NOTE

COOKIES AND WIRES: CAN FACEBOOK LURE USERS INTO DIVULGING INFORMATION UNDER THE WIRETAP ACT'S PARTY EXCEPTION?

Richard T. Wang†

† B.A., Washington University in St. Louis, 2017; J.D. Candidate, Cornell Law School, 2022; General Editor, *Cornell Law Review*, Vol. 107. Special thanks to Professor James Grimmelmann for enthusiastically sharing his expertise and patiently fielding my questions regarding this Note's topic; to Lily Coad and Hun Lee for their extensive feedback; to Professor Karen Levy, Professor Ron Cytron, Professor Meg Jones, Kevin Negy, Florian Suri-Payer, Ryan Doenges, and Drew Zagieboylo for their generous consultations; and to Lilly Wang and Charles Mawby for their continual support. Lastly, thank you to all the members of *Cornell Law Review* for their hard work in preparing this Note for publication. All errors are my own.

INTRODUCTION

The advent of the Internet brought immeasurable benefits[1] to society in various ways—providing convenient access to information,[2] facilitating the purchase and sale of goods (from Amazon[3] to Fintech[4]), and offering an invaluable method of social and political communication.[5] Cookies, invented in

---

1 *See* Lisa Eadicicco, *Obama Wants to Reclassify the Internet by Turning It Into a Utility*, BUSINESS INSIDER (Nov. 10, 2014, 9:36 AM), https://www.businessinsider.com/president-obama-thinks-the-internet-should-be-a-utility-2014-11 [https://perma.cc/FZD2-C9TS] (noting that former-President Barack Obama argued that the FCC should recognize the Internet as a vital service); *Internet Access Is 'a Fundamental Right'*, BBC NEWS, http://news.bbc.co.uk/2/hi/8548190.stm [https://perma.cc/YR82-K5QS] (last updated Mar. 8, 2010) ("Almost four in five people around the world believe that access to the Internet is a fundamental right . . . .").

2 Kotagiri Ramamohanarao, Kapil Kumar Gupta, Tao Peng & Christopher Leckie, *The Curse of Ease of Access to the Internet*, *in* Information Systems Security 234 (Patrick Drew McDaniel & Shyam K. Gupta, eds., Lecture Notes in Computer Science Series No. 4812, 2007) ("The Internet has emerged as one of the most convenient and widely used media for exchanging information. The amount of information that it contains is unprecedented . . . [and] the main factor that led to its success is the ease with which anyone can access this information.").

3 Clare Duffy, *How Jeff Bezos Changed the World*, CNN, https://www.cnn.com/2019/08/16/tech/jeff-bezos-amazon/index.html [https://perma.cc/LMB5-XVWF] (last updated Aug. 16, 2019) (noting that Amazon "disrupted the retail industry" with its implementation of online shopping).

4 *See* Lenny Sanicola, *What is FinTech?*, HUFFPOST (Feb. 13, 2017, 2:50 PM), https://www.huffpost.com/entry/what-is-fintech_b_58a20d80e4b0cd37efcfebaa [https://perma.cc/KD4A-8WVA] (noting how FinTech companies have used Internet-based applications to provide financial services to consumers).

5 *See* Matt Richtel, *E-Mail Gets an Instant Makeover*, N.Y. TIMES (Dec. 20, 2010), https://www.nytimes.com/2010/12/21/technology/21email.html [https://perma.cc/V7J4-ZN67] (noting the rise in preference among young people for online chats and text messages due to their ability to facilitate real time communication); Richard T. Wang & Patrick D. Tucker, *How Partisanship Influences What Congress Says Online and How They Say It*, 49 AM. POL. RES. 76, 76 (2021) (citing GARY LEE MALECHA & DANIEL J. REAGAN, THE PUBLIC CONGRESS: CONGRESSIONAL DELIBERATION IN A NEW MEDIA AGE 18 (2012); Scott E. Adler, Chariti E. Gent & Cary B. Overmeyer, *The Home Style Homepage: Legislator Use of the World Wide Web for Constituency Contact*, 23 LEGIS. STUD. Q. 585, 585) (noting that members of Congress believe the Internet provides an important and low-cost means of communicating with their constituents).

1994, further enhanced the Internet's utility by offering a means for Internet applications to possess memory.[6] For example, cookies allow websites to "remember" a user's login information so that users do not have to repeatedly fill out their usernames and passwords upon subsequent visits.[7] Prior to cookies, websites treated each user's visit as if it were their first.[8] However, while websites use cookies to enhance the user's Internet experience, they also use cookies in a manner that poses a difficult challenge with regards to data privacy.[9] For example, when a user visits a first-party website, their information (such as their browser history) is often collected by third-party websites through cookies (usually without the user's knowledge).[10] Third-party websites then determine a user's interests based on their browsing history in order to generate personalized advertisements tailored to those interests.[11] But the information collected by third-party websites provides more than simply a summary of a user's interests—a user's web browsing history is inextricably linked to their personal information, including their "location, interests, purchases, employment status, sexual orientation, financial challenges, medical conditions," and other information that the user likely did not consent to collection.[12]

Internet users have consistently voiced concerns over data privacy throughout the past two decades.[13] A majority of

---

6 John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES (Sept. 4, 2001), https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html [https://perma.cc/RLM9-UJMM].

7 Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*, 76 S. CAL. L. REV. 893, 898 (2003).

8 Schwartz, *supra* note 6.

9 *See* Geoffrey A. Fowler, *87 Percent of Websites are Tracking You. This New Tool will let You run a Creepiness Check*, WASH. POST (Sept. 25, 2020, 3:08 PM), https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight/ [https://perma.cc/5HPX-4RQN] ("At least 87 percent of the world's most-popular Web domains engage in some form of digital tracking without you ever signing in . . . .").

10 *See id.*; Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 4 (2018).

11 *See* Jefferson Graham, *Privacy and Who's Tracking You: Where's the Villain?*, USA TODAY (June 28, 2019), https://www.usatoday.com/story/tech/talkingtech/2019/06/28/apple-google-facebook-amazon-which-gets-blame-for-tracking-you/1529075001/ [https://perma.cc/VQ3T-DKEA] (last updated July 2, 2019).

12 Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, *in* PROCEEDINGS OF THE 2012 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 413, 415 (2012).

13 *See Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the H. Subcomm. On Commerce, Trade, and Consumer Protection*, 107th Cong. 10 (2001) [hereinafter *Hearing*], ("86% of Internet users think

Americans believe that Internet companies should seek consent before acquiring user information and that website tracking practices (e.g., cookies) are a harmful invasion of privacy.[14] Furthermore, a majority of Americans believe they have little control over the data collected about them by companies and about half of that majority believe they have no control over who has access to their online searches.[15] Despite these concerns, the United States has largely left the ways in which companies collect and utilize user data unregulated.[16] Because Congress has failed to establish a general data privacy regime, Internet users frequently turn to the Wiretap Act to seek redress in cases involving user data and privacy.[17] However, the Wiretap Act's statutory language has largely failed to keep up with the development of Internet communications[18] and courts have struggled to apply the Act in such contexts.[19] As part of the courts' struggle to interpret and apply the Wiretap Act to Internet communications, the Ninth Circuit recently issued a holding in *In re Facebook, Inc. Internet Tracking Litigation*[20] (hereby referred to as "*In re Facebook*") deviating from the Third

---

Internet companies should ask people for permission to use personal information when people give it to them."); Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/6APE-5Z2N] ("[F]indings show Americans . . . have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age.").

14 *Hearing*, *supra* note 13.

15 Madden & Rainie, *supra* note 13.

16 *See* Dobkin, *supra* note 10, at 8 ("[T]here is no sweeping standard for how private firms treat data . . . ."); Yonatan Lupu, *The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?*, 9 VA. J.L. & TECH. 1, 5 (2004) ("Despite continuous calls for a definitive legislative stance on the protection of online privacy rights, Congress has not enacted a comprehensive statute.").

17 Lupu, *supra* note 16, at 5.

18 *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557, 1559 (2004) (noting that Congress last amended the Wiretap Act in 1986, before the creation of the World Wide Web, and that the Wiretap Act has "failed to keep pace with changes in and on the Internet").

19 The Fifth Circuit has characterized the Wiretap Act as "famous (if not infamous) for its lack of clarity." Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); *see also In re* Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003) ("We share the concern . . . about the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions of online communications."); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) ("When the Fifth Circuit observed that the Wiretap Act 'is famous (if not infamous) for its lack of clarity', it might have put the matter too mildly.").

20 956 F.3d 589 (9th Cir. 2020).

Circuit's holding in *In re Google Inc. Cookie Placement Consumer Privacy Litigation*[21] (hereby referred to as "*In re Google*") regarding the applicability of the Wiretap Act's party exception to third-party websites' cookies practices.[22]

This Note analyzes the circuit split regarding the Wiretap Act's party exception and cookies, and recommends a framework to aid in the application of the Wiretap Act to Internet communications. Part I of this Note provides background information on how cookies operate, the history of the Wiretap Act, and previous litigation concerning the meaning of "intercept" under the Wiretap Act. Part II discusses several important cases involving the Wiretap Act and cookies. Part III describes the split between the Third and Ninth Circuits' interpretations of the Wiretap Act's party exception in *In re Google* and *In re Facebook*, respectively. Part IV argues that courts should establish an additional "surreptitious tampering" framework to provide guidance on the meaning of "intercept" under the Wiretap Act and that it is ultimately unclear as to whether third-party websites can use cookies to perform an interception. Part IV continues to argue that Google and Facebook should not qualify for the Wiretap Act's party exception (assuming they are able to intercept, and have intercepted, users' communications through the use of cookies). Part V discusses the limitations of the "surreptitious tampering" framework and the need for congressional legislation.

I
BACKGROUND

A. The Cookies Process

Cookies provide websites with a means of "remembering" user information.[23] When an Internet user visits a web page, their browser sends a message—a "GET request"—to the web page's server telling the server what information is being requested and instructing the server to send the information back to the user.[24] The server responds by sending the requested information to the user's browser and the web page

---

21 806 F.3d 125 (3d Cir. 2015).

22 The U.S. Supreme Court has denied certiorari to hear Facebook's appeal of the decision in *In re Facebook*, leaving the disagreement in interpretation between the Ninth and Third Circuits unresolved. Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021).

23 *See* Schwartz, *supra* note 6.

24 *In re* Facebook, Inc., 956 F.3d at 607.

contents are displayed on the user's computer screen.[25] If the user is visiting a web page for the first time, the server might also send a "first-party cookie" along with the requested information.[26] The user's browser receives the cookie, a small text file, and saves it locally onto the user's computer hard drive.[27] The cookie contains a unique identifier and collects data about the user, including "the date and time of the visit, the specific pages within a site the user accessed, and . . . the information the user gave when filling out online forms."[28] If the user visits the web page again in the future, the user's browser will send the information stored in the cookie (in addition to the usual GET request) to the web page's server.[29] The web page's server will then send the web page contents and other information based on the information stored in the user's cookie (e.g., auto-populating the login information or placing previous items in the user's shopping cart) back to the user.[30] First-party cookies rarely present an issue with regards to user consent—the information collected by the cookie is information that the user intentionally communicates to the web page's server by visiting the web page and entering the information.[31]

Third-party cookies, on the other hand, are more problematic with regards to user consent.[32] As explained above, when a user visits a web page, their browser will send a GET request to the web page's server, and the server will send back information; however, in the context of third-party cookies, first-party websites will host third-party code that instructs the user's browser to send an *additional* GET request to a third-party

---

25 *See id.*

26 *See* Michal Wlosik & Michael Sweeney, *What's the Difference Between First-Party and Third-Party Cookies?*, CLEARCODE (Nov. 2, 2018), https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/ [https://perma.cc/KN4G-83KL] (last updated Mar. 16, 2021).

27 Siebecker, *supra* note 7, at 896.

28 Lupu, *supra* note 16, at 2.

29 *See id.*

30 Siebecker, *supra* note 7, at 897.

31 *See* Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. & TECH. 1, 21 (2011) ("[T]he use of first-party cookies is widely accepted . . . ."); Damian Clifford, *EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster-Tracking the Crumbs of Online User Behavior*, 5 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 194, 195 (2014) (noting that first-party cookies are generally exempt from the European Union's Data Protection Framework "unless they are also used for tracking or profiling purposes").

32 Christie Dougherty, *Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation*, 12 NE. U. L. REV. 629, 646 (2020).

website.[33] This additional GET request contains a copy of the user's request to the first-party website (including the URL of the web page that the user initially requested to see).[34] If the user's browser is sending a GET request to the third-party website for the first time, the third-party website will place a cookie onto the user's computer and create a corresponding "advertisement profile."[35] On the other hand, if the user already has a cookie, the user sends the information stored in the cookie (with the GET request) to the third-party website.[36] The third-party website matches the cookie's unique identifier with the user's advertisement profile.[37] In either case, the third-party website records the URL information (obtained from the GET request) in the user's advertisement profile and returns personalized advertisements based on the information contained in the profile (thus completing the web page that the user sees on their screen).[38] The third-party website will continually update the user's advertisement profile whenever the user visits a first-party website containing the third-party's code, thereby monitoring users' browsing history across different websites.[39] The third-party cookies process is broadly outlined below (hereby referred to as the "Cookies Process"):[40]

1. The user's browser sends a request to the website asking it to send a page back to it.
2. The website sends some information back to the requesting browser. It also sends back a message to the browser telling it where it can get additional pieces of data (e.g., third-party advertisements) that will be collected and displayed in the rendered web page presented to the user.
3. In response to the website's message regarding additional data, the user's browser automatically sends additional requests to the different computers (third parties) that host the additional data to complete the web page.

---

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

34 *See id.*

35 *See* Joseph Newman, Note, *Cookie Monsters: Locally Stored Objects, User Privacy, and Section 1201 of the DMCA*, 41 AIPLA Q.J. 511, 519 (2013); Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2217 (2019).

36 *See* Newman, *supra* note 35, at 519.

37 De Zayas, *supra* note 35, at 2217.

38 Newman, *supra* note 35, at 519.

39 De Zayas, *supra* note 35, at 2216; Newman, *supra* note 35, at 519–20.

40 Orin Kerr, *Websurfing and the Wiretap Act*, WASH. POST (June 4, 2015, 1:29 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/ [https://perma.cc/WHN3-WPEJ].

The additional requests include the URL of the web page that the browser is trying to see.

4. The different computers at the third parties send their pieces of information back to the browser to complete the web page. The computers also update the user's profile with the URL information from the request.

B. The Wiretap Act

Congress passed the Wiretap Act in 1968, prohibiting the interception[41] of all wire communications and those oral communications conducted where the participants were justified in their expectation of privacy.[42] In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) in response to the technological developments in modes of communications, such as cellular phones and emails.[43] Title I of the ECPA amended the Wiretap Act to prohibit the interception of electronic communications while Title II (the Stored Communications Act, or SCA) "added protections for wire and electronic communications retained in computer storage facilities."[44] In essence, the Wiretap Act is thought to prohibit interception of communications during *transmission* while the SCA prohibits unauthorized access of communications *in storage* and, as such, the distinction between "in transit" and "in storage" is crucial to determining how much privacy a particular communication is afforded at any given moment.[45] Although the SCA is outside the scope of this Note, the SCA generally affords fewer procedural protections to the privacy of a communication in comparison to the Wiretap Act.[46]

Lastly, the Wiretap Act contains several exceptions that allow defendants to avoid liability under the Act even if they have intercepted a communication. Two of these exceptions—

---

41 The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Subpart I.C of this Note will discuss the definition of "intercept" in greater detail; subpart IV.A will recommend a framework to further clarify the meaning of "intercept."

42 Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home*, 2 J. HIGH TECH. L. 87, 88 (2003); *see also* 18 U.S.C. § 2511(1).

43 Rahavy, *supra* note 42, at 88.

44 Michael D. Roundy, *The Wiretap Act—Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications following* United States v. Councilman*'s Rejection of the Storage/Transit Dichotomy*, 28 W. NEW ENG. L. REV. 403, 413 (2006).

45 Samantha L. Martin, Note, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 443–44 (2006).

46 *See id.* at 444.

the consent exception and the party exception—will be discussed later in the Note.[47]

C. "Intercept" Under the Wiretap Act

The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[48] Ever since the passage of the ECPA, the Wiretap Act has been marred with convoluted litigation involving its definition of "intercept" and its application to modern-day Internet communications.[49] Putting cookies aside for the moment, the Wiretap Act appears to be ill-equipped to handle even emails—a mode of communication that Congress *intended* to address with the ECPA (as opposed to cookies).[50]

1. *How Emails are Transmitted*

The Internet is "a network of interconnected computers that facilitates the transfer of information from one computer to another."[51] Emails transmitted through the Internet are first broken down into smaller pieces of data—"packets"—and then sent along a series of intermediate routers until the packets reach their destination.[52] During this process, the intermediate routers "store the packets in memory, retrieve the address of their destination, and determine where to send the packets next."[53] These routers may sometimes reassemble the packets to copy the contents of the email in case they cannot immediately transfer the packets.[54] Upon transfer, the routers delete the copies shortly thereafter.[55] Once all of the packets

---

47 *See infra* subpart II.A and Part III; *see also* 18 U.S.C. § 2511(2)(d) (outlining the Wiretap Act's consent and party exceptions).

48 18 U.S.C. § 2510(4).

49 The Fifth Circuit has characterized the Wiretap Act as "famous (if not infamous) for its lack of clarity." Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); *see also In re* Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003) ("We share the concern . . . about the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions of online communications."); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) ("When the Fifth Circuit observed that the Wiretap Act 'is famous (if not infamous) for its lack of clarity, it might have put the matter too mildly. Indeed, the intersection of the Wiretap Act and the [SCA] is a complex, often convoluted, area of the law.").

50 Lupu, *supra* note 16, at 4.

51 Martin, *supra* note 45, at 448.

52 *See id.* at 448–49.

53 *See id.* at 449.

54 *See id.*

55 *See id.*

arrive at their destination—the recipient's mail server—they are reassembled to form the original email message.[56] A "mail delivery agent" then delivers the email to the recipient user's inbox, where the user may access and read the email.[57] This whole process usually takes less than a few seconds.[58] Thus, in contrast to oral and wire communications, emails are constantly "in transit" and "in storage" simultaneously—a "linguistic but not a technological paradox."[59]

2. *The "Storage/Transit Dichotomy" and the "Contemporaneous" Requirement*

Courts have struggled to determine whether a third-party surveillant's acquisition of an email in transient storage incidental to its transmission is an interception in violation of the Wiretap Act or an unauthorized access to stored communications in violation of the SCA; their previous holdings have produced a relatively unclear answer.[60] In *Steve Jackson Games, Inc. v. U.S. Secret Service*, the Fifth Circuit held that the government did not violate the Wiretap Act when it seized a computer and read private emails stored on the computer without a wiretap order.[61] In issuing its holding, the Fifth Circuit relied on a canon of statutory construction[62] known as the *Russello* presumption: "Congress's inclusion of particular language in one section of a statute and omission of similar language in a parallel section should be read as a deliberate inclusion and exclusion, respectively, of the matter contained in that language."[63] In particular, the Fifth Circuit noted that the Wiretap Act's definition of "wire communication" included "any *electronic storage* of [wire] communication" and that the Act's definition of "electronic communication" did not contain similar language to include "any electronic storage" of electronic communication.[64]

---

56 *See id.* at 449–50.

57 *See id.* at 450.

58 *See id.*

59 *See id.* at 443.

60 *See* Martin, *supra* note 45, at 447 (noting that courts addressing this issue have made inconsistent holdings because the Wiretap Act's text, structure, and legislative history "do not shed sufficient light on the meaning of the statute").

61 36 F.3d 457 (5th Cir. 1994).

62 A canon is a judicial principle or method of reasoning that courts may use when construing a statute. *See* Anita S. Krishnakumar & Victoria F. Nourse, *The Canon Wars*, 97 TEX. L. REV. 163, 168 (2018).

63 Roundy, *supra* note 44, at 422.

64 *Steve Jackson Games, Inc.*, 36 F.3d at 461. The definition of "wire communications" was later amended in 2001 by the Patriot Act to remove the language concerning wire communications in electronic storage. *See* Martin, *supra* note 45, at 451–52.

Consequently, the Fifth Circuit determined that Congress did not intend for "intercept" to apply to electronic communications in electronic storage, including the emails in the instant case (which were held in electronic storage, i.e., the computer's hard drive).[65] The Fifth Circuit's interpretation of "intercept" under the Wiretap Act is known as the "storage/transit dichotomy."[66]

In *United States v. Councilman*, the First Circuit dealt with the same issue of applying the Wiretap Act to emails acquisitioned in transient electronic storage.[67] In *Councilman*, the defendant duplicated the incoming emails of his clients and read the duplicates without authorization.[68] The duplication occurred while the emails were in temporary electronic storage (either in the computer's random access memory or hard disks).[69] The defendant argued that the emails were not electronic communications protected by the Wiretap Act because they were acquired while in transient storage, and, in doing so, relied on the same *Russello*-presumption reasoning adopted by the Fifth Circuit in the *Steve Jackson* decision.[70] The First Circuit, however, rejected the defendant's argument.[71] The First Circuit first held that the *Russello* presumption is weakened if (1) the language of the two provisions at issue is not parallel[72] and (2) the history of the two provisions is complex.[73] The First Circuit continued to note that the definitions for "wire communication" and "electronic communication" were not linguistically parallel, and that the latter definition was "drafted from scratch" under the ECPA.[74] Next, the First Circuit recognized that another canon of construction conflicted with the *Russello* presumption—"[w]here Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent."[75] In particular, the First Circuit

65 *Steve Jackson Games, Inc.*, 36 F.3d at 461–62.
66 Roundy, *supra* note 44, at 418–19.
67 418 F.3d 67 (1st Cir. 2005); Roundy, *supra* note 44, at 421–22.
68 *Councilman*, 418 F.3d at 70–71.
69 *See id.* at 71.
70 *See id.* at 72–73.
71 *See id.* at 79.
72 "[I]f the language of the two provisions at issue is not parallel, then Congress may not have envisioned that the two provisions would be closely compared in search of terms present in one and absent from the other." *Id.* at 74.
73 *Id.* ("For example, if the first provision was already part of the law, whereas the second is entirely new, Congress may have paid less attention to subtle differences between the two.").
74 *See id.* at 75.
75 *See id.* at 75–76 (quoting TRW v. Andrews, 534 U.S. 19, 28 (2001)).

noted that Congress had expressly stipulated several exceptions to the definition of "electronic communication," and these exceptions did not include electronic communications held in electronic storage.[76] The First Circuit ultimately found that these factors sufficiently rebutted the defendant's application of the *Russello* presumption.[77] Turning to legislative intent, the First Circuit determined that Congress passed the ECPA with the intent to protect email communications from interception and that Congress did not intend to influence the definition of "electronic communication" by adding the language concerning "electronic storage" to the definition of "wire communication."[78] Consequently, the First Circuit held that "electronic communication" under the Wiretap Act includes such communication held in "transient electronic storage . . . intrinsic to the communication process for such communications"[79] and that the defendant intercepted the emails in violation of the Wiretap Act.[80]

The Seventh Circuit also adopted the First Circuit's approach when it addressed a similar case in *United States v. Szymuszkiewicz*.[81] In *Szymuszkiewicz*, the government charged the defendant for violating the Wiretap Act when he created a rule in his supervisor's inbox to forward incoming emails to the defendant's inbox.[82] The defendant argued that he should have been charged under the SCA rather than the Wiretap Act.[83] The defendant asserted that the word "'interception' means catching a thing in flight" and that he did not intercept the emails because the emails had already reached their destination—the supervisor's inbox—before they were copied and forwarded to the defendant.[84] The Seventh Circuit, however, found that the emails were duplicated on the server side, and thus the emails were copied and forwarded to the

---

76 *See id.*

77 *See id.*

78 *See id.* at 76, 78.

79 *See id.* at 79.

80 *See id.* at 85. Note, however, that the Ninth Circuit has held the opposite. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 n.6 (9th Cir. 2002) ("The dissent, amici, and several law review articles argue that the term 'intercept' must apply to electronic communications in storage because storage is a necessary incident to the transmission of electronic communications . . . . While this argument is not without appeal, the language and structure of the ECPA demonstrate that Congress considered and rejected this argument.").

81 622 F.3d 701 (7th Cir. 2010).

82 *See id.* at 703.

83 *See id.*

84 *See id.*

defendant's inbox *before* they reached the supervisor's inbox.[85] Citing *Councilman*, the Seventh Circuit held that the Wiretap Act applied to the emails even if they were duplicated while residing in the servers (transient electronic storage intrinsic to the emails' communication process).[86]

The Seventh Circuit also clarified a requirement for an interception under the Wiretap Act: the defendant's acquisition of the communication must be contemporaneous with the transmission of the communication.[87] The "contemporaneous" requirement was primarily established by the Fifth Circuit in *United States v. Turk*.[88] Although *Turk* was decided before Congress amended the Wiretap Act with the ECPA, many circuits have held that Congress intended to retain the "contemporaneous" requirement for interception under the Wiretap Act.[89] In *Szymuszkiewicz*, the Seventh Circuit applied the "contemporaneous" requirement on a "human" timeframe—the court held that the defendant acquired the emails contemporaneously with their transmission because both the defendant

---

85 *See id.* at 703–04. The Seventh Circuit also surmised, in dicta, that the defendant would have violated the Wiretap Act even if the emails were copied and forwarded *after* arriving in the supervisor's inbox. Specifically, the court analogized the supervisor's computer to an intermediary router sending the emails' packets along to their destination (in this case, the defendant's inbox). Citing *Councilman*, the court concluded that the Wiretap Act would apply to the emails in transient electronic storage at the supervisor's computer during its transmission to the defendant's computer. *See id.* at 706. Note that not all courts take this position. *See* Bunnell v. Motion Picture Ass'n of Am., 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (holding that the defendant did not intercept emails by configuring the plaintiff's email server software to copy and forward emails to defendant's inbox); Global Policy Partners, LLC v. Yessin, 686 F. Supp 2d 631, 638 (E.D. Va. 2009) ("[I]nterception [under the ECPA] includes accessing messages in transient storage on a server during the course of transmission, but does not include accessing the messages stored on a destination server."). *See also* Martin, *supra* note 45, at 474 (arguing that emails that have reached their proper recipient but have remained unopened by the addressee should be considered "stored" for the convenience of the addressee, rather than as necessary to their transmission, and should thus be under the protection of the SCA rather than the Wiretap Act).

86 *Szymuszkiewicz*, 622 F.3d at 706.

87 *See id.* at 705–06. This requirement is henceforth referred to as the "contemporaneous" requirement.

88 United States v. Turk, 526 F.2d 654 (5th Cir. 1976); Roundy, *supra* note 44, at 418.

89 *Szymuszkiewicz*, 622 F.3d at 705–06; Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876–77 (9th Cir. 2002); United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994); Fraser v. Nationwide Mut. Ins., 352 F.3d 107, 113–14 (3d Cir. 2003). Note that the First Circuit in *Councilman* chose not to reach this issue. *See* 418 F.3d 67, 79–80 (1st Cir. 2005) ("Because the facts of this case and the arguments before us do not invite consideration of either the existence or the applicability of a contemporaneity or real-time requirement, we need not and do not plunge into that morass.").

and his supervisor "received each [email] with *no more than an eyeblink* in between."[90] In issuing its holding, the Seventh Circuit reasoned that "the pace of transmission [of emails] would depend on the packets' travel, not just the order in which they were originally generated. If, for example, more packets were lost for one [email] than another, or if one [email]'s packets traveled through more-congested routers, the [emails] would arrive at different times. Transmission speed also depend[ed] on the email protocol selected. The time at which each recipient obtained each [email] also depended on whether the recipient's computer was connected to the Outlook server when the [email] reached the server."[91] In other words, the Seventh Circuit argued that the "contemporaneous" requirement *must* be applied on a human timeframe because the technological process by which packets operate makes it "impossible to apply a timing requirement to information sent over [the Internet]."[92] Other courts, however, have adopted a different approach by applying the "contemporaneous" requirement on a "machine" timeframe. In particular, the Ninth Circuit held in *Konop v. Hawaiian Airlines* that "intercept" means "to stop, seize, or interrupt in progress or course before arrival,"[93] thus requiring that the acquisition of the communication occur *before* the communication mechanically reaches its intended recipient.[94]

---

90 *Szymuszkiewicz*, 622 F.3d at 706 (emphasis added).

91 *Id.* at 705.

92 Christian Levis, Note, *Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 191, 214–215 (2011). This Note finds the Seventh Circuit's reasoning unconvincing. As other courts have held, "acquisition" under the Wiretap Act occurs "when the contents of a . . . communication are captured or redirected in any way." United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992). Consequently, even if it is unclear *a priori* as to when a defendant receives a duplicated email relative to the arrival of the original email in the recipient's inbox, the defendant nonetheless "captures" the message *during* its transmission and *before* its arrival in the intended recipient's inbox—the duplication occurs at the email's server, before the server sends the original email to the intended recipients inbox. *Szymuszkiewicz*, 622 F.3d at 704. Courts interpreting the holding in *Szymuszkiewicz*, however, have rejected the application of *Rodriguez* in cases involving electronic communications. *See* Shefts v. Petrakis, 2013 WL 489610 at *1 n.2 (C.D. Ill. Feb. 8, 2013).

93 *See Konop*, 302 F.3d at 879 (quoting WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 630 (1985)).

94 *See* Ruby Knight Inc. v. Dark Stage Lighting Servs. Inc., 2018 WL 1382528 at *4 n.3 (D. Ariz. Mar. 19, 2018) ("[T]he Seventh Circuit's assertion in *Szymuszkiewicz* that a 'computer ma[king] copies of [emails] . . . within a second of each message's arrival and assembly' is a *contemporaneous* interception is in conflict with the *Konop* Court's conclusion that 'interception' occurs 'before arrival.'" (emphasis added)). The Eleventh Circuit has adopted the Ninth Circuit's approach, holding that "a contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic

The outcome of the above litigation has produced a relatively unclear answer to the meaning of "intercept" under the Wiretap Act in the context of electronic communications.[95] First, the Fifth Circuit's storage/transit dichotomy is intuitively appealing in consideration of the statutory text of the SCA. The SCA, which prohibits unauthorized access to "electronic communication while it is in electronic storage,"[96] defines "electronic storage" extraordinarily broadly—"any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"—suggesting that emails acquisitioned even while in transient electronic storage during transmission would fall under the SCA rather than the Wiretap Act.[97] However, the First and Seventh Circuits' holdings are likely more in the correct direction—Congress passed the ECPA with the intent of protecting emails from interception, and thus it would seem inconsistent for courts to omit Wiretap protections for emails that are in transient electronic storage at various points along the transmission path as a result of the technological framework that makes email possible in the first instance.[98] Accordingly, this Note adopts the First and Seventh Circuits' approach: a surveillant may intercept an electronic communication, even if they acquire the communication while it is in transient storage, if the storage is intrinsic to—and thus a part of—the transmission process for such communications. Second, with regards to the "contemporaneous" requirement, it is unclear whether courts should ap-

---

communications." United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003).

95 *See* Martin, *supra* note 45, at 472 n.215 ("Even after the First Circuit made their final decision in United States v. Councilman, 'the differences in court rulings indicate that the issue [regarding the meaning of 'intercept'] is still ambiguous.'" (quoting *Inslee Praises Court Decision on E-Mail Privacy*, Aug. 11, 2005, http://www.house.gov/inslee/issues/privacy/tech_email_court.html (last visited Jan. 1, 2006))).

96 18 U.S.C. § 2701(a)(2).

97 18 U.S.C. § 2711(1) (incorporating the definition of "electronic storage" under 18 U.S.C. § 2510(17)(A)). *But see* Roundy, *supra* note 44, at 430 (arguing that the language in 18 U.S.C. § 2701(c) implies that it is possible to intercept an electronic communication while it is in electronic storage, although it is unclear whether interception of emails falls under this possibility).

98 Roundy, *supra* note 44, at 428, 428 n.182; *see also* Martin, *supra* note 45, at 466 ("Congress largely rejected the [Department of Justice]'s view that e-mail did not deserve all of the procedural protections provided by the Wiretap Act."). *But see id.* at 469-470 ("Although the First Circuit's final decision in *Councilman* determined that electronic communications in temporary electronic storage en route to their destination are capable of being intercepted in violation of the Wiretap Act, other appellate courts have previously looked towards the . . . legislative history of the Wiretap Act in determining that those communications cannot be so intercepted.").

ply the Seventh Circuit's human timeframe approach or the Ninth Circuit's machine timeframe approach. Because the merits of either approach are outside the scope of this Note, this Note will consider both approaches in its analysis under section IV.B.1.[99]

II
COOKIES LITIGATION UNDER THE WIRETAP ACT

Application of the Wiretap Act to other forms of Internet communication—beyond email—is equally, if not more, troublesome. The Wiretap Act is largely inadequate to address cookies,[100] and Congress could not have contemplated the invention of cookies when it passed the ECPA.[101] Nonetheless, in the absence of a federal data privacy regime,[102] plaintiffs have historically invoked the Wiretap Act's broad language of "electronic communication" to seek relief from third-party companies' alleged misuse of cookies to inconspicuously collect user information.[103]

A. The Wiretap Act's Consent Exception

The Wiretap Act includes several exceptions to the general prohibition of interception of electronic communications.[104] One of the most important exceptions in the context of web monitoring is the consent exception,[105] which states that a defendant does not violate the Wiretap Act if one of the parties to the communication has given prior consent to the defendant's interception.[106] The consent exception has allowed

---

99 Note that GET requests are transmitted via the Internet in a similar process as emails. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001) (explaining how data is transmitted over the Internet).

100 *See* Lupu, *supra* note 16, at 4 (claiming that the Wiretap Act "do[es] not adequately address the interception of online information by Web monitors").

101 *See id.* at 7 (arguing that "Congress could not have contemplated that companies would be formed with the purposes of designing monitoring technology, seizing information from other users, bundling that information into aggregate statistics, and selling these to their clients" when it drafted the ECPA).

102 *See* Dobkin, *supra* note 10, at 8; Lupu *supra* note 16, at 5.

103 Lupu, *supra* note 16, at 5, 7; *see also* Filip Babic, *Rethinking Online Privacy Litigation as Google Expands Use of Tracking: Giving Meaning to Our Online Browsing and the Federal Wiretap Act*, 36 HASTINGS COMMC'N & ENTM'T L.J. 471, 480 (2013) (noting that the Wiretap Act can be "read broadly"); Martin, *supra* note 45, at 466 ("Congress indicated that the term 'electronic communication' [under the Wiretap Act] should be defined broadly . . . .").

104 18 U.S.C. § 2511(2).

105 Lupu, *supra* note 16, at 7.

106 18 U.S.C.§ 2511(2)(d). However, defendants may not qualify under the consent exception if they intercepted a communication for the purpose of committing a criminal or tortious act. *See id.*

third-party companies to largely escape liability under the Wiretap Act in cases involving cookies.[107] For example, in *In re DoubleClick*, plaintiffs alleged that the online advertising company DoubleClick violated the Wiretap Act by using cookies to intercept electronic communications between Internet users and DoubleClick-affiliated websites.[108] Specifically, users found that whenever they visited a DoubleClick-affiliated website, their computer simultaneously contacted DoubleClick's server to send personal information such as names, email addresses, home and business addresses, telephone numbers, searches performed on the Internet, and the websites they visited.[109] DoubleClick conceded that it intercepted users' communications but argued that it qualified under the Wiretap Act's consent exception.[110] The court sided with DoubleClick, holding that the affiliated websites were parties to the users' communications and that the websites consented to DoubleClick's interception by soliciting DoubleClick's advertising services.[111] The court also noted that DoubleClick's activities were neither criminal nor tortious. Specifically, the court found that DoubleClick was not "primarily motivated" to commit a criminal or tortious act when it intercepted the communications, nor were such intentions a determinative factor behind DoubleClick's acts.[112] Instead, the court believed that DoubleClick intercepted the communications as part of its "highly-publicized market-financed business model in pursuit of commercial gain"—a permissible goal under § 2511(2)(d).[113]

In another case dealing with similar facts—*In re Pharmatrak, Inc. Privacy Litigation*—plaintiffs alleged that the defendant Pharmatrak intercepted users' communications to Pharmatrak's client websites through the use of cookies.[114] Plaintiffs claimed that Pharmatrak used its cookies to collect information regarding users' "names, addresses, telephone

---

107 Lupu, *supra* note 16, at 7–8.

108 154 F. Supp. 2d 497, 499–501, 500 (S.D.N.Y. 2001).

109 *See id.* at 503.

110 *See id.* at 514.

111 *See id.*

112 *See id.* at 518.

113 *See id.* at 518–19. The court noted that DoubleClick's "technology and business strategy have been described, and indeed promoted, in the company's Security and Exchange Commission . . . filings and have been the focus of numerous articles in prominent periodicals and newspapers[,]" and concluded that "DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites." *Id.*

114 329 F.3d 9, 12 (1st Cir. 2003).

numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website."[115] Pharmatrak argued that it qualified for the Wiretap Act's consent exception because its client websites agreed to host Pharmatrak's code.[116] The district court agreed with Pharmatrak and, citing *DoubleClick*, held that the client websites consented to Pharmatrak's interception by contracting for Pharmatrak's services and hosting Pharmatrak's code on their websites.[117]

On appeal, however, the First Circuit found that the district court erroneously construed the client websites' consent.[118] The First Circuit held that a "reviewing court must inquire into the *dimensions of the consent* and then ascertain whether the interception exceeded those boundaries," and found that the district court failed to inquire as to the precise limits of the client websites' consent.[119] In particular, the First Circuit argued that the district court misapplied the holding in *DoubleClick*.[120] In that case, the court held that affiliate websites consented to DoubleClick's interception when they "purchased [DoubleClick's] services *for the precise purpose* of creating individual user profiles."[121] The First Circuit argued that the instant case was a "mirror image" of *DoubleClick* because the client websites solicited Pharmatrak's services on the explicit condition that Pharmatrak *refrain* from collecting personal information.[122] Consequently, the First Circuit determined that neither the client websites nor its users consented to Pharmatrak's interception, and thus held that Pharmatrak violated the Wiretap Act.[123]

---

115 *See id.* at 14–15.

116 *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 11 (D. Mass. 2002), *rev'd sub nom.*, 329 F.3d 9 (1st Cir. 2003).

117 *See id.* at 12. The district court continued to note that plaintiffs failed to demonstrate that Pharmatrak acted with a tortious purpose. *See id.*

118 *In re Pharmatrak, Inc.*, 329 F.3d at 13.

119 *Id.* at 19–20 (quoting Gilday v. Dubois, 124 F.3d 277, 297 (1st Cir. 1997)); Lupu, *supra* note 16, at 13.

120 *In re Pharmatrak, Inc.*, 329 F.3d at 20.

121 *See id.* (emphasis added).

122 *See id.* at 20.

123 *See id.* at 20–21. The First Circuit also rejected Pharmatrak's argument that there was no interception because "there were always two separate communications: one between the Web user and [Pharmatrak's] Client, and the other between the Web user and Pharmatrak." *See id.* at 22. In doing so, the First Circuit held that "the Wiretap Act merely require[s] that the acquisition occur at the same time as the transmission; [it] do[es] not require that the acquisition somehow constitute the *same* communication as the transmission." *Id.* (empha-

B. URLs as Content Under the Wiretap Act

The Wiretap Act defines "contents" as "any information concerning the substance, purport, or meaning of [a] communication."[124] In *In re Google*, the Third Circuit dealt with the question of whether information collected by third-party websites—URLs—are content within the meaning of the Wiretap Act.[125] The district court in the same case held that URLs were not content but rather extrinsic information used to route a communication.[126] However, the Third Circuit rejected the district court's "categorical assessment that location identifiers *never* 'concern the substance' . . . of a communication," holding that routing information may be considered as content if it is "part of the substantive information conveyed to the recipient" rather than solely performing a routing function.[127] The Third Circuit further recognized that URLs may simultaneously perform a routing function while taking on a form as content.[128] For example, the Third Circuit noted that URLs sometimes reproduce a phrase entered by a user into a search engine by appending the phrase to the end of the URL.[129] Consequently, the search phrase not only performs a routing function (as part of the URL), but also "reveal[s the] contents, *i.e.*, the 'substance' and 'meaning' of the communication[,] that the user is conducting a search for information on a particular topic."[130] Under this understanding, the Third Circuit held that Google's broad collection of URLs through the use of cookies likely involved the collection of some URLs that could be considered content under the Wiretap Act.[131]

---

sis added). The holdings previously discussed above in section I.C.2 also illustrate that one may intercept a communication merely by duplicating it.

124 18 U.S.C. § 2510(8).

125 806 F.3d 125, 139 (3d Cir. 2015).

126 *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 444 (D. Del. 2013), *aff'd in part*, *vacated in part*, *remanded*, 806 F.3d 125 (3d Cir. 2015) ("[A] URL is a location identifier and does not 'concern the substance, purport, or meaning' of an electronic communication." (quoting 18 U.S.C. § 2510(8))).

127 *In re Google Inc.*, 806 F.3d at 136. *See also* Kerr, *supra* note 40 (explaining how URLs can be considered both routing information and content).

128 *See In re Google Inc.*, 806 F.3d at 138.

129 *See id.*

130 *See id.* at 137 (quoting 18 U.S.C. § 2510(8)).

131 *See id.* at 139.

III
THE CIRCUIT SPLIT REGARDING THE WIRETAP ACT'S PARTY EXCEPTION

In April 2020, the Ninth Circuit heard *In re Facebook*, a case involving Facebook's cookies practices and the Wiretap Act's party exception.[132] The party exception states that a defendant does not violate the Wiretap Act if the defendant is a party to the intercepted communication.[133] The Ninth Circuit's holding in *In re Facebook* marks a split with the Third Circuit's holding in *In re Google*.[134]

A. The Third Circuit's Holding in *In re Google*

In *In re Google*, partially discussed above, plaintiffs alleged that Google violated the Wiretap Act by intercepting electronic communications via cookies in contravention of users' cookie blockers.[135] Although Google assured users that certain cookie blockers adequately blocked third-party cookies from collecting user information, Google (as well as other defendant advertising companies) nonetheless exploited loopholes in the cookie blockers to use its cookies to collect user information.[136] In its brief, Google argued that it did not violate the Wiretap Act because it qualified under several of the Wiretap Act's exceptions.[137] Specifically, Google argued that it qualified under the Wiretap Act's party exception because the users voluntarily sent the GET requests directly to Google's servers (making Google a party to the users' communications),[138] and that it qualified under the Wiretap Act's consent exception because affiliated websites hosted Google's code and thus consented to Google's interception.[139] The Third Circuit ultimately ruled in Google's favor, adopting Google's argument that Google was a party to the communication—the users "sent [URL information]

---

132 956 F.3d 589 (9th Cir. 2020).

133 18 U.S.C. § 2511(2)(d).

134 *See infra* subparts III.A, B.

135 *In re Google Inc.*, 806 F.3d at 131–33.

136 *See id.*

137 Defendant Google Inc.'s Opening Brief in Support of Its Motion to Dismiss the Consolidated Amended Complaint at 16–17, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434 (D. Del. 2013) (No. 1:12-md-02358).

138 *See supra* subpart I.A. (outlining the Cookies Process).

139 Defendant Google Inc.'s Opening Brief in Support of Its Motion to Dismiss the Consolidated Amended Complaint, *supra* note 137, at 16–17.

directly to [Google]'s servers" and thus Google was "the intended recipient[ ] of the GET requests [it] acquired."[140]

The Third Circuit further rejected plaintiffs' argument that the party exception should not apply for equitable reasons.[141] Specifically, plaintiffs argued that Google was only able to collect users' information by surreptitiously circumventing their cookie blockers, and that while the users voluntarily sent the GET requests to Google, they were "induced to do so by deceit."[142] The Third Circuit, however, noted that the statutory language of the party exception did not expressly exclude "intended recipients [of a communication] who procured their entrance to a conversation through a fraud in the inducement, such as, here, by deceiving the plaintiffs' browsers into thinking the cookie-setting entity was a first-party website."[143] The Third Circuit also noted that Congress specifically referenced *United States v. Pasha* during its discussions concerning the party exception when it first drafted the Wiretap Act.[144] In *Pasha*, police officers conducted a legal search of the defendants' premises and impersonated the defendants when answering the defendants' telephone.[145] The Seventh Circuit held that the police officers did not intercept the communications despite the fact that some of the callers were misled into believing that they were speaking with the defendants.[146] The Seventh Circuit held that interception requires a third party to overhear a conversation through "surreptitious means"—a tampering with the "established means of communication"—and concluded that "impersonation of the intended receiver is not an interception."[147] As a result, the Third Circuit held that by referencing *Pasha*, Congress "strongly intimated that one who impersonates the intended receiver of a communication may still be a party to that communication for the purposes of the [Wiretap

---

140 *In re Google Inc.*, 806 F.3d at 142–43. Interestingly, neither the district court nor the Third Circuit appear to have addressed Google's argument concerning the Wiretap Act's consent exception. *See id.*; *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 443–44 (D. Del. 2013).

141 *See In re Google Inc.*, 806 F.3d at 143.

142 *See id.*

143 *See id.*

144 *See id.* at 144; United States v. Pasha, 332 F.2d 193 (7th Cir. 1964) (citing Clemons v. Waller, 82 F. App'x 436, 442 (6th Cir. 2003)).

145 *Pasha*, 332 F.2d at 198.

146 *See id.*

147 *See id.* Note that *Pasha* dealt with the Federal Communications Act of 1934, a predecessor to the Wiretap Act. *See* Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 32 (2003) (noting that the statutory regulation of wiretaps shifted from the Federal Communications Act to the Wiretap Act).

Act] and that such conduct is not proscribed by the statute," and thus held that Google's "impersonation" did not preclude it from qualifying under the party exception.[148]

B. The Ninth Circuit's Holding in *In re Facebook*

In *In re Facebook*, plaintiffs alleged that Facebook violated the Wiretap Act when it collected users' information via cookies.[149] In particular, Facebook indicated through its Data Use Policy and Help Center that "logged-out user data would not be collected, but then collected it anyway."[150] In response, Facebook argued that it did not violate the Wiretap Act because it qualified under the Act's party exception—users sent their information directly to Facebook and Facebook was consequently a party to those communications.[151] The Ninth Circuit, however, dismissed Facebook's argument.[152] Although the Ninth Circuit acknowledged that *In re Google* was analogous to the instant case,[153] and although Facebook essentially appealed to the same reasoning supporting the Third Circuit's holding, the Ninth Circuit declined to issue a similar ruling.[154] Instead, the Ninth Circuit noted that the First and Seventh Circuits had "implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to communications" under the Wiretap Act.[155] The Ninth Circuit further concluded that the Third Circuit's interpretation of the party exception contravenes the legislative intent behind the Wiretap Act: the Wiretap Act's purpose is to "prevent the acquisition of the contents of a message by an unauthorized third-party" and "permitting an entity [such as Facebook] 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."[156] As such, the Ninth Circuit

---

148 *In re Google Inc.*, 806 F.3d at 144.

149 956 F.3d 589, 596–97 (9th Cir. 2020).

150 *See id.* at 602.

151 Defendant Facebook, Inc.'s Reply in Support of Motion to Dismiss Plaintiffs' Second Amended Consolidated Class Action Complaint (Fed. R. Civ. P. 12(b)(1) & 12(b)(6)) at 8–9, *In re* Facebook Internet Tracking Litig., 290 F. Supp. 3d 916 (N.D. Cal. 2017) (No. 5:12-md-02314).

152 *In re Facebook, Inc.*, 956 F.3d at 607.

153 *See id.* at 608.

154 *See id.*

155 *See id.* at 607. The Ninth Circuit is referring to the First Circuit's holding in *In re Pharmatrak, Inc.* and the Seventh Circuit's holding in *United States v. Szymuszkiewicz*, discussed above in subpart II.A and section I.C.2, respectively.

156 *In re Facebook, Inc.*, 956 F.3d at 608.

held that Facebook was not a party to the intercepted communications within the meaning of the Act.[157]

IV
ANALYSIS

A. The "Surreptitious Tampering" Framework

In *In re Facebook*, the Ninth Circuit noted that both the First and Seventh Circuits have implicitly assumed that third-party cookies can be used to intercept communications.[158] Neither of the Circuits, however, have explicitly elaborated *how* cookies may be used to perform an interception.[159] Instead, both the First and Seventh Circuits restricted their analyses to the *temporal aspect* of the third-parties' acquisition of users' communications.[160] Consequently, their holdings do not establish a sufficient framework to determine whether Google and Facebook have intercepted users' communications in the instant cases. For example: if *A* sends a message to *B*, has *B* intercepted *A*'s message? The First and Seventh Circuits' holdings illustrate that *B* met the "contemporaneous" requirement for interception under the Wiretap Act—*B*'s acquisition of *A*'s message occurred contemporaneously with the transmission of *A*'s message—but the question remains unanswered. In essence, the "contemporaneous" requirement alone is insufficient to establish interception—courts must also consider *how* one acquires a user's communication to warrant a finding of interception.

Granted, the Wiretap Act uses broad language to define "intercept," suggesting that *any* acquisition of the contents of a communication can be interpreted as an interception.[161] Under this interpretation, *B* has indeed intercepted *A*'s message. While this conclusion is intuitively absurd (*A* voluntarily sent

---

157 *See id.*

158 *See id.* at 607 ("The First and Seventh Circuits have implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to communications within the meaning of the Act.").

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

160 *In re Pharmatrak, Inc.*, 329 F.3d at 21–22; *Szymuszkiewicz*, 622 F.3d at 705–06.

161 *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002) (noting that the Wiretap Act's definition of "intercept," standing alone, suggests that an individual "intercepts" an electronic communication merely by "acquiring" its contents, regardless of when or under what circumstances the acquisition occurs; however, "courts . . . have clarified that Congress intended a narrower definition of 'intercept' with regards to electronic communications"); 18 U.S.C. § 2510(4).

the message to *B*!), the First Circuit in *Szymuszkiewicz* took it one step further when it surmised, in dicta, that a person may intercept the content of their own conversation.[162] The First Circuit continued to note that the person would not violate the Wiretap Act because they were a party to their conversation.[163] There are two issues with the First Circuit's interpretation. First, it is hard to imagine that Congress contemplated that one could intercept the contents of one's own communication when it drafted the Wiretap Act.[164] Second, Congress likely intended the party exception to preclude third parties who intercepted a communication, but who also acquired the communication *legitimately* (e.g., by participating in the communication as a party), from violating the Wiretap Act—the party exception establishes a requirement of "but-for" causation between the defendant's interception of a communication and the defendant's acquisition of a communication for purposes of imposing liability under the Act.[165] Indeed, the First Circuit's interpretation of the party exception appears artificially manufactured to address the absurd case of one "intercepting" oneself. Thus, just as courts have read the "contemporaneous" requirement into the meaning of "intercept" under the Wiretap Act to bring the language closer in line with legislative intent, so should courts adopt the following framework.

This Note proposes that courts adopt a "surreptitious tampering" framework. Such a framework imposes a requirement (in addition to the "contemporaneous" requirement) for a finding of interception under the Wiretap Act. This additional requirement will henceforth be referred to as the "surreptitious tampering" requirement and is illustrated as follows: assume that a user has a reasonable expectation of how a mode of communication will operate.[166] A third party satisfies the "surreptitious tampering" requirement if they surreptitiously tamper with the mode of communication so that it no longer operates in the way the user expects. Such a requirement is

---

162 *Szymuszkiewicz*, 622 F.3d at 707.

163 *See id.*

164 *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 608 (9th Cir. 2020) ("[T]he Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an *unauthorized third-party* or '*an unseen auditor*.'" (emphasis added)).

165 *See* Roundy, *supra* note 44, at 434 ("The essential kernel of interception . . . is that the surveillance activity—the acquisition—occurs at the time of the communication and *thereby causes* the communication's contents to become known to the unauthorized person conducting the surveillance." (emphasis added)).

166 "User" is defined as either the sender or the receiver of a communication (or both).

based on the holding in *Pasha*, discussed above in subpart III.A, and is consistent with the existing case law concerning electronic communications.[167] For example, in *Szymuszkiewicz*, discussed above in section I.C.2, the supervisor reasonably expected her inbox not to forward incoming emails to third-party inboxes.[168] Consequently, the defendant surreptitiously tampered with his supervisor's mode of communication when he improperly accessed his supervisor's inbox to create a rule that caused the inbox to operate in a manner inconsistent with the supervisor's expectations.[169] The defendant in this case satisfies the "surreptitious tampering" requirement for interception (thus illustrating the consistency between the framework and the holding).

The "surreptitious tampering" framework also brings the language of the Wiretap Act closer in line with legislative intent. Applying the framework to the above example concerning *A* and *B*, *B* can no longer be found to have intercepted *A*'s message—*B* did not surreptitiously tamper with *A*'s mode of communication to cause the mode to operate in a manner inconsistent with *A*'s expectations. Furthermore, the framework precludes the First Circuit's understanding that one may "intercept" oneself—it is likely impossible for one to tamper with one's own mode of communication to cause it to no longer operate according to one's reasonable expectations.[170]

Lastly, it is important to consider the relationship between the "surreptitious tampering" framework and consent. As the First Circuit held in *In re Pharmatrak*, discussed above in subpart II.A, consent must be actual rather than constructive or "casually inferred."[171] Such a construction of consent necessarily entails knowledge of the act that the user is consenting to. As a result, under the "surreptitious tampering" framework, a user's consent to an act may influence the user's "reasonable expectations" of how a mode of communication will operate.

---

167 *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (holding that there was no interception because there was no "tampering with the established means of communication"); *see also* O'Brien v. O'Brien, 899 So. 2d 1133, 1137 (Fla. Dist. Ct. App. 2005) (holding that the wife intercepted her husband's electronic communications by surreptitiously installing a spyware program on her husband's computer).

168 United States v. Szymuszkiewicz, No. 07–CR–171, 2009 WL 1873657, at *2 (E.D. Wis. June 30, 2009), *aff'd*, 622 F.3d 701 (7th Cir. 2010).

169 *See id.*

170 A person would have knowledge of their own tampering, which necessarily influences their expectations concerning how the mode of communication will operate.

171 329 F.3d 9, 19–20 (1st Cir. 2003).

For example, recall the scenario involving *A* and *B* but with a slight modification: *A* sends a message to *B* but has now consented to *C*'s interception of *A*'s message. Because *A* consented to *C*'s interception, *A* now reasonably expects the mode of communication to operate in a manner that accounts for *C*'s interception. Nonetheless, *C* has still performed an interception under the "surreptitious tampering" framework because *C* has surreptitiously tampered with the mode of communication to operate in a manner inconsistent with *B*'s reasonable expectations (*B* did not consent to, nor know of, *C*'s interception).[172] According to the consent exception, *C* is not in violation of the Wiretap Act despite intercepting *A*'s message. Now consider the following scenario: both *A* and *B* have consented to *C*'s "interception" of *A*'s message to *B*. Under the "surreptitious tampering" framework, it is impossible for *C* to have intercepted *A*'s message—both *A* and *B* have knowledge of *C*'s act, and thus *C* cannot tamper with the mode of communication to cause it to operate in a manner inconsistent with either *A* or *B*'s reasonable expectations.[173] Note that the "surreptitious tampering" framework remains consistent with the language of the Wiretap Act. In particular, the consent exception stipulates that it is not unlawful for a person to *intercept* a communication if "*one of the parties* to the communication" has given prior consent to their interception.[174] Thus, as the consent exception recognizes, a third party still intercepts a communication even if one of the parties consents to their interception; moreover, the consent exception does not use the language "one *or all of the parties*," perhaps implicitly recognizing that a third party cannot perform an interception if *all* of the parties consent to the third party's tampering.[175]

---

172 Recall that "user," as used in the "surreptitious tampering" framework, means either the sender or the receiver (or both). *See supra* note 166 and accompanying text.

173 In other words, *C*'s tampering is no longer surreptitious.

174 18 U.S.C. § 2511(2)(d) (emphasis added).

175 Even if Congress did not intend to make such an implication, the "surreptitious tampering" framework remains consistent with the language of the consent exception. Note, however, that some state legislatures have passed telecommunications and wiretap statutes with all-party (or "two-party") consent exceptions. *See* Fla. Stat. Ann. § 934.03 (West) ("It is lawful . . . for a person to *intercept* a wire, oral, or electronic communication when *all of the parties* to the communication have given prior consent to such interception." (emphasis added)). While Congress's understanding of "intercept" vis-à-vis consent likely differs from that of the state legislatures in these cases, any future congressional amendment to include an all-party consent exception to the Wiretap Act could raise challenges to the "surreptitious tampering" framework.

B. Did Google and Facebook Intercept Users' Communications?

An analysis as to whether Google and Facebook intercepted users' communications is warranted before a discussion concerning the Third and Ninth Circuits' split on the Wiretap Act's party exception.[176] To warrant a finding that Google and Facebook intercepted users' communications, Google and Facebook must (1) acquire the contents of users' communications contemporaneously with the transmission of the communication and (2) surreptitiously tamper with the users' mode of communications. Ultimately, it is unclear whether Google and Facebook have actually intercepted users' communications.

1. *It is Unclear Whether Google and Facebook Satisfy the "Contemporaneous" Requirement*

As discussed above in section I.C.2, courts have imposed a "contemporaneous" requirement for an interception under the Wiretap Act, with the Seventh Circuit adopting a human timeframe approach and the Ninth Circuit adopting a machine timeframe approach. Whether Google and Facebook acquire users' communications contemporaneously with the transmission of the communication depends on (1) how one interprets the Cookies Process and (2) which timeframe—human or machine—applies.[177] The Cookies Process can be interpreted in two ways: either as a "single communication" that begins when the user requests to see a web page via a GET request and ends when the web page loads onto the user's screen, or as a "multipart exchange" in which each leg of the Cookies Process is treated as a distinct communication.

If the Cookies Process is interpreted as a single communication, then Google and Facebook satisfy the "contemporaneous" requirement on both a human and machine timeframe. As outlined in the Cookies Process, the user sends a GET request to the third-party website (such as Google or Facebook) in leg three, which necessarily occurs *after* the communication begins in leg one.[178] Furthermore, the entirety of a web page's

---

176 If Google and Facebook did not perform an interception under the Wiretap Act, then they have no need to assert a defense under the Wiretap Act's party exception.

177 Recall the Cookies Process discussed above in section I.A. Because the Cookies Process is the communication at issue in *In re Google* and *In re Facebook*, and because it is fundamentally the same in both cases, this analysis of the Cookies Process will apply to both cases.

178 If the user's browser does not send a GET request to the first-party website in leg one, it will not be instructed to send the second GET request to the third-

contents will not load (and thus leg four will not complete) until after the user sends the GET request to the third-party website.[179] Consequently, the user sends the GET request to the third-party website *before* the communication ends in leg four. As a result, the third-party website's acquisition of the user's GET request is contemporaneous with its transmission on a machine timeframe—the third-party website mechanically acquires the user's GET request after the communication begins but before the communication ends.[180]Furthermore, the third-party website's acquisitions is also contemporaneous on a human timeframe—it acquires a user's GET request "with no more than an eyeblink" after the first-party website receives the original GET request.[181]

On the other hand, if the Cookies Process is interpreted as a multi-part exchange, then Google and Facebook satisfy the "contemporaneous" requirement on a human, but not machine, timeframe. The "multi-part exchange" interpretation treats each of the four legs of the Cookies Process as a separate and distinct communication. As previously described, the user sends the GET request to the first-party website in leg one and the additional GET request to the third-party website in leg three. Because leg three necessarily begins after the *completion* of leg one,[182] the user's browser has already completed its transmission of the GET request to the first-party website before it sends the additional GET request to the third-party website. As a result, the third-party website's acquisition of the user's GET request is not contemporaneous with its transmission on a machine timeframe—there is no "stop, seiz[ure], or interrupt[ion] in [the] progress or course before [the] arrival [of

party website in leg three. *See Using HTTP Cookies*, MDN WEB DOCS: MOZ://A, https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies [https://perma.cc/68KR-XKDL] ("*After* receiving an HTTP request, a server can send one or more Set-Cookie headers with the response.") (emphasis added) (last visited Nov. 8, 2021).

179 The web page's contents include contents provided by the third-party website (e.g., advertisements) in response to the user's GET request in leg three.

180 Indeed, the plaintiffs in In re Facebook implicitly rely on this characterization of the Cookies Process in their brief: "Facebook actually receives . . . information [from its cookies] before the content of the user's request shows up on the user's screen." Plaintiffs' Opposition to Defendant's Motion to Dismiss Plaintiffs' Corrected First Amended Consolidated Class Action Complaint at 14–15, *In re* Facebook Internet Tracking Litig., 290 F. Supp. 3d 916 (N.D. Cal. 2017) (No. 5:12-md-02314) (emphasis added).

181 *Szymuszkiewicz*, 622 F.3d at 706.

182 *See Using HTTP Cookies*, *supra* note 184.

the user's GET request to the first-party website]."[183] However, because the third-party website acquires the contents of the user's GET request "with no more than an eyeblink" after the first-party website receives the original GET request, it again acquires the user's communication contemporaneously with its transmission on a human timeframe.[184]

The merits of either interpretation of the Cookies Process are outside of the scope of this Note and, as this Note will argue in Part V, should be considered and addressed by Congress. However, it may be worth noting that while no court has, at the time of this writing, appear to have addressed the interpretation of the Cookies Process as a single communication (i.e., a *conversation*),[185] one can reasonably argue that the Cookies Process should be analogized as separate conversations under the current framework. For example, in *Caro v. Weintraub*, the Second Circuit dismissed the appellant's argument that the appellee was not a party to the conversation and that "there were actually multiple conversations that occurred in the kitchen."[186] The court noted, among other things, that the appellee was physically present at the table during the conversation in the kitchen and "view[ed] the discussion in the kitchen as one conversation."[187] One can analogize the Cookies Process to the instant case: *A*, *B*, and *C* are sitting at a table and are verbally conversing with one another. *B* finds some-

---

183 Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002) (quoting WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 630 (1985)).

184 United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010). It is also worth noting that the instant cases involving cookies can be distinguished from *Szymuszkiewicz*. Unlike the transmission of emails, which the Seventh Circuit in *Szymuszkiewicz* believes is impossible to subject to a timing requirement, *see supra* note 95 and accompanying text, cookies operate in a strict time-sequence of events—it is *definitively* the case that the user's GET request is sent to, and received by, the first-party website *before* the user's browser sends an additional GET request to the third-party website. *See Using HTTP Cookies*, *supra* note 184. Consequently, the Seventh Circuit's human timeframe approach may be inapposite for cases involving cookies based on the court's expressed reasoning.

185 The Ninth Circuit in *In re Facebook* described the Cookies Process as creating, mechanically, a "*separate* but simultaneous, channel" between the user's browser and the third-party website, but the court did not rule on the issue of whether that channel should be considered as part of a greater conversation between the user and the first-party website (although it has implied that such a channel is indeed part of a greater conversation given its ruling in *Konop* regarding the "contemporaneous" requirement). *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596 (9th Cir. 2020).

186 Caro v. Weintraub, 618 F.3d 94, 97 (2d Cir. 2010).

187 *Id.* at 97–98, 98 n.5. Note, however, that it is not entirely clear whether the court relied on the physical location of the parties to the conversation when concluding that only a single conversation took place.

thing that *A* said interesting and asks for more details (i.e., a user requests a first-party website to see a web page); *A* shares more details (the first-party website sends some of the web page contents back to the user) and suggests that *B* call their mutual friend, *D* (who is *not* physically present at the table), for more information (the first-party website instructs the user's browser to send an additional GET request to a third-party website). *B*, while remaining at the table, calls *D* on the phone and begins chatting with *D* (the user's browser sends the additional GET request to a third-party website);[188] meanwhile, *A* and *C* continue conversing (the first-party website is still sending web page content to the user's browser during this time).[189] One can reasonably argue that there are two, separate conversations occurring simultaneously: *A*'s conversation with *B* and *C* at the table, and *B*'s conversation with *D* over the phone.[190]

2. *Google and Facebook Satisfy the "Surreptitious Tampering" Requirement*

Both Google and Facebook satisfy the "surreptitious tampering" requirement. In *In re Google*, Google publicly reassured users that their cookie blockers would prevent third-party websites from collecting their information via cookies.[191] Users who enabled a cookie blocker subsequently possessed a reasonable expectation that their communications with first-party websites were private from third-party websites. However, Google exploited a loophole in the cookie blockers so that it could continue to acquire the communications between users and first-party websites even when users employed a cookie blocker, and thus Google surreptitiously tampered with the mode of communication by causing it to operate in a manner inconsistent with users' reasonable expectations. Similarly, in *In re Facebook*, Facebook assured its users through its Data Use Policy and Help Center that it did not collect their information when they visited affiliated websites while they were logged

---

188 For the sake of simplicity, *B* in this analogy knows that they are communicating with the third-party *D* (a potential point of difference between this analogy and the case of third-party cookies).

189 Technically, a true analogy would require *A* to continue to verbally communicate to *B* while *B* is conversing with *D* on the phone. However, in this analogy, *A* continues to converse with *B* and *C* to make the analogy more (humanly) intuitive; ultimately the main point is that the original conversation among *A*, *B*, and *C* is still continuing.

190 The analogy is admittedly imperfect as online communications occur in cyberspace rather than in a physical setting.

191 *In re Google* is discussed above in subpart III.A.

out of Facebook.[192] Users subsequently possessed a reasonable expectation that their communications with first-party websites would not be privy to Facebook when they were logged out of Facebook. Thus, Facebook surreptitiously tampered with the mode of communication by causing it to operate in a manner inconsistent with users' reasonable expectations when it used its cookies to collect data from users who were logged out of their Facebook accounts.[193]

C. Google and Facebook Should Not Be Exempt Under the Wiretap Act's Party Exception

As mentioned above, the Wiretap Act's party exception states that a defendant does not violate the Wiretap Act if the defendant is a party to the intercepted communication.[194] In *In re Google*, the defendant online advertising companies argued that "[w]hen one person communicates something to another, the recipient is, in plain English, a party to that communication . . . regardless of what caused the communication or whether the sending party intended for the communication to happen."[195] Although the defendants' argument is linguistically correct, it nonetheless contravenes legislative intent. Google intercepts users' communications precisely because its code (hosted by first-party websites) instructs users to send a GET request to Google's servers. Allowing Google to then qualify under the party exception as a consequence of the technological underpinning of its interception allows Google to essentially "manufacture a statutory exception through its own accused conduct."[196]

---

192 *In re Facebook* is discussed above in subpart III.B.

193 Ironically, Facebook might not satisfy the "surreptitious tampering" requirement had it abstained from making any statement regarding its data collection practices. By explicitly and publicly informing users it would not collect their information when they were logged out of Facebook, Facebook established the "reasonable expectation" standard necessary to make the "surreptitious tampering" framework operate. As this Note will argue in Part V, it is unclear what users' "reasonable expectations" are when it comes to cookies practices without an accompanying user data policy by third-party websites.

194 18 U.S.C.§ 2511(2)(d). For the purposes of this discussion concerning the Wiretap Act's party exception, assume that Google and Facebook have met both the "contemporaneous" and "surreptitious tampering" requirements and have thus intercepted users' communications.

195 Brief of Defendants-Appellees Media Innovation Grp., LLC, WPP PLC, and Vibrant Media Inc. at 20, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125 (3d Cir. 2015) (No. 13-4300).

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

The Third Circuit characterizes Google's behavior differently, arguing that Google had "procured their entrance to [the] conversation through . . . fraud."[197] In particular, the Third Circuit analogized *In re Google* to *Pasha*, arguing that Google had impersonated the first-party websites.[198] However, the Third Circuit's analogy is erroneous—Google's misrepresentation relates to its cookies practices, not to its identity as a receiver of a communication. This distinction is fundamental. First, *Pasha*'s holding narrowly applies to misrepresentation in identity.[199] Second, Google's misrepresentation of its cookies practices is *part and parcel* of its interception—Google's use of its cookies would not have been an interception (under the "surreptitious tampering" framework) were it not for Google's misrepresentation concerning how its cookies operated vis-à-vis cookie blockers. In other words, Google's misrepresentation induced users to form reasonable expectations concerning its cookies, which Google then proceeded to violate, satisfying the "surreptitious tampering" requirement.

As the Ninth Circuit held in *In re Facebook*, permitting third parties such as Google and Facebook to qualify under the party exception in the instant cases would contravene legislative intent behind the Wiretap Act.[200] The First Circuit made a similar remark in *In re Pharmatrak*—in responding to Pharmatrak's argument that users visiting client websites thereby consented to Pharmatrak's interception, the First Circuit described Pharmatrak's argument as "frivolous . . . [because] [o]n that theory, every online communication would provide consent to interception by a third party."[201] While *In re Pharmatrak* involved the Wiretap Act's consent exception, the First Circuit's concern applies in this context as well: *every* online communication between users and affiliated websites would provide a means for third-party websites to escape liability under a strict construction of the party exception. Therefore, the Ninth Circuit's holding in *In re Facebook* should apply to Facebook, Google, and other analogous cases involving the collection of user information via third-party cookies—"simultaneous, unknown duplication and communication of GET re-

197 *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 143 (3d Cir. 2015).
198 *See id.* at 143–44.
199 United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964).
200 956 F.3d 589, 608 (9th Cir. 2020).
201 329 F.3d 9, 21 (1st Cir. 2003).

quests do not exempt a defendant from liability under the party exception."[202]

Furthermore, the "surreptitious tampering" framework also provides a basis for excluding third-party websites from qualifying under the party exception. Specifically, a third party may qualify under the Wiretap Act's party exception if, and only if, the third party intercepts a communication under the "surreptitious tampering" framework but also acquires the communication through a means that would not be considered an interception under the framework.[203] Consider the following case examples:

1. Unbeknownst to *A*, *B* created a rule to forward *A*'s incoming emails to *B*. *A* sends *B* an email. *B* has violated the "surreptitious tampering" framework, but has also acquired *A*'s email through a means that would not be considered an interception under the framework. *B* qualifies under the party exception.

2. *A* places its third-party cookies on *B*'s website and publishes a data policy stipulating that *A* will not collect information from users who visit *B*'s website with a cookie blocker enabled. *C* visits *B*'s website with a cookie blocker enabled, *B*'s website instructs *C*'s browser to communicate with *A*, and *A*'s cookies collect *C*'s information. *A* violated the "surreptitious tampering" framework and has not acquired *C*'s communication through any other means that would not be considered an interception under the framework. Although *A* is linguistically a "party" to *C*'s communication, *A* will not qualify under the party exception.

3. *A* is conversing with *B* and accidentally and unknowingly "pocket dials" *C*. *C*, by answering *A*'s phone, intends to acquire *A*'s communications. *C* does not know *A*'s phone call was by accident and hears *A* communicate with *B*. There is no interception because *A*'s phone behaved as one would reasonably expect.[204]

---

202 *In re Facebook, Inc.*, 956 F.3d at 608."

203 This argument is based on the "but-for" causation element regarding the Wiretap Act's party exception. *See supra* note 165 and accompanying text.

204 A recently published Note provides an alternative approach to interpreting the Wiretap Act's party exception. 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 (2021). In the Note, the author argues that third-party websites should not be considered parties to users' communications because they are neither "intended recipients" nor "intended destinations" of the communications in question. *Id.* at 988-89. While generally compelling, the author's framework faces two potential issues. First, it is a matter of interpretation

The second case example illustrates that the "surreptitious tampering" framework provides a basis for precluding third-party websites, such as Google and Facebook, from qualifying under the Wiretap Act's party exception.[205]

V
LIMITATIONS OF THE "SURREPTITIOUS TAMPERING" FRAMEWORK AND THE NEED FOR CONGRESSIONAL LEGISLATION

Although the "surreptitious tampering" framework brings the statutory language under the Wiretap Act closer in line with legislative intent, it also faces limitations. In particular, it requires a determination of a user's "reasonable expectation" of how a mode of communication operates. This requirement is problematic in cases of third-party cookies where third-party websites have not publicly informed users how their cookies will operate.[206] In these cases, it is not clear what a user's "reasonable expectation" is with regard to a particular website's cookies practices. One might argue that because cookies are

---

as to whether the third-party websites are "unintended destinations." After all, the users' browsers (acting on behalf of users) intend to send the subsequent GET requests to the particular third-party website addresses. Second, the author's framework bars the (arguably desirable) application of the party exception to third case example. Under the author's framework (which maintains the current statutory framework of the meaning of "intercept"), *C* intercepted *A*'s communications with *B*. Furthermore, under the author's framework, *C* can no longer appeal to the party exception to avoid liability under the Wiretap Act because *C* is neither an intended recipient nor an intended destination to *A*'s communication. Such an outcome is problematic, especially given that *C* does not know that *A*'s call was unintentional until after *C* has already intercepted *A*'s communications.

205 While this Note focuses on the circuit split concerning the application of the Wiretap Act's party exception, it is worth mentioning that Google and Facebook are unlikely able to appeal to the Act's consent exception in the instant cases. Because both Google and Facebook made representations as to how their cookies operated, it is arguable that affiliated websites agreed to host their code to the extent the websites believed the code would behave in accordance to their representations. *In re Pharmatrak*, 329 F.3d at 19–20 (holding that consent must be actual rather than constructive or "casually inferred").

206 A 2012 survey of the most-visited websites in the United States found that 31.14% of the websites failed to disclose whether third-party cookies were allowed. Note, however, that this survey was conducted prior to the implementation of the European Union's General Data Protection Regulation in 2018. *See* Dennys Marcelo Antonialli, Note, *Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes*, 8 STAN. J. C.R. & C.L. 323, 343 (2012). *See also* David A. Zetoony, *What Percentage of Websites Have a Cookie Banner?*, GREENBERGTRAURIG (Nov. 30, 2020), https://www.gtlaw-dataprivacydish.com/2020/11/what-percentage-of-websites-have-a-cookie-banner/ [https://perma.cc/J9KS-PTRU] ("Based upon a review of the websites of the companies listed in the Fortune 500, approximately [only] 35% of websites utilize some form of a cookie banner.").

almost ubiquitous in our lives,[207] one should (by default) reasonably expect websites to operate with third-party cookies.[208] However, this expectation develops from a user's subjective experience and their repeated interactions with the Internet rather than an objective source, such as a statute or a website's user data policy. An objective source is preferable given that there might be users who sparsely interact with the Internet and are thus insufficiently exposed to the ubiquity of third-party cookies to reasonably expect, by default, that every website they visit might host such cookies.

Congressional legislation is needed to spur the development of default rules—either by directly establishing the default rules or by requiring websites to publish user data policies—so that both courts and users have a reference with regard to how one should "reasonably expect" Internet communications, such as cookies, will operate.[209] For example, Con-

---

207 Fowler, *supra* note 9 (finding that out of the 80,000 most-popular domains on the Web, "[o]nly 13 percent of sites didn't load any ad trackers or third-party cookies").

208 James Grimmelmann, *Spyware vs. Spyware: Software Conflicts and User Autonomy*, 16 OHIO ST. TECH. L. J. 25, 60 (2020).

209 It may be preferable for Congress to establish and apply a standardized rule to all third-party cookie policies as it would eliminate the need for users to familiarize themselves with each individual website's cookie policy. *See* Bianca Ferrari, *'It's Bad Design On Purpose' – Why Website Cookie Banners Look Like That*, VICE (Aug. 4, 2021, 4:15 AM), https://www.vice.com/en/article/m7epda/its-bad-design-on-purpose-why-website-cookie-banners-look-like-that [https://perma.cc/9J2R-8LCJ] (noting that some cookie consent banners took the author more than five minutes to read; and that research indicates that "people spend on average less than a minute on a website" and "might find the prospect of just a couple of seconds of clicking and reading through a pop-up enough of a burden to just select the 'accept all' option and get it over with"). A standardized approach may be feasible given that all third-party cookies largely operate the same way. Matt Burgess, *We Need to Fix GDPR's Biggest Failure: Broken Cookie Notices*, WIRED (May 28, 2020, 6:00 AM), https://www.wired.co.uk/article/gdpr-cookie-consent-eprivacy [https://perma.cc/X94H-46AZ] ("Cookie notices come in all shapes and sizes – however, *they largely work in the same way*." (emphasis added)). While websites will have to tailor their cookie policies to describe the particular information they are collecting from users, a standardized rule may simplify the process in which users digest each policy (e.g., by requiring standard disclosures and clear and concise formatting). For example, Facebook released a notification feature that clearly and concisely alerts users which third-party apps are collecting what information. Puxuan Qi, *New Facebook Login Feature With Added Controls*, FACEBOOK FOR DEVELOPERS (Jan. 14, 2020), https://developers.facebook.com/blog/post/2020/01/14/new-facebook-login-feature-with-added-controls/ [https://perma.cc/9THS-KU8N] (providing a sample alert that clearly displays the third-party app name, date and time accessed, and user information (such as profile photo, email address, birthday, Friends list, and Page likes) collected). *See also* Dobkin, *supra* note 10, at 47 n.168 (arguing that Congress should establish a federal regime concerning data privacy because (1) many service providers serve consumers in all fifty states and (2) a federal regime would be more predictable than state-equivalents for users and service providers alike).

gress can choose to directly create default rules by passing legislation resembling the European Union's General Data Protection Regulation (GDPR),[210] which includes a "cookie directive" that requires websites to show a pop-up asking users for consent to use cookies.[211] Such legislation might also mimic the recently adopted California Consumer Privacy Act (CCPA), which requires businesses to provide notice to users as to the kinds of information that they collect.[212] Or Congress can simply create a default rule under which users should reasonably expect the websites they visit to use third-party cookies to collect certain information from them (such as the web pages they visit) *until* the users learn otherwise (e.g., by reading the website's user data policy) *or unless* they have enabled a cookie blocker. Alternatively, Congress can indirectly create default rules by requiring websites themselves to establish the particular privacy policies (although Congress might perhaps choose

---

Note Congress has created "default rules" for other, more traditional methods of communications, such as telecommunications. *See Customer Privacy*, FED. COMM. COMMISSION, https://www.fcc.gov/general/customer-privacy [https://perma.cc/Y2FJ-DZLQ] (last visited Jan. 6, 2021) (stating that the Federal Communications Act "require[s] telecommunications carriers . . . to protect 'customer proprietary network information,' or CPNI. CPNI includes some of the most sensitive personal information that carriers and providers have about their customers as a result of their business relationship (*e.g.*, phone numbers called; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting). To protect consumer privacy, the Commission's rules require carriers/providers to file reports, annually, to certify their compliance with the CPNI rules.").

210 The GDPR requires websites to give "clear, concise, and non-disruptive notice and to receive affirmative and unambiguous consent from an internet user before collecting 'personal data' about the internet user." De Zayas, *supra* note 35, at 2218 n.46. Under the GDPR, "personal data" includes "any information about an identifiable natural person who may be directly or indirectly identified by an identification number or online identifier," such as cookie identifiers. *Id.* The GDPR has been followed by "significant reductions in the volume of third-party cookies set without consent on many European news sites." TIMOTHY LIBERT, LUCAS GRAVES, & RASMUS KLEIS NIELSEN, CHANGES IN THIRD-PARTY CONTENT ON EUROPEAN NEWS WEBSITES AFTER GDPR, (2018), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf [https://perma.cc/RFK2-SQX2].

211 Grimmelmann, *supra* note 208, at 60 (2020).

212 *See* Cal. Civ. Code § 1798.100(b) (2021). Both the GDPR and the CCPA also require businesses to delete users' personal information upon request. *See Art. 17 GDPR: Right to Erasure ('Right to be Forgotten')*, GDPR.EU, https://gdpr.eu/article-17-right-to-be-forgotten/ [https://perma.cc/6L9H-RV9L] (last visited Nov. 8, 2021); Cal. Civ. Code § 1798.105(a). Users outside the jurisdiction of the GDPR and CCPA normally cannot request businesses to delete their personal information collected via cookies. *See* VOX, *How Ads Follow You Around the Internet*, YOUTUBE (Feb. 3, 2020), https://youtu.be/HFyaW50GFOs?t=264 [https://perma.cc/9MQK-9BD5] (noting that once a third-party website uses cookies to collect personal information, "there's no getting it back").

to establish baseline privacy protections to prevent third-party websites from self-imposing excessively lenient default rules).[213] Ultimately, it is less important which approach Congress takes as long as Congress establishes an objective reference regarding a user's "reasonable expectation."[214]

Furthermore, the "surreptitious tampering" framework is also limited in that it does not provide a resolution to the debate concerning whether courts should interpret the Cookies Process as a single communication or as a multi-part exchange. As explained above, third-party websites escape liability under the Wiretap Act if courts (1) apply the "contemporaneous" requirement on a machine, rather than human, timeframe and (2) interpret the Cookies Process as a multi-part exchange rather than a single communication. The merits of either interpretation of the Cookies Process are outside the scope of this Note; this Note merely argues that Congress must weigh in on the debate by establishing clear

---

213 Although some websites have established privacy policies, they are currently not legally required to do so. *See* Dobkin, *supra* note 10, at 9 ("At present, the only protection users have is the privacy policies that service providers design and implement themselves, and there is no baseline protection to fall back on if they withdraw or weaken these policies."). If Congress chooses to require websites to publish user data policies, websites must explicitly notify users how it will acquire and use their data. *See In re* Google Inc., 13-MD-02430-LHK, 2013 WL 5423918, at *13 (N.D. Cal. Sept. 26, 2013) (holding that users did not consent to Google's interceptions when they agreed to Google's Terms of Service and Privacy Policies because "th[e] policies did not *explicitly* notify [users] that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising" (emphasis added)). Congress should also prohibit websites from using cookies *until* users are able to view the relevant user data policy and affirmatively demonstrate consent. *See* Antonialli, *supra* note 206, at 349–50 (raising the concern that some websites have attributed user consent to the visitation of the website and thus "by entering a website to read its privacy policy, before even reading it, you are already being tracked and considered to have given 'consent'"). Furthermore, any self-imposed regulation must ensure that users are provided with a reasonable and non-burdensome means of demonstrating consent. *See supra* note 207; *but see* Jacob Leon Kröger, Otto Hans-Martin Lutz & Stefan Ullrich, The Myth of Individual Control: Mapping the Limitations of Privacy Self-management (July 15, 2021) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776 [https://perma.cc/8WCB-3Q62] (arguing that the concept of privacy self-management is fundamentally flawed and cannot be fixed by "making it more user-friendly or efficient" because "people's privacy choices are typically irrational, involuntary and/or circumventable due to human limitations, corporate tricks, legal loopholes and the complexities of modern data processing").

214 Note that the default rules provide an objective reference as to a user's "reasonable expectations," even if the user is not subjectively aware of such rules. The existence of default rules has provided an opportunity for users to reasonably learn how their modes of communication will operate, and thus the burden is now on users to learn more about the technology they are using.

legislative guidelines as to how courts are to evaluate the Cookies Process under the Wiretap Act.

CONCLUSION

The Wiretap Act is currently inadequate to address contemporary Internet communications including the Cookies Process. While this Note suggests that courts adopt an additional "surreptitious tampering" framework to clarify Congress's intent behind the meaning of "intercept" under the Wiretap Act, the framework is insufficient to determine whether third-party websites, such as Google and Facebook, are able to use cookies as a method of interception. Congressional legislation is needed to resolve competing interpretations of the Cookies Process in order to determine whether such websites have actually intercepted users' communications.[215] With regard to the circuit split between the Third and Ninth Circuits' holdings in *In re Google* and *In re Facebook*, respectively, courts should recognize the Ninth Circuit's holding as authoritative: First, adopting a strict construction of the Wiretap Act's party exception to permit third-party websites to qualify under the exception would allow them to "manufacture a statutory exception

---

215 It is worth noting that Google intends to phase out cookies from its Chrome browser in 2023. Vinay Goel, *An Updated Timeline for Privacy Sandbox Milestones*, GOOGLE: THE KEYWORD (June 24, 2021), https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/ [https://perma.cc/5JA6-Y2CJ]. Because Google Chrome controls two-thirds of the global browser market, and because other browsers such as Safari and Firefox already block third-party cookies by default, some have theorized that Google's plan to phase out third-party cookies will render the practice of third-party cookie tracking "effectively extinct." Nicolás Rivero, *The Digital Ad Industry Is Rewriting the Bargain at the Center of the Internet*, QUARTZ (Apr. 25, 2021), https://qz.com/2000490/the-death-of-third-party-cookies-will-reshape-digital-advertising/ [https://perma.cc/KH5T-PQFZ]. Nonetheless, Internet tracking is here to stay. *See id.* ("There are three major proposals for how the industry can continue to show consumers relevant ads and measure the effectiveness of marketing campaigns without relying on third-party cookies. Google is championing a browser-based tracking model; publishers and brands are developing ad models that rely on their own first-party data; and some parts of the adtech industry are pushing for a new form of identity-based tracking that would bear some similarities to the cookies of yore."). *See also* Sara Morrison, *Google Is Done With Cookies, but That Doesn't Mean It's Done Tracking You*, VOX (Mar. 3, 2021, 5:50 PM), https://www.vox.com/recode/2021/3/3/22311460/google-cookie-ban-search-ads-tracking [https://perma.cc/HM6U-CZ8N] ("Google announced . . . that third-party cookies are over — at least, as far as its ad networks and Chrome browser are concerned . . . [but] [i]t doesn't mean that Google will stop collecting your data, and it doesn't mean the company will stop using your data to target ads."). Consequently, this Note hopes to continue to provide clarity on the application of the Wiretap Act in the context of online communications as third-party websites develop new methods of Internet-based tracking.

through [their] own accused conduct."[216] Such a holding is, as the Ninth Circuit held, a clear contravention of Congress's intent to protect the privacy of electronic communications.[217] Second, the "surreptitious tampering" framework provides a basis for precluding third-party websites, such as Google and Facebook, from qualifying under the party exception.

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

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