Washington and Lee Journal of Civil Rights and Social Justice

Volume 29 | Issue 1 Article 7

Fall 2022

Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online

Hayden Driscoll
Washington and Lee University School of Law, driscoll.h22@law.wlu.edu

Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online

Hayden Driscoll*

Abstract

The federal Wiretap Act—originally enacted to curtail the government's unbridled use of wiretaps to monitor telephonic communications—was amended in 1986 to provide a private right of action, extending the Act's Fourth Amendment-like protections to private intrusions. Since the advent of the internet, plaintiffs have attempted to predicate claims of unauthorized online privacy intrusions on the Wiretap Act. In response, defendants claim they are parties to the communications at issue and should be absolved of liability under the Act's party exception. The federal circuit courts of appeal disagree on how the party exception applies in the internet context. This Note evaluates the courts' differing conclusions and rationales and proposes two solutions, both of which share the common thread of applying heightened notice and consent requirements to online communications.

Table of Contents

[*] J.D. Candidate, May 2022, Washington & Lee University School of Law. First and foremost, I would like to express my gratitude for my primary support system: my wife, Kassidy, and my son, Asher. Their love and support provided me with a necessary foundation throughout the process of writing this Note. I would also like to thank my faculty advisor, Professor Joshua Fairfield, for his guidance and technological expertise. Finally, I want to thank my note editor, Shad Brown, for his encouragement and constructive feedback.

I. Introduction

"There are few things as revealing as a person's search history,"[1] and yet, Google collects this information on over 3.5 billion searches each day.[2] And Google isn't the only one privy to this information.[3]

After catching up on his Facebook news feed, John logged out of his account and began performing some searches on Google. John had been having internal struggles recently and was concerned about his mental health, so he began searching for options using search terms, such as "therapists near me." John spent hours visiting different therapists' websites and reading articles on mental health, using even more specific search terms to try and figure out what was going on with him.

The next day, John came across a blog post by Nik Cubrilovic, which detailed Facebook's tracking practices and revealed that even when Facebook users were logged out, Facebook continued tracking its users across the internet, collecting—among other things—the URLs users visited.

John became concerned that the research he had done the previous day was not private. Would others know John had searched for help with his mental health? Upon further investigation, John learned that URLs contain search terms, allowing Facebook to see exactly what John had searched for. This wasn't the worst part. John also learned that Facebook didn't keep this data to itself; it sold the data to others. John was thoroughly disgruntled and felt that his privacy had been violated. He wanted to hold Facebook responsible and stop it from sharing this sensitive information with others. But he wasn't sure how to do this.[4]

[1] Alfred Ng, *Google is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020, 1:21 PM) [https://perma.cc/7Z8K-DLNY] .

[2] *See* Maryam Mohison, *10 Google Search Statistics You Need to Know in 2021*, OBERLO (Apr. 3, 2020) (explaining that Google statics understand user behavior) [https://perma.cc/AV6W-XWWG].

[3] *See* Part III (describing how cookies are used to collect data from users across the internet).

[4] This narrative is based loosely on the facts of *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), with some creative liberties taken to illustrate the problem in a more relatable way.

Internet companies want to be parties to all our communications. It is no secret today that companies like Facebook and Google are invisible, silent observers of our daily interactions, listening to every conversation, observing our daily routines, and then tracking these behaviors and selling the information to others.[5] What is not as well known, however, is the little to no recourse internet users have when these companies go too far.[6]

Some internet users have resorted to filing suit against tech companies under the Electronic Communications Privacy Act of 1986,[7] i.e., the federal Wiretap Act, claiming that the companies are guilty of wiretapping when they "intercept"[8] information in electronic communications submitted by internet users online and then use that information to profit via targeted advertising.[9]

In response, tech companies claim they are parties to the online communications because if they are considered parties, they are exempted from liability per the Wiretap Act's party exception.[10] Federal circuit courts of appeal disagree on what

[5] *See* Dennis Anon, *How Cookies Track You Around the Web and How to Stop Them*, PRIVACY.NET (Feb. 24, 2018) (explaining how cookies track internet users across the web) [https://perma.cc/UTZ2-ZY28]; *see also* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019) ("A majority of Americans believe their online and offline activities are being tracked and monitored by companies and the government with some regularity.") [https://perma.cc/J3SQ-7MBB].

[6] *See* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018) ("As the data universe keeps expanding, more and more of it falls outside the various specific laws on the books.") [https://perma.cc/UP89-9ABZ].

[7] 18 U.S.C. §§ 2510–2522 (2018).

[8] *See* 18 U.S.C. § 2511(1)(a) (2018) (providing criminal and civil sanctions for "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept, any wire, oral, or electronic communication"); *see also id.* §§ 2511(4)–(5) (describing civil and criminal liability for a violation of subsection [1]).

[9] *See, e.g.*, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596–97 (9th Cir. 2020) (setting out the background of the plaintiffs' claim that Facebook had violated, among other laws, the Wiretap Act when it continued tracking Facebook users after they had logged out of their Facebook accounts).

[10] 18 U.S.C. § 2511(2)(d) (2018); *see also, e.g.*, *id.* at 607–08 (considering whether Facebook was exempted from liability under the Wiretap Act as a "party" to the communications at issue).

constitutes a "party" within the meaning of the Act.[11] This means that if John chooses to sue Facebook under the Wiretap Act in the Ninth Circuit, he has a shot at winning. On the other hand, if he sues in the Third Circuit, he will likely lose.

This Note proposes solutions to the circuit split and explains why tech companies that surreptitiously duplicate and forward internet users' online communications without their knowledge or consent violate the Wiretap Act, as the Act's overall objective of protecting the privacy of communications is still relevant even though the Act was not drafted with the online context in mind.

Part II discusses the history of the Wiretap Act and provides the relevant language of the Act's party exception.

Part III introduces cookies as the technological backdrop for the discussion on the party exception. That Part then discusses the invention of the cookie and how the technology has evolved since and become problematic in the data privacy context, particularly with regard to third-party cookies and tracking. Next, that Part provides a detailed explanation on how cookies function to track users across the internet. And finally, that Part discusses how tech companies have been able to circumvent private attempts at protecting internet users' data, illustrating the need for an effective legal recourse.

Part IV summarizes four cases relevant to the issue and presents the circuit split that serves as the crux of this Note.

Finally, Part V proposes solutions to the principal issue that has divided federal appeals courts—the lack of a definition of "party" in the Wiretap Act. That Part first advocates for a heightened knowledge-and-consent standard to replace the notice-and-consent standard prevalent in privacy law. It then lays out two proposed solutions: (1) Congress should amend the Wiretap Act and provide a definition for "party"; or (2) the Supreme Court should provide lower courts with an interpretation of "party" that can be applied in the internet context.

[11] *See In re Facebook*, 956 F.3d at 607–608 (describing the different interpretations of the term "party" among the federal circuit courts of appeal).

II. The Wiretap Act

A. History of the Wiretap Act

The Wiretap Act proscribes the unauthorized interception and disclosure of wire, oral, and electronic communications.[12] The original version of the Wiretap Act—the Communications Act—was enacted in 1934 as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications.[13] Originally, the Act was primarily concerned with regulating the government's use of wiretaps,[14] which directly reflects Fourth Amendment law, as the Fourth Amendment only protects citizens against unlawful *governmental* intrusions.[15] Significantly, through the Electronic Communications Privacy Act ("ECPA") of 1986, Congress amended the Wiretap Act to provide a private right of action, extending the statute's Fourth Amendment-like protections to private intrusions as well.[16]

One of the major concerns Congress expressed in the 1986 amendment to the Wiretap Act was that the legislation was not

[12] *See* 18 U.S.C. § 2511 (2018) (describing the elements: unauthorized interception, disclosure, and use of wire, oral, or electronic communications.).

[13] *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 378–79 (2014) (explaining the Wiretap's history and the concerns that prompted the enactment of its predecessor statute); *see also* S. REP. NO. 99-541, at 1–2 (1986) (explaining that the Wiretap Act was enacted in the first place as a way of extending Fourth Amendment protections).

[14] *See* Kerr, *supra* note 13, at 379 ("Unlike the Communications Act, however, the Wiretap Act includes a carefully crafted privacy regime regulating lawful interceptions.").

[15] *Fourth Amendment*, LEGAL INFO. INST. ("[T]he Fourth Amendment does not guarantee protection from all searches and seizures, but only those done by the government and deemed unreasonable under law.") [https://perma.cc/2Z7X-YQKM].

[16] *See In re* Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) ("The post-ECPA Wiretap Act provides a private right of action . . . ."); *see also In re* 381 Search Warrants Directed to Facebook, Inc., 132 A.d.3d 11, 20 (N.Y. App. Div. 2015) (interpreting the SCA, which, like the Wiretap Act, is part of the ECPA, as "narrowly tailored to provide a set of Fourth Amendment-like protections for computer communications").

keeping up with the technological advancements of the time.[17] At that time, the technological advancements that prompted the amendment to the legislation were "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing."[18]

Since 1986, technology, specifically within the telecommunications industry, has continued to advance rapidly.[19] From 2000 to 2010 alone, many landmark advancements were made, including 2G, 2.5G, and 3G mobile networks, the advent of WiFi networks, and smartphones, among others.[20] Since 2010, advancements have included the invention of the Cloud, the telecom industry's use of the Internet of Things for connectivity, and Artificial Intelligence.[21] Technology has been developing at exponential rates, while legislation has failed to keep up.[22] The Wiretap Act has not been legislatively amended in any meaningful way to account for technological advancements since 1986, which is extremely problematic, as courts have attempted to apply the outdated statute to new technologies.[23] This has inevitably created

[17] *See* S. REP. NO. 99-541, at 2 (1986) ("[The existing law] has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry.").

[18] *See id* (describing the technological developments that moved the amendment forward).

[19] *See* Jim Machi, *Top 10 Telecom Advancements of the Past 10 Years*, DIALOGIC (Dec. 14, 2010, 11:29 AM) (listing 10 technological advancements within the telecommunications industry from 2000 to 2010) [https://perma.cc/LZ3L-K8L8?type=image].

[20] *See id.* (listing the technologies that have transformed the telecom sector).

[21] *See* Bernard Marr, *The 7 Biggest Technology Trends that Will Transform Telecoms in 2020*, FORBES (Oct. 14, 2019, 12:27 AM) (discussing some of the largest technological advancements and trends within the telecommunications industry leading up to 2020) [https://perma.cc/25AZ-9M23].

[22] *See* Manav Tanneeru, *Can the Law Keep up with Technology?*, CNN (Nov. 17, 2009) ("Legal experts said it's difficult for the law to keep up with emerging technology.")[https://perma.cc/PAN9-HU6Z]; *see also* Marci Harris, *Here's What Happens When Tech Outpaces Government*, APOLITICAL (Sept. 12, 2019) (explaining that the exponential pace of technological development creates a "pacing problem" when paired with the lagging pace of policy change) [https://perma.cc/4CYX-FFSH].

[23] *See* Kerr, *supra* note 13, at 385–86 (explaining two subsequent amendments to the 1986 amendment of the Act that had little effect on its basic structure).

legal confusion, specifically in the context of online communications.[24]

B. The Party Exception

The Wiretap Act excepts from liability anyone considered "a party to the communication."[25] The problem arising from this exception is the Act's failure to define "party," which has resulted in differing interpretations from the federal circuit courts.[26] As the following Part will illustrate, this lack of uniformity among the federal circuit courts becomes a major issue in the internet context where internet companies like Facebook and Google are constantly working to circumvent efforts to protect internet users' privacy.

III. The Technological Landscape

Although there are multiple methods used to gather internet users' information, this Note will focus on the most well-known and commonly used method employed by internet companies today: cookies.[27] The use of cookies serves here to illustrate the problems that arise with differing interpretations of "party" within the meaning of the Wiretap Act. However, the problems identified, and the solutions proposed in this Note, are applicable broadly, and the use of cookies as an example is not to be construed as a constriction on the applicability of the proposed solutions.

[24] *See* Orin Kerr, *Websurfing and the Wiretap Act*, WASH. POST (June 4, 2015) ("Applying the Wiretap Act to the Internet can be tricky because the Internet enables person-to-computer communications.") [https://perma.cc/VJT4-7YKK].

[25] *See* 18 U.S.C. § 2511(2)(d) (2018) (describing the permissibility of a person not acting under the color of the law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception).

[26] *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (2020) ("The Wiretap Act does not define the term 'party' in its liability exemption, and the other circuit courts that have considered the Act's scope have interpreted the term in different ways.").

[27] *See What Is Online Tracking and How Do Websites Track You?*, KOOFR BLOG (identifying the different ways users are tracked across the internet and identifying cookies as the most well-known and commonly used method) [https://perma.cc/44T6-74JC].

A. The Evolution of Cookies

1. The Invention of the Cookie

In 1994, Lou Montulli invented the cookie.[28] His purpose in creating the technology was to give the internet memory.[29] Before the invention of the cookie, Montulli says surfing the web was a lot like having a conversation with the character Dory from Disney's *Finding Nemo*,[30] who suffers from short-term memory loss.[31] "Cookies are small text files stored on your devices" that provide websites with information to help them identify you as the same person and ultimately improve users' browsing experience.[32] Without cookies, anytime a user added something to a virtual cart and clicked away, that item would disappear; and each time a user loaded a new page on Facebook, he or she would have to log in again.[33] Therefore, cookies are desirable and help the internet function properly.[34]

2. First- and Third-Party Cookies

The original cookie invented by Montulli is now referred to as a "first-party cookie."[35] First-party cookies are created by the owners of the websites users visit and "allow website owners to

[28] Cleo Abram, *How Ads Follow You Around the Internet*, VOX (Feb. 3, 2020, 10:30 AM) [https://perma.cc/5WXJ-EYWM].

[29] *See id.* (explaining the purpose of the cookie).

[30] FINDING NEMO (Disney 2003).

[31] Abram, *supra* note 28; *see also* Vicki Arkoff, *The Ultimate Guide to 'Finding Nemo'*, HOWSTUFFWORKS, (describing Dory as the character who introduces herself by saying "I suffer from short-term memory loss. It runs in my family . . . at least I think it does . . . where are they?") [https://perma.cc/22TA-CURR].

[32] *See What Is Online Tracking and How Do Websites Track You?*, KOOFR BLOG [hereinafter *What Is Online Tracking*] (laying out the different ways users are tracked across the internet and identifying cookies as the most well-known and commonly used method) [https://perma.cc/44T6-74JC].

[33] *See* Abram, *supra* note 28 (explaining how cookies work).

[34] *See id.* (explaining how cookies can be useful to the user).

[35] *See id.* (distinguishing between first- and third-party cookies and identifying first-party cookies as the original cookies invented by Montulli).

collect analytics data, remember language settings, and perform other useful functions that provide a good user experience."[36] However, Montulli did not anticipate how his creation would evolve.[37] In addition to the basic functions that help the internet work properly, cookies can be used to track users across the internet and store their browsing histories over long periods of time.[38] This is the problematic function of third-party cookies.[39]

Third-party cookies, as is evident from their name, are created by entities other than the owners of a particular website.[40] One example of this is the Facebook "like" button or "share" option users frequently encounter on different websites they visit.[41] This allows Facebook (the third party) to access the same information website owners collect through first-party cookies.[42] Facebook then uses that data to create user profiles and send users advertisements based on their online behavior.[43] The use of third-party cookies by companies like Facebook becomes particularly

[36] *See What's the Difference Between First and Third-Party Cookies?*, COOKIEPRO (last updated Sept. 3, 2021) [hereinafter *What's the Difference*] (defining first-party cookies as one "set by the publisher's web server or any JavaScript loaded on the website") [perma.cc/4VRD-QG8Y].

[37] *See* John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES (Sept. 1, 2001) (explaining how cookies began as a harmless way to give the internet memory but evolved into a mechanism for potentially impinging users' privacy on the internet) [perma.cc/H6VS-QK3E].

[38] *See What Is Online Tracking, supra* note 32 (explaining the different ways websites track their users, including through the use of third-party cookies).

[39] *See id.* ("The problematic cookies are the third-party cookies or tracking cookies that store your browsing history over a long period of time and across many pages.").

[40] *See What's the Difference*, *supra* note 36 (defining third-party cookies).

[41] *See* Paris Martineau, *Facebook is Tracking You on Over 8.4 Million Websites*, THE FUTURE (May 18, 2018, 1:37 PM) (quoting Facebook's Head of Public Policy as referencing the Facebook Like button and Share button as two ways Facebook tracks data) [perma.cc/N3ME-3ZS2].

[42] *See What's the Difference*, *supra* note 36 (explaining that first-party cookies are accessible "to the domain that created [them]," while third-party cookies are accessible "on any website that loads the third-party server's code").

[43] *See* Martineau, *supra* note 41 (explaining how Facebook tracks its users and what it does with that tracking data).

disquieting upon learning that the number of websites that allow Facebook to track users surpasses eight million.[44]

B. How Cookies Function

To understand the potentially dangerous effects of the irresponsible use of cookies and how the Wiretap Act's party exception plays in, it is necessary to understand how cookies function. Cookies are small text files placed on your device or browser anytime you visit a website.[45] While these cookies collect multiple pieces of data from users' interaction with websites,[46] the piece of information of focus in internet litigation involving the use of cookies is the Universal Resource Locator ("URL").[47] "URLs both identify an internet resource and describe its location or address."[48] URLs also provide other "significant information regarding the user's browsing history": the identity of the individual internet user, the identity of the web server visited, the name of the web page visited, and the search terms the user used to find the web page, among other things.[49] This information collected through URLs is referred to in the tech world as a "referer header" or "referer."[50] The "referer" also tells the website an internet user is currently browsing what webpage that user was visiting immediately prior. In other words, it tells the current

[44] *See id.* (stating that in April 2018, Facebook like buttons appeared on at least 8.4 million other websites, "[m]eaning if you've so much as glanced any one of those eight to eleven million websites, you've been logged by Facebook").

[45] *See What Is Online Tracking*, *supra* note 32 (explaining how cookies work on your electronic device).

[46] *See id.* (describing multiple ways websites collect user data and the different types of data collected).

[47] *See In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 135 (3d Cir. 2015) (discussing the alleged Wiretap Act violation and URLs as the content having been intercepted); *see also In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596 (9th Cir. 2020) (stating background facts and identifying URLs as communication content at issue in the case).

[48] *In re Facebook*, 956 F.3d at 596.

[49] *See id.* (listing the types of information revealed through a URL address).

[50] *See id.* (explaining that a "referer" is what the collected URL is called in technical parlance).

website's server where the user came from. All this information is collected as cookies monitor the GET requests submitted by users.

When an internet user clicks on a link or types in URL information in the address bar, the user's web browser sends what is called a GET request to the website's server.[51] That GET request tells the website's server what page the internet user wants to see and requests that the website server send that web page back to the internet user's browser.[52] Before the advent of third-party cookies, the information transmitted to the website owner's server through this communication and the use of the website owner's first-party cookie would only be available to the internet user and the owner of the website visited.[53] The third-party cookie changed that: now, when the internet user submits a GET request to a website that interacts with one of Facebook's millions of third-party cookies, either a new third-party cookies is placed on the internet user's computer, or a an already existent third-party cookie is accessed, which then instructs the internet user's browser to copy the GET request and forward it to Facebook as well.[54] This happens without the knowledge of the internet user.[55]

Thus, when internet users visit a website, they are consenting to their information being sent to the server connected to that website. At the same time, the third-party cookie allows an unrelated company to receive the same information internet users' browsers communicate to the website's server, without any

[51] *See id.* at 607 (explaining how GET requests work).

[52] *See id.* (explaining the two purposes of GET requests).

[53] *See* Michal Wlosik & Michael Sweeney, *What's the Difference Between First-Party and Third-Party Cookies?*, CLEARCODE (last updated July 23, 2021) (explaining that "[f]irst-party cookies are stored by the domain (website) you are visiting directly, while [t]hird-party cookies are created by domains other than the one you are visiting directly") [perma.cc/5EH9-SKX3].

[54] *See In re Facebook*, 956 F.3d at 607 (explaining how third-party websites with Facebook plug-ins transmit identical GET requests to Facebook's server so that both Facebook and the current third-party website receive the same URL information about users).

[55] *See id.* at 603 ("That this . . . information can be easily collected without user knowledge is similarly significant."); *see also In re* Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003) ("The pharmaceutical companies' websites gave no indication that use meant consent to collection of personal information by a third party. Rather Pharmatrak's involvement was meant to be invisible to the user, and it was.").

affirmative attempt on the users' part to connect with that third-party company.

C. Circumvention of Private Efforts to Block Third-Party Cookies

Private efforts to protect users' information from third-party cookies have been—and will likely continue to be—unsuccessful, necessitating a change in the applicable law. In response to internet users' concerns over the amount of data collected by companies like Facebook, other tech companies have made efforts to protect users' privacy by blocking third-party cookies.[56] For example, last year, Apple updated its browser, Safari, to block third-party cookies by default as a part of its Intelligent Tracking Prevention ("ITP").[57] In direct response to Apple's efforts to block third-party cookies, Facebook created a new version of what it calls the Facebook Pixel—a technology that acts as a first-party cookie and allows website owners to track internet users' behavior.[58] The new version of Facebook's Pixel was announced at the end of 2015, and Facebook made its use mandatory in 2017—the same year Apple launched the ITP.[59]

[56] *See* Kerry Flynn, *WTF Are Facebook's First-Party Cookies for Pixel?*, DIGIDAY (Oct. 9, 2018) ("Apple and Firefox recently announced that they will be blocking third-party cookies . . . ") [perma.cc/DY39-XC7P]; *see also In re* Google, 806 F.3d at 131 (explaining that Safari's opt-out cookie blocker, which is activated by default, was advertised as a unique feature "to better protect [] your privacy . . . .").

[57] *See* Nick Statt, *Apple Updates Safari's Anti-Tracking Tech with Full Third-Party Cookie Blocking*, THE VERGE (Mar. 24, 2020, 3:07 PM) (explaining steps Apple has taken to increase web privacy on its devices) [perma.cc/EE9S-JVM8].

[58] *Compare id.* (explaining that Apple launched its ITP in 2017), *with* Ana Gotter, *Are You Ready for the New Facebook Conversion Pixel?*, AGORAPULSE (last updated Aug. 24, 2021) (reporting that Facebook created the Pixel in 2015 and made its use mandatory in 2017, not coincidentally, the same year Apple launched the ITP) [perma.cc/87GU-7TMQ]. *See also* Flynn, *supra* note 56 ("This change was made in light of web browsers like Apple's Safari, Mozilla's Firefox and ad blocking preventing third-party cookies from being trackable.").

[59] *See* Statt, *supra* note 57 ("Apple first launched ITP within Safari [in 2017] . . . ."); *see also* Gotter, *supra* note 58 (explaining that Facebook launched the new version of its pixel in 2015 and made its use mandatory in 2017).

Facebook's new Pixel performs the same functions of a third-party cookie, namely, it duplicates communications submitted to websites and forwards them to Facebook, but it does so under the guise of a first-party cookie.[60] Here's how it works: if a website owner wants to utilize Facebook's analytical tools, it must "create" a Pixel through Facebook by selecting which user behaviors it is interested in tracking and providing Facebook's Pixel creator with a name for the Pixel.[61] Facebook then produces a piece of code that the website owner can then manually copy and paste into its website's code.[62] This is basically reverse plagiarism; it is akin to someone completing an essay and asking you to give it a title and sign your name to it, making it appear to anyone who happened to read the essay as if you were the true author. And because Facebook made use of the new Pixel mandatory, website owners who want to advertise through Facebook are effectively forced to create one of these disguised third-party cookies and place it on their websites.[63] Because these cookies appear, from a browser's standpoint, to have been created by the website owner, any third-party cookie blockers employed will be completely circumvented by the disguised third-party cookie.[64] Essentially, the Pixel is a wolf in sheep's clothing.

This is not the first time a company has connivingly circumvented attempts to protect internet users' privacy.[65] Another example of this happened in 2011 when Google deceivingly bypassed Safari's attempts to block third-party

[60] *See* Flynn, *supra* note 56 (characterizing Facebook's launch of the new version of its pixel as a "first-party cookie" in response to efforts to block third-party cookies).

[61] *See Show Your Ads to the Right People with Facebook Pixel*, META FOR BUSINESS (describing the steps to creating and using Facebook's Pixel) [perma.cc/CF4N-GC64].

[62] *See id.* (explaining the various uses for a Facebook Pixel).

[63] *See* Gotter, *supra* note 58 ("Facebook . . . made the change to the new pixel mandatory . . . .").

[64] *See* Flynn, *supra* note 56 (characterizing Facebook's launch of the new version of its pixel as a "first-party cookie" in response to efforts to block third-party cookies).

[65] *See* Liam Tung, *Google Pays $17m to Settle Safari Cookie Privacy-Bypass Charge*, ZDNET (Nov. 19, 2013) (covering the settlement between Google and Apple in 2013 for Google's deceit in bypassing Apple's Safari browser's third-party cookie blocker) [https://perma.cc/P5CR-FF3A].

cookies.[66] Contemporaneous to this bypass, Google assured internet users that they could rely on Safari's default settings to block third-party cookies.[67] The case resulting from that deceit will be detailed in Part IV.

Both the examples detailed above prove that big tech companies that rely on ad revenue will always find a way to get the data they need, even if they have to resort to deceitful tactics.[68] And the ultimate effect of these tactics, in the context of the Wiretap Act and its party exception, is to make these third-party companies appear as the intended parties of the communications internet users submit to websites through GET requests, therefore absolving them of any liability under the Act. But are they actually parties to the communications? The federal circuit courts are split on the answer to this question. That circuit split will be explored below.

IV. The Circuit Split

This Part will summarize four pertinent cases. The first two cases included are *In re Pharmatrak, Inc.*[69] and *United States v. Szymuszkiewicz*.[70] In each of those cases, the First and Seventh Circuits, respectively, held that the defendants were subject to liability under the Wiretap Act.[71] The courts in those cases implicitly found the Act's party exception to be inapplicable.[72] While *Pharmatrak* illustrates a court's application of the Wiretap

[66] *See id.* (explaining an example of Google attempting to avoid efforts to protect user privacy).

[67] *See id.* (providing another example of deceit by Google in their attempts to bypass user privacy protections).

[68] *See id; see also* Flynn, *supra* note 56 (demonstrating that if privacy protection is preventative of companies gathering data they need, they will use other means to obtain this data).

[69] 329 F.3d 9 (1st Cir. 2003).

[70] 622 F.3d 701 (7th Cir. 2010).

[71] *See In re Pharmatrak*, 329 F.3d at 18–23; *see also Szymuszkiewicz*, 622 F.3d at 706–07 (explaining the result of both of these cases).

[72] *See In re* Facebook, 956 F.3d 589, 607 (9th Cir. 2020) ("The First and Seventh Circuits have implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to the communications within the meaning of the Act.").

Act to the use of cookies on the internet,[73] *Szymuszkiewicz* serves as an example of how the Act has been applied to an internet case where the defendant installed software on his boss's computer that functioned similarly to cookies.[74]

The next two cases summarized in this part are *In re Google, Inc. Cookie Placement Consumer Privacy Litigation*[75] and *In re Facebook, Inc. Internet Tracking Litigation*.[76] Those cases represent the circuit split for which this note proposes solutions. Both cases address the application of the Wiretap Act's party exception in the internet context—more specifically to internet companies' use of third-party cookies.[77]

A. *In re Pharmatrak, Inc.*

Pharmatrak was an enterprising company that provided a service known as "NETcompare" to pharmaceutical companies.[78] That service accessed and collected certain information about internet users as they browsed the pharmaceutical companies' websites.[79] This information was then provided to the pharmaceutical companies and allowed them to compare their websites' traffic and usage with that of other companies in the pharmaceutical industry.[80] Even though the pharmaceutical

[73] *See In re Pharmatrak*, 329 F.3d at 15 (discussing the use of cookies in the case).

[74] *See Szymuszkiewicz*, 622 F.3d at 702–03 (explaining that the defendant had implemented a "rule" on his boss's computer that duplicated and forwarded all email messages to the defendant that his boss had received); *see also supra* Part III.B (explaining how cookies can be used to duplicate and forward internet communications to third parties).

[75] 806 F.3d 125 (3d Cir. 2015).

[76] 956 F.3d 589 (9th Cir. 2020).

[77] *See In re Google*, 806 F.3d at 140; *see also In re Facebook*, 956 F.3d at 607–08 (applying the Wiretap Act's party exception to the use of third-party cookies and finding the Wiretap Act's party exception inapplicable to the use of third-party cookies).

[78] *See In re Pharmatrak*, 329 F.3d at 12 (explaining what type of company Pharmatrak was and the service they provided).

[79] *See id.* (explaining how the NETcompare service operated and the function it served).

[80] *See id.* (elaborating on how NETcompare is utilized by pharmaceutical companies to compare website traffic with other similar companies).

companies were adamant that personally identifiable information not be collected by NETcompare, such information was found on Pharmatrak's servers, and the users whose information was found sued Pharmatrak in a class-action lawsuit.[81]

NETcompare operated similarly to Facebook's Pixel.[82] Pharmatrak instructed the pharmaceutical companies to install a piece of code onto the webpages they wished to track.[83] This code instructed the computers of users who visited the websites to communicate directly with Pharmatrak's server.[84] Through this communication, Pharmatrak's server either placed or accessed a "persistent cookie" on the user's computer.[85] A persistent cookie is a cookie that *does not expire when a user ends his or her online session*.[86] These persistent cookies tracked internet users across multiple websites and collected information, such as the URLs they visited, and that data was recorded on Pharmatrak's web servers.[87]

Pharmatrak would send monthly reports to the pharmaceutical companies, comparing the data collected from each company's webpage to that collected from other pharmaceutical companies' webpages.[88] Although the reports did not contain any personally identifiable information, and although Pharmatrak assured its clients that NETcompare could not collect such information, Pharamtrak had indeed collected personally

[81] *See id.* (revealing that private information, which was not supposed to be collected, was found on Pharmatrak's servers, leading to the lawsuit).

[82] *See* Part III. C (explaining that Facebook's Pixel works and operates in a similar manner to NETcompare).

[83] *See In re* Pharmatrak 329 F.3d at 9 (detailing Pharmatrak's instructions to companies to include code which would allow the website to be tracked).

[84] *See id.* (explaining that the installed code instructed computers to communicate directly with Pharmatrak).

[85] *See id.* at 14 (detailing the consequences of the communication between the code and the computer that enabled constant tracking of the website by Pharmatrak).

[86] *See id.* (defining what a persistent cookie is while implying that a non-persistent cookie is one that expires upon the cessation of the online session, highlighting the intrusiveness of this type of cookie).

[87] *See id.* (outlining how the persistent cookie tracked data across multiple websites that were recorded by Pharmatrak).

[88] *See id.* (revealing what Pharmatrak did with the data once it was obtained).

identifiable information about some users.[89] The information found on Pharmatrak's servers included "names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website."[90]

The reason only some users' personal information was collected was due to an interaction between NETcompare and code written by one pharmaceutical client.[91] That client used the GET method to transmit information from a rebate form on one of its medications. The client subsequently altered the code for that specific webpage to use the POST method of transmission instead.[92]

Because NETcompare collected URLs submitted by users visiting the pharmaceutical companies' websites, it collected the information included in the GET requests submitted on this particular client's webpage. No evidence suggested that Pharmatrak had instructed its clients to use either the GET or POST methods in their installation of the NETcompare code.[93]

The First Circuit outlined all the elements of a claim brought under the Wiretap Act, and it addressed and analyzed the consent exception in § 2511(2)(d) but ignored the party exception.[94] The First Circuit ultimately reversed and remanded the case for further proceedings, finding that Pharmatrak could be held liable under the Wiretap Act, implicitly finding that Pharmatrak was not a "party" to the communications from online users.[95]

[89] *See id.* at 15 (showing the inconsistencies between Pharmatrak action and what it told its customers).

[90] *See id.* (explaining the type of date collected by Pharmatrak).

[91] *See id.* (discussing the reason that only some users personal information was gathered and not all users).

[92] *See id.* at 15–16 (explaining the GET method of transmission appends information submitted by the internet user to the URL, while the POST method only includes information submitted by users in the body of the request and thus, such information would not be visible to third parties collecting the URLs visited by users).

[93] *See id.* (showing that Pharmatrak had not instructed its clients to act in certain capacities).

[94] *See id.* at 20 (evaluating the consent exception without mentioning the party exception).

[95] *See id.* at 13. (summarizing the conclusion of the case).

B. United States v. Szymuszkiewicz

Szymuszkiewicz was a revenue officer who was fearing for his job, as his driver's license had been suspended for drunk driving, and he was regularly required to drive as part of his job.[96] In response to this concern, Szymuszkiewicz set up a forwarding rule on his supervisor's Microsoft Outlook account, which instructed Outlook to forward all the supervisor's emails to Szymuszkiewicz.[97] Szymuszkiewicz was ultimately convicted of violating the Wiretap Act.[98]

Even though the technology at issue in *Szymuszkiewicz* was not cookie-based, its functionality was similar to a cookie's in that it was placed on the unsuspecting internet user's computer by a third party, and it copied and forwarded communications between the internet user and another party to the third party (in this case, Szymuszkiewicz).[99]

In its opinion, the Seventh Circuit focused primarily on the different elements of a claim brought under the Wiretap Act and did not address the party exception directly.[100] The court ultimately held that Szymuszkiewicz was properly convicted for violation of the Act, implicitly finding that he was not a party to the communications at issue.[101]

C. In re Google, Inc. Cookie Placement Consumer Privacy Litigation

In 2015, the Third Circuit found that Google, among others, was "the intended recipient[] of the transmissions at issue—i.e. GET requests that the plaintiffs' browsers sent directly to [Google's] servers," and therefore, they could not be held liable

[96] United States v. Szymuszkiewicz, 622 F.3d. 701, 702 (7th Cir. 2010).

[97] *Id.* at 703.

[98] *See id.* at 707 ("Thus Szymuszkiewicz acquired the emails by using at least three devices: Infusino's computer . . . the Kansas City server . . . and his own computer.").

[99] *See* Part III.B (explaining how third-party cookies function).

[100] *See id.* at 703–07 (discussing the different elements of the Wiretap Act but not the party exception).

[101] *Id.* at 707.

under the Wiretap Act.[102] In that case, Google identified and exploited a loophole in Safari's third-party cookie blocker.[103] That loophole was meant to be an exception to Safari's cookie blocker, which allowed third parties to install cookies on users' browsers only if the browsers submitted a particular form to the third party.[104] "Google used code to command users' web browsers to automatically submit a hidden form to Google when users visited websites embedded with Google advertisements."[105] This allowed Google to then place third-party cookies on users' browsers despite Safari's contrary intention.[106]

Significantly, Google not only knew about Safari's intention to provide users with enhanced privacy by blocking third-party cookies, but Google also reassured visitors to its public website that Safari's default blocker "would prevent the installation of tracking cookies."[107] A consolidated class-action lawsuit ensued, and one of the claims was that Google had violated the Wiretap Act.[108]

In evaluating the Wiretap Act claim, the Third Circuit found that Google was the intended party to the communications at issue despite the fact that Google had deceitfully induced internet users into a false sense of security and continued tracking them by surreptitiously circumventing Safari's cookie blocker.[109] In its reasoning, the court concluded, "[W]e do not agree that a deceit upon the sender affects the presumptive non-liability of parties under § 2511(2)(d)."[110] In making this conclusion, the court pointed to *United States v. Pasha*,[111] a Seventh Circuit decision that held

[102] *In re* Google, 806 F.3d 125, 142–43 (3d Cir. 2015) (finding that the defendants did nothing unlawful).

[103] *Id.* at 132 (explaining that Safari's cookie blocker had an exception, including permitting third-party cookies).

[104] *Id.* at 132 (detailing how the exception to the cookie blocker was intended to work).

[105] *Id.*

[106] *See id.* (describing how Google was able to utilize this loophole to its advantage).

[107] *Id.*

[108] *Id.* at 133.

[109] *See id.* at 142–43 (finding Google was an intended party to the communication).

[110] *Id.* at 143.

[111] 332 F.2d 193 (7th Cir. 1964)

that a police officer's impersonation of the intended recipient of a phone call did not violate the Wiretap Act.[112]

To support this conclusion, the Third Circuit also referenced the Sixth Circuit's reasoning in *Clemons v. Waller*,[113] which pointed out that when Congress amended the Wiretap Act in 1986, it "specifically mentioned *Pasha* in its discussion of the 'party exception to the communication' provision."[114] In *Clemons*, the Sixth Circuit went on to reason that § 2511(2)(c), which excepts parties acting under the color of law from liability under the Wiretap Act if they are considered parties to the communication, is synonymous with § 2511(2)(d), which applies to private parties.[115] Additionally, the Sixth Circuit quoted the Seventh Circuit in *Pasha* in reasoning that the party exception to the Wiretap Act "largely reflects existing law. Where one of the parties consents, it is not unlawful . . . . '[P]arty' would mean the person actually participating in the communication."[116]

Thus, the Third Circuit concluded that Google could not be held liable for its deceit under the Wiretap Act.[117] However, there are many flaws to this reasoning, which are discussed in conjunction with the proposed solutions in Part V.

D. In re Facebook, Inc. Internet Tracking Litigation

In 2020, the Ninth Circuit found that Facebook was not a "party" within the meaning of the Wiretap Act in its duplication

[112] *See id.* at 198 ("Although the callers . . . were unaware that they were not being heard by the intended receivers and some were even misled into believing they were talking to one or the other defendants, the conversation between the callers and the agent cannot be said to have been intercepted.").

[113] *See* 82 Fed. App'x 436, 442 (6th Cir. 2003) (finding investigator was party to fax transmission from telephone company).

[114] *In re* Google, 806 F.3d 125, 144 (3d Cir. 2015) (citing Clemons v. Waller, 82 Fed. App'x 436,442 (6th Cir. 2003)).

[115] *See id.* (reasoning that § 2511(2)(c) is "pari materia with § 2511(2)(d)").

[116] *Clemons*, 82 Fed. Appx. at 442 (quoting S. Rep. No. 90-1097, at 93–94 (1968) (citing United States v. Pasha, 332 F.2d 193 (7th Cir. 1964))).

[117] *See id.* at 145 ("Based on the facts . . . the defendants were parties to any communication that they acquired, such that their conduct is within the § 2511(2)(d) exception.").

and forwarding of users' GET requests.[118] There, the class alleged that Facebook had used cookies to track users throughout the internet, even when they were not logged into Facebook.[119] Additionally, internal communications between Facebook executives revealed that they "were aware of the tracking of logged-out users and recognized that these practices posed various user-privacy issues."[120]

In its reasoning, the Ninth Circuit referred to the First Circuit's decision in *In re Pharmatrak* and the Seventh Circuit's decision in *Szymuszkiewicz*. Both cases, as explained above, implicitly found that the defendants were not parties within the meaning of the Wiretap Act and could be held liable for their interceptions of electronic communications.[121]

The Ninth Circuit agreed with the First and Seventh Circuits' implicit findings and held that Facebook was "not exempt from liability as a matter of law under the Wiretap Act . . . as a party to the communication,"[122] reasoning that "[p]ermitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule."[123]

V. Proposed Solutions

This Part proposes two solutions to the circuit split summarized above. Both solutions have as a primary objective the protection of internet users' information, with requirements in excess of the status quo notice-and-consent requirements typical in privacy law. The first solution proposed is for Congress to update the Wiretap Act to include a definition for "party." Such a definition should be narrow in the interest of protecting internet

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

[119] *Id.* at 596.

[120] *Id.*

[121] *See In re Facebook*, 956 F.3d at 607 (explaining both cases and the implication derived from each that the defendants were not parties to the communications within the meaning of the Wiretap Act).

[122] *Id.* at 608.

[123] *Id.*

users' information. The second solution proposed is for the Supreme Court to interpret the Wiretap Act's party exception with the Act's objective of protecting the privacy of communications in mind, rejecting the Third Circuit's interpretation in *In re Google*, and providing lower courts with a clear test with which to analyze the party exception in the internet context.

A. Heightened Notice-and-Consent Requirement

A well-versed privacy law practitioner may read the two proposed solutions in this Part and, at first blush, view them as synonymous with the notice-and-consent requirement generally found in privacy law.[124] However, the knowledge and consent requirements proposed here are not to be conflated with the status quo notice-and-consent requirements typically applied in the online context that have been scrutinized by privacy experts.[125] Instead, the solutions below intend a heightened requirement for an entity to be considered a "party" to online communications for purposes of the Wiretap Act. Additionally, the solutions proposed are not intended to solve data privacy issues on the internet, but rather, they are proposed to resolve the circuit split and provide a workable definition of "party" for purposes of the Wiretap Act's party exception.

Heightened knowledge and consent requirements are necessary, as the likely reaction of companies subject to the solutions proposed here would be to amend their end user license agreements, for example, to specifically mention that by clicking the "I Agree" button, users are agreeing that the company is a "party" to all their communications; or companies may provide an obscure banner providing internet users with the option to opt-out of the company's privacy practices.[126] The same mechanisms that

[124] *See* Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AMERICA (Mar. 23, 2020) (explaining that notice-and-consent requirements are the status quo in privacy law, particularly on the internet, and this is failing to adequately protect consumers online) [perma.cc/E4MH-VLNN].

[125] *See id.* (noting that privacy experts are increasingly condemning the notice-and-consent requirements online companies are required to abide by as useless).

[126] *See* Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting Over Privacy: Introduction*, COASE-SANDOR WORKING PAPER SERIES IN LAW AND

have been used to contract around consumers' rights to their day in court should not be allowed in the privacy context online to treat internet users' privacy rights as an afterthought.[127]

Instead, when it comes to being considered a "party" for purposes of online communications, the knowledge and consent requirements proposed in this Part should be viewed as additional, separate requirements for which a discrete paragraph in a user agreement or privacy notice will not suffice. This will be discussed in more depth in the subparts below.

B. Congress Should Update the Wiretap Act to Include a Definition for "Party"

The issue that led to the circuit split summarized in the previous Part was Congress's failure to define "party" within the meaning of the Wiretap Act and its party exception.[128] It follows, then, that the seemingly simplest solution would be for Congress to define the term and resolve the circuit split.

The question that inevitably arises is how Congress should define the term. Any definition of the term should be crafted with the Wiretap Act's primary objective in mind: "to protect effectively the privacy of communications"[129] from "unseen auditors."[130]

It is important to point out that the issue with internet companies' collection of users' information is not merely the collection of information itself, but rather, the fact that such collection is being done *without users' knowledge*.[131] It is clear that

ECONOMICS, No. 792, at S8 (2017) ("Firms that develop business models that are constrained by statutory privacy rules would post privacy notices that effectively override these rules.").

[127] *See id.* at S6 (posing the question of whether clicking "agree" is sufficient to disclaim privacy rights and discussing the use of this mechanism to contract over such things as warranties and arbitration).

[128] *See In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 607 (9th Cir. 2020) ("The Wiretap Act does not define the term "party" in its liability exception, and the other circuit courts that have considered the Act's scope have interpreted the term in different ways.").

[129] *In re* Pharmatrak, Inc, 329 F.3d 9, 18 (1st Cir. 2003).

[130] S. REP. NO. 90-1097, at 2154 (1968).

[131] *See* Timothy Morey et al., *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015) (recognizing that "revelations about companies' covert activities . . . make customers nervous" but that "customers

through the collection and use of users' data, companies can provide more value than they otherwise would be able to.[132] In this sense, user data is treated as currency, providing products and services to users in exchange for their data, rather than money.[133]

Thus, a definition for "party" would need to have the objective of protecting users' information in mind, while also avoiding the complete obliteration of internet companies' ability to collect such information. The objective should thus be to enable internet users to more effectively use their data as a bargaining chip by requiring more transparency, which would result in users having more control over the use of their data.[134]

1. The Knowledge Requirement

The first requirement for someone to be considered a party to any communication should be knowledge of that someone's presence in the communication. This requirement is in line with Congress's expressed intent to prevent "an unseen auditor" from intercepting communications.[135] Unseen implies unknown. So, as a threshold element, Congress should require that any entity claiming to be a party to a particular communication be known to those actually communicating.

This knowledge requirement is not to be confused with notice requirements currently used in existing law.[136] "We've all seen it

appreciate that data sharing can lead to products and services that make their lives easier and more entertaining, educate them, and save them money") [https://perma.cc/3VNL-JD8C].

[132] *See id.* (explaining the trade between companies that collect data and consumers from whom the companies collect that data and how value is perceived differently based on what data is being collected for).

[133] *See id.* ("If companies understand how much data is worth to consumers, they can offer commensurate value in return for it.").

[134] *See* Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019) (presenting results of a study that showed the vast majority of Americans feel they have little to no control over how their data is used by companies that collect it online) [https://perma.cc/RHY4-EV5T].

[135] S. REP. NO. 90-1097, at 2154 (1968).

[136] *See* Kerry, *supra* note 6 ("Our existing laws also rely heavily on notice and consent . . . .") [https://perma.cc/QH3U-DF9B]; *see also* Park, *supra* note 124

before: you enter a website and a banner pops up along the bottom, asking you to 'click here' to accept the site's terms of service and privacy policy."[137] This is supposed to provide the information necessary for internet users to consent to the use of their data, among other things; however, studies show that next to no one actually reads the terms of service or privacy policies.[138] While this practice may be sufficient to constitute notice under current law, it is not enough to provide the requisite knowledge proposed here for an entity to be considered a party to internet users' online communications.

How can internet users give informed consent if they are not truly informed? Notice should no longer be sufficient. Knowledge should be the new standard, and the law must require more of online companies who glean obtuse profits from the use of users' data. While this conversation is ongoing and will inevitably require more research and creative solutions, one first step would be to impose a temporal requirement to the provision of knowledge. Instead of presenting internet users with the notice one second before they can access the website or application, users should be presented with the information when it becomes relevant.[139]

One example that illustrates how much more effective this practice has the potential to be is "Facebook's pop-up for posting a photo," which "offers a bright 'who can see this?'" link that explains that aspect of Facebook's privacy terms.[140] It is one thing to be aware that something happens—it is entirely different to know something is *happening*. Requiring internet companies to provide

(explaining the longstanding practices required by the notice and consent framework).

[137] Park, *supra* note 124.

[138] *See* David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, THE GUARDIAN (Mar. 3, 2017) ("[O]n average, these more careful joiners spent around a minute with the thousands of words that make up NameDrop's privacy and service agreements. And then they all agreed to them.") [https://perma.cc/WZJ8-HXBH].

[139] *See id.* (proposing as a way of addressing the no-reading problem moving "the contract out of the one-second moment before access is granted, and to place its terms before the user when they become relevant"); *see also* Ombri Ben-Shahar & Lior Strahilevitz, *supra* note 126, at S8 ("Firms that develop business models that are constrained by statutory privacy rules would post privacy notices that effectively override these rules.").

[140] *See id.*

internet users with information on how their data is being used in real time may not fix the issue altogether, but it would be a good first step. Studies have shown that "when design invites people to consider their options, at least some do."[141]

When it comes to design, the obscure banners that pop up at the bottom of websites are also insufficient to provide the requisite knowledge. A true conspicuousness requirement should be imposed that would actually give internet users pause. An enhanced conspicuousness requirement, combined with a real-time knowledge requirement, would diverge from the current status quo and prompt more users to consider what is being presented.[142] At the very least, timing and design changes could be more effective at educating users on the use of their data as it is being collected, providing them with the knowledge necessary to provide *effective*, not just *informed*, consent, which will be discussed below.

2. The Consent Requirement

In addition to the knowledge element, internet users' consent should be required. Current privacy law standards require "informed consent," but as has been discussed already, the consent given by internet users online is not informed in the real sense.[143] Part of the reason users lack the sufficient knowledge to truly consent to how companies collect and use their data is that users are charged with an unrealistic and onerous duty to comb through thousands of words in digital contracts.[144] This burden should be

[141] *See id.* (explaining that a study changing how users were presented with the privacy notice resulted in a 26% difference between those who simply agreed and those who opted out of the data collection).

[142] *See* Ben-Shahar & Strahilevitz, *supra* note 126, at S9 (positing that consumers may so easily agree to opt in, or fail to opt out, because of lack of information and arguing that "informed consumers might refuse to opt in or might initiate their own opt outs," while "uninformed consumers . . . would stick with any default rule").

[143] *See* Part V.B.1 (discussing the fact that internet users don't actually read privacy notices and are not truly informed of what they are agreeing to online).

[144] *See* Berreby, *supra* note 138 (explaining that "reading an average American's digital contracts would take almost 250 hours a year" and arguing that burden is exhausting and irrational); *see also* Kerry, *supra* note 6 (arguing that informed consent may have been "practical two decades ago, but it is a

shifted to the companies profiting from the use of internet users' data.

One way to shift this burden would be to require an opt-in, rather than the current opt-out, regime for consent to collection and use of user data.[145] This would require internet users to affirmatively consent to the collection and use of their data by, for example, presenting users with a "yes" and "no" option, rather than an option to change the default settings.[146] Apple has made this change, and it has resulted in frustration from Facebook specifically, evidencing the profound effect such changes may have if implemented across the board.[147] Such a shift would require internet companies to take on the burden of informing internet users in more understandable terms and persuading them to consent, rather than cowering in the safe harbor that is the opt-out regime.[148]

Although the Wiretap Act currently includes a consent exception, that exception is one-sided.[149] This allows an internet company using Facebook's Pixel, for example, to unilaterally

fantasy today," as "a constant streams of online interactions" results in no one reading privacy policies).

[145] *See* Ben-Shahar & Strahlivitz, *supra* note 126, at S8 (explaining that opt-in schemes are more protective "because they require firms to get consumers' affirmative consent to override the pro-consumer status quo," while "opt-out schemes . . . put the burden on consumers to initiate the exit from the pro-business status quo.").

[146] *See* Berreby, *supra* note 138 (explaining that users were 26% less likely to accept privacy policies when users were met with a "yes" and "no" option, rather than a click-to-accept prompt).

[147] *See* Deepa Seetharaman et al., *Facebook Meets Apple in Clash of the Tech Titans—'We Need to Inflict Pain,'* WALL ST. J. (Feb. 13, 2021, 12:00 AM) (discussing Apple's changes to its platforms, requiring users to opt into Facebook's use of their data and Mark Zuckerberg's reaction that Facebook needs "to inflict pain" on Apple) [https://perma.cc/5GQV-TTJN].

[148] *See* Ben-Shahar & Strahilevitz, *supra* note 126, at S8 ("The contractual status of privacy notices means that users grant consent to these practices and thus provide firms a critical safe harbor.").

[149] *See* 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful . . . for a person . . . to intercept a wire, oral, or electronic communication . . . where *one of the parties* to the communication has given prior consent to such interception . . . " (emphasis added)); *see also In re* Pharmatrak, Inc, 329 F.3d 9, 19–21 (1st Cir. 2003) (finding that *neither party* consented to the collection of the information and explaining that the consent of either would have absolved Pharmatrak from liability under the Wiretap Act).

consent to Facebook's collection of users' information as they visit the company's website. Instead of this one-sided consent requirement, a definition of "party" should require the consent of all participants to a particular communication for a third-party participant to be considered a party.

Apple already implemented such a requirement for companies who develop applications for the iOS platform.[150] In September 2020, Apple announced planned changes to the software on its devices.[151] The effect of this update was two-fold: first, it added a new privacy information section to Apple's App Store product pages in an effort to help users understand apps' privacy practices.[152] Second, the update required that apps obtain "user permission to track users across apps or websites owned by other companies, or to access the device's advertising identifier."[153]

In effect, Apple made it easier to determine whether users consent to companies' participation in their online communications with web servers. Now, when iPhone, iPad, and Apple TV users open a different app for the first time, they are greeted by a prompt, asking if they consent to the app sharing information with other companies.[154] The prompt and privacy information section in Apple's App Store provide users with knowledge, and their decision when greeted with the app prompts determines their consent or lack thereof.

Thus, Congress should define "party" to require that all participants in any communication both have knowledge of, and consent to, any third party's involvement in the communication at issue. This will require internet companies to educate users and be more transparent in their collection and use of users' data,

[150] *Details for App Privacy Questions Now Available*, APPLE (Sep. 3, 2020) [https://perma.cc/Q7BC-ZU84].

[151] *See id* (providing an overview of what changes are included in the September 2020 updates).

[152] *See id* (explaining that the privacy information section is intended to help users understand the app's privacy practices).

[153] *Id.*

[154] *See* Nick Statt, *Apple Delays Privacy Feature that Would Let iPhone Owners Keep Ad Tracking at Bay*, THE VERGE (Sep. 3, 2020, 1:16 PM) ("[T]he new feature will show users a prompt when an app has requested their so-called Identification for Advertisers.") [https://perma.cc/RB42-PCGQ].

providing users with greater control over their data and effectively protecting the privacy of communications in general.

C. The Supreme Court Should Proffer a Clear Interpretation of the Wiretap Act's Party Exception

If Congress does not provide a clear definition for "party," the Supreme Court should interpret that term in a way that provides lower courts with a clear standard to use in determining whether the party exception applies, particularly in the internet context. In developing such a standard, the Supreme Court should reject the Third Circuit's interpretation of the party exception in *In re Google*. That interpretation has multiple flaws, which will be discussed below.

1. Principles of Statutory Interpretation

Before discussing the Third Circuit's flawed interpretation of the Wiretap Act's party exception and proposing an alternate interpretation, it is necessary to consider principles of statutory interpretation.

The first step in interpreting any statute is "of course . . . the statutory text."[155] In looking to the text, "[u]nless otherwise defined, statutory terms are generally interpreted in accordance with their ordinary meaning."[156] And that "ordinary meaning" can be ascertained by looking at how the same term is used throughout the same statute or by an appeal to the dictionary.[157] Furthermore, a statute's use of a term presents ambiguity, a court may look to the statute's legislative history to understand Congress's intent

[155] *See* Sebelius v. Cloer, 569 U.S. 369, 376 (2013) (quoting BP America Production Co. v. Burton, 549 U.S. 84, 91 (2006)).

[156] BP America Production Co. v. Burton, 549 U.S. 84, 91 (2006).

[157] *See e.g.*, *id.* (relying on Black's Law Dictionary for the meaning of the word "cognizable" as used in the Federal Tort Claims Act); Asgrow Seed Co. v. Winterboer, 513 U.S. 179, 187 (1995) (relying on regular dictionary definitions to interpret the word "marketing" as used in the Plant Variety Protection Act); Commissioner v. Soliman, 506 U.S. 168, 174 (1993) (relying on the dictionary definition of the word "principal" as used to modify a taxpayer's place of business for purposes of income tax deduction).

and purpose behind the statute and to interpret the term at issue in accordance with that intent and purpose.[158]

2. The Third Circuit's Errant Interpretation of the Party Exception

As a reminder, in *In re Google*,[159] Google assured internet users that Apple's new efforts to block third-party cookies were sufficient, inducing users into a false sense of security, as Google proceeded to circumvent protocols on Apple's Safari so that Google could continue placing third-party cookies on users' browsers without their knowledge.[160] In that case, the Third Circuit concluded that although Google had surreptitiously placed third-party cookies on users' browsers, it was excepted from liability under the Wiretap Act's party exception as a "party to the communication."[161] However, the Third Circuit's reasoning, particularly its interpretation of the Wiretap Act's party exception, is flawed.

The first issue with the Third Circuit's reasoning arises from its comparison of Google's deceitful circumvention of Safari's third-party cookie blocker to a policeman's impersonation of the intended party in *Pasha*.[162] It is a "cardinal rule of statutory construction that no provision should be construed to be entirely redundant."[163] The Third Circuit's comparison of Google to the police officer treats

[158] *See, e.g.*, United States v. Turkette, 452 U.S. 576, 588–90 (1981) (relying on RICO statement of findings and purpose to conclude that the term "enterprise" as used in the act included criminal conspiracies organized for illegitimate purposes).

[159] 806 F.3d 125 (3d Cir. 2015).

[160] *See supra* Subpart IV.C (discussing the facts of *In re Google* and the Third Circuit's reasoning).

[161] *In re Google*, 806 F.3d at 142–43; 18 U.S.C. § 2511(2)(d) (2018).

[162] *In re Google*, 806 F.3d at 143–44 (mentioning that Congress discussed *Pasha* when amending the Wiretap Act).

[163] Kungys v. United States, 485 U.S. 759, 778 (1988).

§ 2511(2)(c) and (2)(d) as synonymous,[164] which would essentially render one provision or the other "entirely redundant."[165]

Additionally, Congress clearly did not intend the two provisions to be synonymous. This is implied by the fact that Congress left the two provisions separate when it updated the Wiretap Act in 1986. If Congress truly intended the same analysis to be applied to those acting under and without the color of law, it could have easily consolidated the two provisions into one. Instead, Congress left the two provisions separate, indicating the intent that the party exception be applied somewhat differently to private parties as opposed to police officers. This inference is supported by the inherently different interests involved in each scenario.

When a police officer is acting under the color of law and impersonates an intended recipient to catch criminals, as was the case in *Pasha*, there are clearly different interests involved than when Google deceives consumers as they browse the internet. In the first scenario, the public's interest is at stake, while in the second scenario, Google is the one benefiting from its deceitful actions. One potential reason Congress decided to leave the two provisions separate was because it knew that these different interests must be considered when determining whether the party exception would absolve someone of liability under the Wiretap Act. This obvious distinction should have played into the Third Circuit's reasoning and resulted in a finding that Google, unlike a police officer protecting the public's interest, could be held liable for its actions under the Federal Wiretap Act.

The next issue with the Third Circuit's comparison between the police officer's and Google's deceitful ploys is that the two instances are distinguishable in an important way. In *Pasha*, the police officer was pretending to be someone else, and the callers on the other end of the communication *knew the communication was taking place*, even though they did not know who was on the other end of the communication.[166] In Google's case, the communicator

[164] *See In re Google*, 806 F.3d at 144 ("In discussing § 2511(2)(c), which is in pari materia with § 2511(2)(d) . . . ") (citing Clemons v. Waller, 82 Fed. Appx. 436, 442 (6th Cir. 2003)).

[165] *Kungys*, 485 U.S. at 778.

[166] *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) (explaining that the callers in the case were "unaware they were not being heard by the

was not only unaware of who the communication was going to, but the communicator also did not know the separate duplication and forwarding of its communications was happening in the first place.[167] To the contrary, Google assured users that they were protected from the placement of third-party cookies.[168]

Another major issue with the Third Circuit's decision can be attributed to a misunderstanding of how third-party cookies function. In the court's explanation of the complaint, it said, "Google used code to command users' web browsers to automatically submit a hidden form to Google when users visited websites embedded with Google advertisements."[169] That form triggered an exception in Safari's third-party cookie blocker and allowed Google to place cookies on users' browsers without the users' knowledge.[170] In its decision, the court contradicted this explanation and said that Google was the intended recipient of the users' website submissions, even though, according to its own explanation, the users had no knowledge the information was being duplicated and forwarded to Google.[171] Contrarily, they were under the impression, because of Google's deceit, that their information was not being gathered and that third-party cookies were being blocked by Safari's default settings.[172]

Thus, if the Third Circuit followed its own explanation in its application of the law, it should have decided that Google was not a party to the communication at issue. The court failed to explain how Google was the intended recipient of the communications when there could not have been any sort of intent on the part of

intended receivers and . . . misled into believing they were talking to one or the other of the defendants").

[167] *See In re* Google 806 F.3d 125, 132 (3d Cir. 2015) (explaining that Google exploited loopholes to place third-party cookies on users' browsers while simultaneously reassuring visitors to its site that their browsers' default settings would block such placement).

[168] *See id.* ("Google not only contravened the cookie blockers—it held itself out as respecting the cookie blockers.").

[169] *In re* Google, 806 F.3d at 132.

[170] *See id.* (explaining the functionality of the hidden form).

[171] *See id.* ("[Google] had discovered, and [was] surreptitiously exploiting, loopholes in . . . the cookie blocker.").

[172] *See id.* (explaining that Google assured its users that Safari's cookie blocker would block all third-party cookies by default).

the communicator (the user in this instance). The only party who intended the communications to go to Google was Google itself.

Ironically, after its decision in *In re Google*, the Third Circuit contradicted itself by finding correct a jury instruction that defined a party as "a participant whose presence is known to the other parties contemporaneously with the communication."[173] This jury instruction is directly contradictory to the Third Circuit's finding in *In re Google*, which considered Google a party to the communications at issue, even though Google's presence in the communications was not known to the internet users.

3. The Correct Interpretation of the Party Exception

The party exception to the Wiretap Act says, in relevant part, "[i]t shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication . . . ."[174] Significantly, the term "party" is only used in two other places within the Wiretap Act: in the immediately preceding provision, which excepts from liability those who act under the color of law "where such person is a party to the communication";[175] and in the Act's definition of "aggrieved person."[176] These uses of the term do not shed much light on its intended definition.

Merriam-Webster's definition of "party" is "a person or group participating in an action or affair."[177] Furthermore, Merriam-Webster defines "participate" as "to take part" or "to have a part or share in something."[178] Thus, the plain language definition derived from an appeal to each of these definitions in the dictionary is that a person who is a party to a communication actually participates by having some part or share in the communication. This definition

[173] United States v. Eady, 648 Fed. App'x 188, 191 (3d Cir. 2016).

[174] 18 U.S.C. § 2511(2)(d) (2018).

[175] *Id.* § 2511(2)(c).

[176] *See id.* § 2510(11) ("'[A]ggrieved person' means a person who was a *party* to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.") (emphasis added).

[177] *Party*, MERRIAM-WEBSTER, [https://perma.cc/FW76-948N].

[178] *Participate*, MERRIAM-WEBSTER, [https://perma.cc/E4ZX-5GV5].

logically implies that a party to a communication is known to the other party or parties to that communication and is contributing something to it, rather than merely listening in or, in this case, duplicating and forwarding communications created and submitted by the actual parties to the communication.[179]

For example, the police officer in *Pasha* was a party to the communication at issue in that case, as he was participating by sharing the communication with the other party.[180] His presence was known, even though his identity was not.[181] And he was impersonating someone—in other words, he was actually contributing to the conversation, not merely listening in.[182] It follows that duplicating and forwarding a communication to which someone does not contribute would not be conduct that would make that person a "party" to the communication. That conduct would be entirely separate from the line of communication between two parties and instead falls squarely within the Act's definition of "intercept," which includes the "acquisition of the contents of any . . . electronic communication . . . ."[183]

This is not to say that to contribute to a communication, a person must necessarily actively participate. Someone who passively listens can still be a party to a communication, but the fact that the person is listening must still be known to the other party. Otherwise, the entire purpose of the Wiretap Act would be frustrated.[184]

[179] *See* United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964) ("Interception connotes a situation in which by surreptitious means a third party overhears a telephone conversation between two persons . . . . [I]mpersonation of the intended receiver is not an interception . . . .").

[180] *See id.* at 196 (describing the actions of the police officers).

[181] *See id.* at 198 ("The bettor intended his words to reach the officer, albeit the bettor thought he was someone else.").

[182] *See id.* at 198 (explaining that the call occurred between the callers and the police officer and that they had a conversation).

[183] 18 U.S.C. § 2510(4) (2018).

[184] *See In re* Pharmatrak, Inc. 329 F.3d 9, 18 ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications."); *see also In re* Facebook Inc. Internet Tracking Litig, 956 F.3d 589, 608 ("Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule.").

In the Wiretap Act's legislative history, it addresses—albeit briefly—the party exception: "'party' would mean the person actually participating in the communication."[185] The logical question that follows from this brief attempt at a definition of "party" is what "actually participating" would look like.

A district court in Illinois followed the Third Circuit's interpretation in *In re Google* and found that even if a person is not an intended recipient, that person can still be considered a party to a communication if that person actually participates in the communication at issue.[186] What is unclear from this definition of a party the Third Circuit posited is how an entity can be considered an active participant in a communication if all that entity is doing is placing a cookie on the user's computer that secretly duplicates and forwards to a third party the communications the user intended to communicate to the website the user was visiting. The Third Circuit's loose application of its definition of "party" would render useless the preclusion of intercepting electronic communications in the first place, as any entity could utilize techniques unknown to the average user and collect users' information without the users' knowledge but still be considered a "party" under the law and be exempt from any liability for such deceit.

This result would run directly contrary to Congress's intention, as articulated in the Wiretap Act's legislative history. This type of scenario is precisely the type of scenario Congress was trying to prevent with its amendment to the Wiretap Act in 1968: "No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by *an unseen auditor* . . . ."[187]

"Actually participating" should be interpreted along the same lines proposed in the previous subpart about Congress's update to

[185] S. REP. NO. 90–1097, at 2182 (1968).

[186] Zak v. Bose Corp., No. 17-cv-02928, 2020 WL 2762552, at *2 (N.D. Ill. 2020) ("A person who takes part in a conversation or whose presence is known to other participants is a party to the communication. Such a person is considered a party to the communication even if the person was not an intended participant.").

[187] S. REP. NO. 90–1097, at 2154 (emphasis added).

the Wiretap Act to effectively define "party."[188] This would mean that for an entity to be considered "actually participating" in a communication, internet users should be aware of the entity's involvement and consent to it.

The two issues that would likely be a focus of litigation in these contexts would be (1) whether an internet user had the requisite knowledge of an entity's involvement and (2) whether that entity obtained an internet user's consent.

In resolving the first issue, courts should use a heightened reasonable-person standard, considering the same factors as are discussed in Part V.B.1 above. And that standard should have as its subject the complainant. Thus, the first question to be resolved would be whether a reasonable person in the position of the complainant would have known about the defendant's involvement. To prove knowledge, a defendant would have to show that it conspicuously provided notice to the complainant—for example, through Apple's new privacy features discussed above or through requirements imposed by California's recently enacted privacy laws.[189]

If a defendant fails to provide evidence showing that a reasonable person in the complainant's shoes would have had knowledge of the defendant's involvement in a communication, the first element to being considered a "party" to the communication is left unsatisfied, and it is unnecessary to continue the analysis further. However, if the first element is satisfied, the defendant must then show that the complainant consented to the defendant's involvement in the communication. This would be somewhat easier to analyze, as it would merely require a court to look at how the complainant acted after being put on notice that the defendant would be involved in the communication at issue. For example, if

[188] *See supra* Subpart V.A (discussing the requirements that should be incorporated into a new definition of "party" in the Wiretap Act if Congress were to amend the act to include such a definition).

[189] *See supra* Subpart V.B.2 (explaining new features Apple is introducing to educate users about the use of their data on the internet and give them more control); *see also See How the CCPA Affects The Cookie Policy*, CLYM (Apr. 7, 2020) (discussing California's new privacy laws, which require websites that use cookies to inform users of such uses and provide them with an easy way of opting out of cookies and managing how websites use information collected through cookies) [https://perma.cc/U855-UMZ8].

the complainant visited a website and closed out or left the website shortly after being put on notice of another party's involvement, the natural inference would be that the complainant had not consented to the defendant's collection or use of the complainant's data. This element should also be judged according to the heightened consent standard outlined in Part V.B.2 above, requiring an opt-in regime and transparency.

VI. Conclusion

Internet companies collect a bevy of data about internet users on a daily basis, and those companies want to be parties to all online communications. The Wiretap Act represents a potential tool that can be used to hold these companies liable if they overstep; however, internet companies may find safe harbor in the Act's party exception. The existing circuit split on whether internet companies are parties to online communications makes the outcome of factually similar cases dependent on jurisdiction.

To resolve this circuit split, either Congress should provide a clear definition for "party" in the Wiretap Act, or the Supreme Court should proffer its own interpretation of the term. In either case, a heightened knowledge-and-consent standard should be applied to grant internet users greater transparency, giving them more control over their data and allowing for *effective*, not just *informed*, consent.