rule on this issue and defendants did not address it on cross-appeal; and (2) the Party Exception does not apply to the defendants because the defendants' means of gaining access to the transmission were tortious under California law. *See id.* at 143–44 (disregarding both arguments for lack of support). The Third Circuit rejected these arguments, maintaining that it has the power to affirm the judgement of the district court on different bases and that the plaintiffs provided no authority to suggest that the Party Exception should not apply when an entity partook in supposedly tortious actions that were wiretapping. *See id.* at 143, 145 (responding to each of the plaintiffs' arguments and affirming the district court's application of the Party Exception).

[70] *See id.* at 143 (maintaining that the statutory language does not forbid entities from gaining party-membership through deceitful or fraudulent means). Fraudulent or deceitful measures can include tricking the plaintiffs' browsers into treating the third party that placed the cookie on the computer as a first-party participant to the communication. *See id.* (providing that in this case, the tricking of the plaintiffs' browsers into treating the defendants as parties to the communication constituted fraud in the inducement); *Fraud*, BLACK'S LAW DICTIONARY, *supra* note 35 (defining fraud in the inducement as an entity's misrepresentation that spurs their admission to a communication or transaction). The court noted that given the purpose of the Act, it may even be likely that Congress anticipated such deceitful purposes when it drafted the Act. *See In re Google Cookie*, 806 F.3d at 143 (suggesting that wiretapping, by nature, connotes a level of deceitful interception). The court cited examples from the Sixth and Seventh Circuits that support such an interpretation of the Act. *See id.* at 144 (first citing

The Third Circuit relied on a broad interpretation of legislative intent, explaining that the Act reasonably permits a party to deceitfully participate in a communication.[71] Ultimately, it affirmed the U.S. District Court for the District of Delaware's dismissal of the plaintiff's Wiretap Act claim.[72] The court held that the defendants, despite gaining access through deceit, were parties to the transmission because they received a direct copy of the communication from the user's browser.[73]

C. Joining the Majority: The In re Facebook *Holding*

The Ninth Circuit's decision in *In re Facebook* further ingrained the circuit split by joining the First and Seventh Circuits' majority view.[74] The Ninth

---

United States v. Pasha, 332 F.2d 193 (7th Cir. 1964); then citing Clemons v. Waller, 82 F. App'x 436, 442 (6th Cir. 2003)) (noting that the Act does not proscribe "interception" of communications by a person impersonating the intended recipient); *see also* United States v. Campagnuolo, 592 F.2d 852, 863 (5th Cir. 1979) (following *Pasha* and determining that an impersonator of the intended recipient did not intercept the communication). In a 1964 case, *United States v. Pasha*, the Seventh Circuit determined that the Act may still consider entities that impersonated the intended recipient of a transmission as a party to the communication. *See* 332 F.2d at 198 (interpreting "party" to mean those who received the communication); *see also In re Google Cookie*, 806 F.3d at 144 (noting that when amending the Act, Congress referenced *Pasha* when discussing who constituted a communication party).

[71] *See In re Google Cookie*, 806 F.3d at 143 (arriving at its conclusion based on the Act's lack of explicit preclusions of deceitful conduct). The court recognized that the Party Exception is unavailable to parties who intercept communications in order to "commit[] any criminal or tortious act." *Id.* at 144–45 (quoting 18 U.S.C. § 2511(2)(d)). In order to lose this protection, however, the court held that the criminal or tortious act in question had to be separate from the interception itself. *See id.* at 145 & n.81 (citing Caro v. Weintraub, 618 F.3d 94, 98, 100 (2nd Cir. 2010)) (stating that, standing alone, an interception that was tortious under California law did not trigger the exception to the Party Exception). The court cited precedent indicating that the Party Exception does not apply only when a defendant intends to use the intercepted transmission to partake in illegal activity past the interception itself. *See id.* (citing *Caro*, 618 F.3d at 98, 100) (bolstering the notion that interception, without intent to use the intercepted data illegally or tortiously, is insufficient to bar the application of the Party Exception).

[72] *See id.* at 145 (affirming the district court's broad interpretation of the Party Exception).

[73] *See id.* at 143 (noting that the Act makes it impossible for parties to a communication to impermissibly intercept said communication). Although the court recognized that the defendants gained membership to the communication through fraud in the inducement, it noted that the Act does not contain any provision prohibiting deceitful conduct. *See id.* (relying on the statute's plain language to show the Act's lack of guidance on a third party's use of deceit to gain party membership). By interpreting the defendants as a party to the communication, the court, consequently, permitted the defendants to use the contents of the users' online communications to sell targeted advertisements. *See id.* at 141 (describing how Google ultimately uses the deceptively acquired data).

[74] *See* Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 608 (9th Cir. 2020) (joining the majority of circuits in holding that copying a transmission concurrent to the users' sending the GET requests did not fall under the Party Exception of the Act when the sender did not consent to the transmission); *see also* United States v. Szymuszkiewicz, 622 F.3d 701, 704–06 (7th Cir. 2010) (providing additional support for the First Circuit's narrow view of the Party Exception); Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 19–21 (1st Cir. 2003) (defining the scope of the Act and the Party Exception). The court rejected the Third Circuit's

Circuit held that the Party Exception did not absolve Facebook of liability under the Act.[75] The court maintained that the exception did not insulate the defendant from liability under the Act because the plaintiffs did not consent to its simultaneous duplication of their communications.[76] The court maintained that the central objective of the Act is to guard private communications from unauthorized duplication and interception.[77] The court reasoned that allowing Facebook to use cookie placement to receive copies of users' search history would run counter to the intention of the Party Exception.[78]

---

interpretation of the exception, reasoning that it was erroneous to interpret the exception to include third parties that gain access to a communication through deceit. *See In re Facebook, Inc.*, 956 F.3d at 608 (rejecting the Third Circuit's overbroad position as insufficient to protect the users' privacy); *In re Google Cookie*, 806 F.3d at 143–45 (settling on a more expansive conception of the Party Exception).

[75] *See In re Facebook, Inc.*, 956 F.3d at 608, 611 (determining that the plaintiffs presented sufficient evidence to establish standing and remanding the case back to the district court to consider the plaintiffs' claims).

[76] *See id.* at 607–08 (providing that the Act serves to protect the privacy rights of the plaintiffs from unknown, unconsented-to interceptions). The court noted that rooted in the Act is Congressional consideration of historic privacy interests pertaining to private, personal communications. *See id.* at 598 (citing S. REP. NO. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556) (noting that the Act is the principal law serving this purpose).

[77] *See In re Facebook, Inc.*, 956 F.3d at 608 (citing Joffe v. Google, 746 F.3d 920, 931 (9th Cir. 2013)) (concluding that permitting the defendants to track and copy the plaintiffs' data violated the Act's principal purpose). In 2013, in *Joffe v. Google, Inc.*, the Ninth Circuit determined that when enacting the Act, Congress did not mean to permit unapproved encroachments on the personal privacy of electronic communications. *See* 746 F.3d at 931 (drawing on the legislative history of the Act to support this principle). In *Joffe*, the concern was whether the Act allowed entities to gather personal data from browsing activity that occurred on unencrypted wireless (Wi-Fi) networks. *See id.* at 924 (determining that the Act prohibited the defendant's appropriation of data from unencrypted Wi-Fi networks). The court maintained that this mode of acquiring data was an unauthorized interception and was counter to Congressional intent for the protections of the Act. *See id.* at 931 (citing *In re Pharmatrak*, 329 F.3d at 18) (referencing the Act's legislative intent).

[78] *See In re Facebook, Inc.*, 956 F.3d at 608 (providing three interrelated justifications for determining that the defendants were unauthorized third parties that accessed and duplicated the plaintiffs' electronic communications, so the Party Exception did not apply). The court was concerned that a more expansive interpretation and application of the Party Exception would result in the exception overshadowing the rule. *See id.* (determining that a broad construction of the exception would run counter to the proper function and legislative intent of the Act). The court added that it was of no consequence that Facebook received a copy of the GET request simultaneous to the users' intended transmission. *See id.* at 607 (detailing that Facebook only received a simultaneous GET request because it had placed tracking cookies on the plaintiffs' browsers, prompting such a transmission to occur). Although the timing of the acquisition is important, the key issue under the Party Exception is whether the plaintiffs had authorized Facebook to access this communication or whether their access constituted an interception. *See id.* (orienting the Act's focus on determining who was a "party" to the communication and questioning whether a first party gave Facebook the requisite consent to gain entrance to the communication).

III. The Ninth Circuit's Holding Promotes the Legislative Intent of the Wiretap Act and Demonstrates the Importance of Data Privacy

The Ninth Circuit's 2020 decision, *Davis v. Facebook, Inc.* (*In re Facebook*), sought to elucidate the meaning of the Party Exception within the context of electronic communications.[79] The Ninth Circuit's ruling joined the majority approach by rejecting the notion that an entity may become party to a communication through deceptive measures.[80] Section A of this Part details the manner in which the court's interpretation of the Act aligns with legislative history and intent.[81] Section B argues that applying the Party Exception to circumstances where a third party gains unauthorized access to a transmission would eviscerate the purpose of the Act.[82]

A. The Ninth Circuit and Majority's Interpretation Supports Legislative Purpose

The legislature and courts have debated the meaning and application of the Act since its inception, paying particular concern to the protections afforded to electronic communications.[83] The Committee on the Judiciary acknowledged that the Act has two key aims—to provide privacy protections for covered transmissions and to outline the conditions and situations under which

---

[79] *See* 956 F.3d 589, 608 (9th Cir. 2020) (providing that, based on the legislative history and intent and the precedent that other circuits established, a logical interpretation of the Act prohibits the unauthorized duplication of users' data).

[80] *See id.* (rejecting the Third Circuit's position that treats entities that use deceitful means to acquire direct transmissions as intended parties to a communication, despite lacking a first party's knowledge and consent).

[81] *See infra* notes 83–88 and accompanying text.

[82] *See infra* notes 89–95 and accompanying text.

[83] *See* Boyden, *supra* note 22, at 682–83, 699 (maintaining that the original definition of an interception under the Act in 1968 was fairly indistinct and that the ECPA's enactment did not remedy the confusion as it simply adapted the original Act to encompass electronic communications). In its description of an interception, the Act does not mention the role of parties in a communication, thereby allowing the defendants to claim party consent. *See id.* at 688–89 (noting that the Act's lack of mention of a non-party intercepting the communication allowed the defendants to argue that they were authorized parties and thus incapable of intercepting the transmission). In effect, the legislature merely established that, based on the concern for privacy protections, unauthorized monitoring and acquisition of communications qualifies as an interception when it occurs without party consent. *See* S. Rep. No. 90-1097, at 66 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2156 (explaining that, in addition to the unpermitted acquisition and surveillance of electronic communications, the Act forbids the subsequent use of that information for advertising, sales, or other uses). Notably, as technology and modes of communication have evolved, so too have discussions of the Act's continued applicability. *See* Guffin, *supra* note 2, § 2.1 (detailing a significant number of cases under the Act, chronologizing the evolving history of courts' interpretations of the Act as technology has evolved). *But see* Kerr, *supra* note 1, at 419 (concluding that the Act, and the ECPA generally, are no longer the best pieces of legislation to address the modern technological landscape and privacy concerns given the increasing reliance on computers and the Internet).

courts authorize interceptions.[84] Central to the Ninth Circuit's holding in *In re Facebook* was the legislative focus on privacy protections.[85] The Act's exceptions require narrow construction because the motivation for the Act was the need for comprehensive protection of Internet users' privacy interests.[86] An unknown third party's interception of a communication, by its nature, is contrary to the Act's desire to protect communications from unauthorized entities.[87] With this construction, the Ninth Circuit correctly determined that, because the Act does not clearly define how an entity becomes a party to a communication, the court should rely on the ordinary meaning of the term "party."[88]

B. The Ninth Circuit's Ruling Protects Against Overly Expansive Constructions of the Party Exception

The Ninth Circuit's ruling protects the integrity of the Act by conserving its intended breadth while maintaining a distinct carve-out for the Party Excep-

---

[84] *See* S. REP. NO. 90-1097, at 66 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 (stating that the Act only permits interceptions that fall into an exception or are done by authorized law enforcement personnel conducting investigatory surveillance). These two purposes ensure the preservation of privacy for oral and wire transmission. *See id.* (limiting the number of third parties accessing the communication allows the Act to safeguard constitutionally assured rights of privacy). The Committee posited that "virtually all" agree that there is limited rationale for allowing an entity to intercept a communication absent party consent. *See id.* at 2156 (explaining its inhibition of unauthorized interception and use of communication contents).

[85] *See In re Facebook, Inc.*, 956 F.3d at 598, 608 (citing Joffe v. Google, 746 F.3d 920, 931 (9th Cir. 2013)) (deducing that the Act's legislative history demonstrates Congress's desire to prevent authorized interceptions of communications).

[86] *See id.* (outlining the chief objective of the Act as the preservation of privacy in (electronic) communications and describing legislative intent's focus as preventing unconsented-to third parties from intercepting communications); Levinson, *supra* note 2, at 483 (highlighting that the Act's legislative focus and history support strong privacy protections). Levinson identified four pertinent canons of interpretation: that courts should interpret statutes according to their plain meaning, that courts should read statutes holistically, that differences in terms demonstrate differences in intent, and *expressio unius est exclusio alterius*. *Id.*; *see also Expressio Unius Est Exclusio Alterius*, BLACK'S LAW DICTIONARY, *supra* note 35 (defining *expressio unius* as the canon that the expression of one notion implicates the exclusion of another, alternative notion). These canons allow courts to apply the Act in a manner that provides substantial privacy protections. *See* Levinson, *supra* note 2, at 483 (discussing the Act in relation to employee rights).

[87] *See In re Facebook, Inc.*, 956 F.3d at 608 (discussing the privacy concerns of the Act that motivated the court's decision); Boyden, *supra* note 22, at 704 (adding that the privacy focus of the Act centers on whether third parties intercept communications without the consent of a first party).

[88] *See In re Facebook, Inc.*, 956 F.3d at 607 (adopting the majority's stance that unauthorized third parties are not "parties" to a communication within the meaning of the term); *see also* Brief for Plaintiff-Appellants [Redacted Version] at 45, Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589 (9th Cir. 2020) (No. 17-17486), 2018 WL 3134964 at *45 (arguing that it is unreasonable to permit Facebook to access all the plaintiffs' communications simply by virtue of having placed tracking cookies on the plaintiffs' computers). A 'party' to a communication is some entity that participates in the transaction. *Party*, BLACK'S LAW DICTIONARY, *supra* note 35.

tion.[89] The holding rejects the Third Circuit's approach on the basis that the Act principally serves to bar unauthorized acquisitions of private communications and should not extend to permit party entrance by deceit.[90] In joining the majority, the Ninth Circuit correctly demonstrated that courts should not apply the Party Exception to entities gaining party membership through deceptive means because it risks the scope of the exception outreaching the applicability of the Act, itself.[91] To allow the Party Exception to encompass unknown third parties who gain access through fraudulent means would render the Act futile.[92] It would be unable to sufficiently protect electronic communication and data privacy because this type of interception is a commonplace means of privacy intrusion.[93] The *In re Facebook* ruling aligns with the central principles of

---

[89] *See In re Facebook, Inc.*, 956 F.3d at 608 (providing that, to preserve the integrity of the Act, the court cannot permit the application of the Party Exception in instances of unauthorized acquisition, duplication, and use of plaintiffs' transmission).

[90] *See id.* (citing *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 143 (3d Cir. 2015)) (determining that an entity is not a party simply because it received a direct copy of a communication when it received the transmission by deceit). The Senate Report provided that, in application, courts should use the Act to prohibit interceptions from "unseen auditors"—these "unseen" entities are unconsented-to third parties, such as Facebook was in *In re Facebook*. *See* 956 F.3d at 908 (using the Act's legislative intent to justify the rejection of the Party Exception where the defendant was an unconsented-to third party and analogizing the defendant to "an unseen auditor"); S. REP. NO. 90-1097, at 67–68 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2154, 2156 (discussing the need to establish the Act in a manner that inhibits the unauthorized acquisition of transmissions).

[91] *See In re Facebook, Inc.*, 956 F.3d at 608 (delineating the majority's narrow construction of the Party Exception as it aligns with legislative intent to broadly protect privacy rights); Levinson, *supra* note 2, at 494 (maintaining that the Court should narrowly interpret the exceptions to the Act that may allow third parties to intercept transmissions in order to prevent over-expansive exceptions that no longer allow for the basic purpose of protecting the privacy of electronic communications). *Compare In re Google Cookie*, 806 F.3d at 144 (finding that within the Seventh Circuit's 1964 case, *United States v. Pasha*, there was support for the notion that an entity is a party to the communication so long as they actually participate in said communication, even if they gain access through deceit or fraud), *with In re Facebook, Inc.*, 956 F.3d at 608 (determining that *In re Google* should not apply broadly to social networks because entities, such as Facebook, are not impersonating a party; rather, they are surreptitiously intercepting a communication through the installation of cookie software on the user's computer), *and* S. REP. NO. 90-1097, at 66–69 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2154–56 (delineating an increasingly restrictive legislative history of the Act, culminating in the carving out of three exceptions that the legislature intended courts to narrowly construe).

[92] *See* Levinson, *supra* note 2, at 482–83 (discussing the broad protections the Act affords, thereby requiring narrow constructions of the exceptions). When enacting the ECPA, the intention was to devise an adaptable tool for privacy protection that would account for new mechanisms of communication and attempted intrusions. *See id.* at 483 (stating that the legislative history demonstrates that Congress intended the ECPA to provide broad privacy protections).

[93] *See In re Facebook, Inc.*, 956 F.3d at 608 (noting the prevalence of using cookies to intercept GET requests and gain access to a user's communications). Claimants have brought a wide range of cases under the Act concerning the invasion of privacy resulting from cookie placement on user hard drives. *See generally* Kletter, supra note 24 (providing an extensive discussion of the various treatments of the Act as it relates to cookie placement to access transmissions). Central to these cases is the concern for the privacy interests of users when communicating electronically. *See* Blumofe v. Pharmatrak, Inc. (*In re* Pharmatrak, Inc. Priv. Litig.), 329 F.3d 9, 18 (1st Cir. 2003) (discussing the

the Act of 1986, underscoring that technological evolution should not lead to forfeitures of personal privacy.[94] *In re Facebook* opens the doors to a future of greater data privacy restrictions, a particularly striking prospect in the age of targeted advertisements, social media dominance, and internet supremacy.[95]

CONCLUSION

The United States Court of Appeals for the Ninth Circuit held in 2020, in *Davis v. Facebook, Inc.* (*In re Facebook*), that unauthorized third parties do not fall within the scope of the Party Exception to the Wiretap Act. In *In re Facebook*, Facebook acquired exact copies of the users' browsing history when they visited websites with Facebook plug-ins, even though the users were not logged into Facebook. The court determined that, although the third party received exact copies, these users did not consent to the simultaneous duplication of their web searches. As such, Facebook unlawfully intercepted the users' transmissions in violation of the Act. The court correctly employed a narrow construction of the Party Exception and protected the integrity of the Act by ensuring that the Party Exception does not become so inclusive as to overshadow the Act itself. It also aligned with legislative purpose and a history of providing broader privacy protections to modes of communication. This will become even more important as technology and modes of communication continue to evolve.

EMILY A. JORDAN

Preferred citation: 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. E. SUPP. II.-205 (2021), http://lawdigitalcommons.bc.edu/bclr/vol62/iss9/13/.

ECPA's right of action against those who intentionally intercept communications without consent from a party to the communication).

[94] *See* 956 F.3d at 608 (embracing, implicitly, that the legislative intent of the Act is to continually protect the privacy of communications as modes of communication evolve); S. REP. NO. 90-1097, at 67 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 (concluding that legislation and Congress should continue to evolve as technology evolves). Some scholars have argued that courts should apply this evolving perspective of privacy across the various laws that the ECPA encompasses, such as the Stored Communications Act. *See* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 71 (2013) (discussing the role of privacy laws in the modern context).

[95] *See* Quinn Emanuel Urquhart & Sullivan, LLP, *June 2020: Facebook, Cookies and Data Privacy: A Watershed Moment?*, JDSUPRA (July 7, 2020), https://www.jdsupra.com/legalnews/june-2020-facebook-cookies-and-data-27641/ [https://perma.cc/H4AK-626E] (advising companies that use tracking cookies of their potential risk under the Act given the Ninth Circuit's construction of the Party Exception); *see also In re Facebook, Inc.*, 956 F.3d 589 (construing the Party Exception narrowly to preserve privacy rights of parties in an electronic communication).