2022

Cookies and the Wiretap Act: Not Always Sweet

Aditi Padmanabhan

Cookies and the Wiretap Act: Not Always Sweet

Aditi Padmanabhan*

Introduction

It has happened to most of us. Your favorite retailer sends you an email alerting you to a sale, so you immediately click on it and start surfing to see if anything catches your interest. While you examine a few items, ultimately self-control wins and you close out of the tab while purchasing nothing. However, the next time you log into Facebook or Instagram, your feed shows you the same shirt or shoes you were considering not five minutes before. While the common joke is that this is just "your personal FBI agent earning his salary," the truth is much more insidious.

In fact, your browser has most likely been tracking your viewing data and selling that information to third parties, which then use this data to provide increasingly (and sometimes terrifyingly) accurate advertisements. And while this has become a boon for social media companies and web browsers, which often insert the code that surreptitiously tracks its users, it reflects a declining respect for data privacy.

However, while this practice has become increasingly prevalent, internet users are also more aware of these practices and are seeking recourse through multiple channels. Many consumers now use ad blockers, which block both ads and tracking devices that would continue to monitor their browsing habits after they have left a website.[1] Legislation such as the General Data Protection Regulations[2] ("GDPR") in Europe and the California Consumer Privacy Act of

*J.D. Candidate, 2022, Seton Hall University School of Law; B.B.A., Ross School of Business, University of Michigan

[1] Augustine Fou, *No More Third Party Cookies, No Problemo*, FORBES (Aug. 31, 2020, 7:37 AM) https://www.forbes.com/sites/augustinefou/2020/08/31/no-more-third-party-cookies---good-or-bad-news/#286e9b045948

[2] 2016 O.J. (L. 119).

2018[3] ("CCPA") have finally passed, but no data privacy legislation has passed at the United States federal level recently.[4] Therefore, more users are filing lawsuits challenging the pervasiveness of these techniques based on older laws designed for different technologies. Following exposés on Google and Facebook's data collection efforts, class actions filed in the Third and Ninth Circuits have charged prominent social media and web browsing companies with unauthorized "interceptions" under the federal Wiretap Act (the "Act").[5] The companies claimed they had immunity under the "party exception," which states that parties to a communication cannot be held liable for an interception under the Act.[6]

However, while the Third Circuit held that, due to the direct transmissions between the plaintiff users and defendant companies, the companies were "parties" to the communication,[7] the Ninth Circuit held that such unauthorized and unknown duplication could not shield a company from liability under the Act.[8] This circuit split creates clear uncertainties, not only in how companies should amend their business practices, if at all, but also how users should consider adjusting their browsing habits. It also could lead to the undesirable outcome of "forum shopping," which is the practice where litigants select the most favorable jurisdiction for their claim.[9] In this case, it is likely that parties looking to charge companies for their data harvesting practices will bring suit in the Ninth Circuit, as the court has already established a favorable precedent for claims brought under the Act.

---

[3] Cal. Civ. Code § 1798.100 et seq.
[4] *Id*.
[5] *See* In re Google Inc., 806 F.3d 125 (3d Cir. 2015); In re Nickelodeon Cons. Priv. Litig., 827 F.3d 262 (3d Cir. 2016); Davis v. Facebook, Inc. (In re Facebook Inc.), 956 F.3d 589 (9th Cir. 2020).
[6] The "Act" refers to the version of the Wiretap Act amended by the ECPA, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et. seq. (1986). Any references to the original Wiretap Act will be as the "original Wiretap Act," Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq. (1968).
[7] *Google*, 806 F.3d at 145.
[8] *Facebook*, 956 F.3d at 608.
[9] Stephen Michael Sheppard, *The Wolters Kluwer Bouvier's Law Dictionary Desk Edition* (Wolters Kluwer eds., Desk ed. 2012).

This comment will examine interpretations of the Act in light of a rapidly evolving technological landscape, as well as propose solutions that will balance business development with respect for individual privacy. Part I of this comment will discuss the evolution of digital marketing and the business and technological models that allow companies to profit from customer's internet searches. It will also discuss virtual "cookies" and how they have augmented this new advertising model. Part II will discuss the key statutes that are the focus of this comment, the Act and Electronic Communications Privacy Act, as well as the party and consent exceptions that many entities have claimed to shield their conduct. Part III will review the Third and Ninth Circuits interpretations of the Act in light of this changing technological landscape and the resulting circuit split. Part IV will make recommendations on how courts should interpret the Act to cope with the rapid expansion of this practice, as well as other legislative and external solutions users should pursue.

Part I: The Technology

This section will cover the developments and business models that have created invasive data tracking and harvesting methodologies. As our technology improves, so too do the tools digital advertisers use to provide services and goods to potential consumers. Increasingly sophisticated data analytics offer advertisers and websites the ability to build detailed profiles of consumers, predict their preferences, and offer a tailored advertising portfolio.[10] Industry experts tout this as a "win-win": users get more specific ads for products they have a greater responsiveness to, while businesses achieve higher brand awareness and increase the likelihood that they will sell a product.[11] This has been reflected in the growth of advertising revenues by large digital and social media companies. Google, for example, generates a substantial amount

[10] Veronica Marotta, Kaify Zhang & Alessandro Acquisti, *Who Benefits from Targeted Advertising*, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00037-100312.pdf
[11] *Id.*

of its revenue through its Google Ads platform, a total of $160.74 billion dollars and almost seventy-one percent of revenues in the most recent fiscal period.[12] Similarly, Facebook earned nearly $40 billion from advertising revenues in 2017, which accounted for nearly eighty-five percent of total revenues.[13] It is estimated that Facebook earns $84 from each North American user and $27 from each of its European users. [14] This difference in earnings is likely due to the stringent data protection laws Europe has put in place in recent years.[15]

Clearly, targeted advertising is a profitable business for corporations. But how do corporations translate site clicks into revenue? This is usually through something called a "cookie." Cookies, unrelated to the dessert, are the software codes that enable much of the sophisticated digital advertising and online user experience that occurs today.[16] When a cookie passes between the user's computer and network server, the server reads the unique identifier and is able to tailor information specifically to the user. [17] While there are several different types of cookies, the one most relevant to this comment is the HTTP cookie. [18] These are cookies used specifically to identify particular users and manage the overall online experience. [19] HTTP cookies allow websites to remember a user's profile, log in, shopping carts, and many more facets that make a consumer's life significantly easier on the day-to-day basis. [20] These sites

---

[12] *All you need to know about Third-Party cookies*, COOKIE SCRIPT, https://cookie-script.com/all-you-need-to-know-about-third-party-cookies.html#:~:text=Third%2Dparty%20cookies%20are%20cookies,see%20which%20websites%20he%20visited.
[13] Brian O'Connell, *How Does Facebook Make Money? Six Primary Revenue Streams*, THE STREET (Oct. 23, 2018), https://www.thestreet.com/technology/how-does-facebook-make-money-14754098.
[14] *Id.*
[15] Angela Chen, *Websites are (probably) making less money because of GDPR*, MIT TECHNOLOGY REVIEW, https://www.technologyreview.com/2019/07/24/134067/gdpr-privacy-revenue-economics-online-business-legislation/#:~:text=It's%20the%20first%20study%20of,into%20effect%20in%20May%202018.&text=The%20data%20showed%20that%20recorded,week%20for%20the%20median%20site.
[16] *Cookies: What you need to know and how they work*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/cookies.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

create cookies, which are stored on a user's web browser, to identify when a user visits a new website and direct what data to record.[21] If a user returns to that site later, the browser returns an "identifier" with data from previous sessions.[22]

Cookies can be defined by which party installs them.[23] First-party cookies are set by the website directly visited by the user, and the data collected is used for calculating page views and the number of users.[24] This data can later be shared with advertisers for targeted advertising purposes.[25] Third-party cookies are set by entities not directly visited by the user, notably when the target websites add third-party elements on their site.[26] Once installed on a user's browser, these cookies track and save user's information for ad targeting and behavioral advertising.[27] The classic example of the third-party cookie is the Facebook "Like" button, which will insert a cookie into the user's computer which Facebook then accesses to identify the user and his or her browsing history.[28]

Cookies can also be labelled based on when they expire.[29] Session cookies are cookies that expire immediately or a few seconds after a user leaves a web browser.[30] They are most often used by e-commerce websites to remember a user's shopping cart and keep them logged in during their session, but expire once the user closes out of the browser.[31] If a website did not use session cookies, items would not remain in a virtual shopping cart until the user got to the checkout page.[32] Persistent cookies, meanwhile, stay on the user's browser for an extended

---

[21] Cookies, *supra* note 16.
[22] *Id.*
[23] Rashmita Behera, *What are Cookies? Different Types of Web Cookies, Explained*, ADPUSHUP (July 1, 2020), https://www.adpushup.com/blog/types-of-cookies/
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Behera, *supra* note 23.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*

period of time and will be stored on the browser until their expiry date or the user deletes them.[33] These are typically used by publishers to track a single user and his or her interactions with their website. [34] While on the positive side, they enable persistent shopping carts, which maintain products in a cart even after a session has ended, they are also the software code used most often to track user's browsing history. [35]

There are some major drawbacks to this kind of immersive experience. The most important and obvious is privacy.[36] Through cookies, unknown marketers are able to collect identifiable personal data about a particular user and leverage it for financial gain. [37] Additionally, cookies pose a security risk, as outside parties can access highly confidential information like home address and credit card information if the data is stored on the user's browser. [38] For example, bad actors are now running pop-ups that can "scrape" a cookie, copying code from the browser's cookie and logging into the targeted site.[39] Auto-fill information can easily be accessed through these means as well. [40] Notably, Yahoo had a major data breach in 2015 and 2016 where hackers used a similar process to bypass the login and password process for at least some of the 500 million Yahoo mail accounts breached.[41] Finally, while companies argue that these cookies can be disabled, many users are not technologically adept to figure out how to do so, particularly when browsers are making it increasingly difficult to disable them.[42]

---

[33] *Use Of Cookies*, SCIENTIFIC AMERICAN, https://www.scientificamerican.com/page/use-of-cookies/.
[34] *Id*.
[35] *Id*.
[36] *The Pros and Cons of Third-Party Cookies*, REQ ANALYTICS, https://req.co/insights/article/pros-and-cons-third-party-cookies.
[37] *Id*.
[38] *Id*.
[39] Erik Bajaras, *Cookie scraping: How data thieves could steal your personal information online*, ABC (Nov. 1, 2018), https://abc13.com/cookie-scraping-what-are-internet-cookies-computer-cookies-security/4600107/.
[40] *Id*.
[41] Alyssa Newcomb, *What Is a Forged Cookie and How Did it Allow Hackers to Get Into My Yahoo Account?*, NBCNEWS (Feb. 16, 2017), https://www.nbcnews.com/storyline/hacking-in-america/what-forged-cookie-how-did-it-allow-hackers-get-my-n721866.
[42] REQ ANALYTICS, *supra* note 36.

While this comment focuses primarily on the negative impact cookies have had on digital privacy, cookies have also been integral to a cohesive digital experience. [43] Cookies are used to streamline much of what consumers do. How many times has one closed out of a page, only to open it back up with their login information still stored or shopping cart still intact? While there are downsides of this technology related to internet privacy, cookies vastly improve the browsing experience in several ways, including:

- Session Management: Allows websites to recognize users and recall unique preferences, such as the type of news or login information;[44]
- Personalization: Cookies use unique data to build targeted advertisements so that users are looking at products they have a greater interest in;[45]
- Tracking: Cookies track previously viewed items, allowing sites to suggest similar goods and keep selected items in a user's online shopping cart.[46]

These increasingly sophisticated tools clearly possess great advantages for which there is no clear substitute. Therefore, the key is to find a way to balance these invaluable benefits with the negative impact on consumer's data privacy, which will be discussed in greater detail below.

Part II: The Statutes

There are two key pieces of legislation that are the subject of this comment. This first is the original Wiretap Act, formally called Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[47] The second is the Electronic Communications Privacy Act of 1986 ("ECPA").[48] The original Wiretap Act passed following extensive reviews, hearings, and vetting by Congress

[43] Behera, *supra* note 23.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq. (1968).
[48] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et. seq. (1986).

and various stakeholders in 1967, while the ECPA passed with far less input due to the lack of public awareness or advocacy groups.[49]

Before the passage of the ECPA, the original Wiretap Act protected only wire and oral communications, and provided considerable statutory limitations on their abuse.[50] The ECPA was passed to provide greater protection to electronic communications and additional clarity on federal privacy protections.[51] It includes three federal statutes: the Act, which amended the original Wiretap Act,[52] the Stored Communications Act, which provides protections for stored wire and electronic communications,[53] and the Pen Register Statute, which covers pen registers.[54]

In addition to the Act, plaintiffs in recent years have brought suit for invasive data monitoring practices under the Stored Communications Act ("SCA"), which protects files stored by service providers and records held about the user by the service provider, such as his or her name or IP address.[55] However, litigants who have tried to bring suit under the SCA for these practices have generally been unsuccessful.[56] Courts have typically held that the legislation more properly encompasses network service providers[57] or centralized data management entities,[58] as opposed to web browsers, and have declined to adopt a broad reading of the SCA.

The Act, as it stands now, prohibits the "interception" of oral, wire, or electronic communications.[59] Notably, the Act provides a private right of action against private entities

---

[49] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 74 (2004).
[50] Dorothy Higdon Murphy, *United States v. Councilman and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?*, 6 N.C. J.L. & TECH. 437, 443 (2005).
[51] *Id.*
[52] 18 U.S.C. §§ 2510–22.
[53] *Id.* §§ 2701–10.
[54] *Id.* §§ 3121–27.
[55] *Id.* §§ 2701–12.
[56] *See infra* notes 56–57.
[57] *Google*, 806 F.3d at 146.
[58] *Facebook*, 956 F.3d 609–10.
[59] 18 U.S.C. § 2510 et seq.

and government actors.[60] This stands in contrast to the Fourth Amendment, which serves to regulate only federal, state, and local actors in the course of criminal investigations.[61] An electronic communication is defined in part as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[62]

If a plaintiff brings a claim under Title I of the ECPA, he or she must show that "a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." [63] If a plaintiff proves all of these elements, a defendant may argue that his or her interception was lawful under one of the listed exceptions.

An interception is the "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."[64] Congress carved out a spaces for "provider[s] of electronic communications services" who "may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain." [65] This is known as the "ordinary course of business exception," and it balances individual privacy with business development of the telecommunications industry, which could otherwise be liable for unintended interceptions. [66] The Act also provides that an interception will not be unlawful for a person acting "under color of law … where such person is a *party* to the communication or one of the parties to the

---

[60] *Id.* § 2520.
[61] United States v. DiTomasso, 81 F. Supp. 3d 304, 308 (S.D.N.Y. 2015).
[62] *Id.* § 2510(12).
[63] In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 22 (1st Cir. 2003).
[64] 18 U.S.C. § 2510(4).
[65] Helen Jazzar, *Bringing an End to the Wiretap Act as Data Privacy Legislation*, 70 CASE W. RES. L. REV. 457, 461 (2019).
[66] *Id.*

communication has *given prior consent* to such interception."[67] These are now commonly known as the "party" exception and the "consent" exception to liability under the Act. Companies which fall under these exceptions can intercept communications lawfully.

Although the party exception is the focus of this comment, as it has recently been claimed by companies hoping to shield themselves from liability under the Act,[68] the consent exception has also been a central focus of privacy litigation. The legislation requires only one party to consent to the interception for the provider to be immune from liability.[69] Pragmatically, user consent would be the easiest for companies to obtain, either through formal user agreements or terms and conditions that a user must explicitly consent to prior to using a company's services. Many companies have a separate privacy and cookie policy to address this issue,[70] and others have taken to generating boilerplate cookie policies for companies looking to protect themselves.[71] And while there has been a fair amount of litigation surrounding the content, reasonableness, and distribution of consent agreements, [72] almost all companies do have language surrounding monitoring content or cookies in their terms and conditions. Alternatively, companies have installed "pop-up" windows notifying users that the site they are trying to access uses cookies, and he or she must accept this practice in order to view the site's contents.

However, the question of whether the site's tracking exceeds this agreement is often nuanced. The trier of fact will have to determine if the intercepted communication exceeds the plaintiff's express consent, and if so, to what degree.[73] This is a highly fact-specific inquiry, a classic example of which occurred in *In Re Yahoo Mail Litigation* ("Yahoo"), where the

---

[67] *Id.* § 2511(2)(c) (emphasis added).
[68] *See generally Google*, 806 F.3d 125; *Facebook*, 956 F.3d 589.
[69] 18 U.S.C. § 2511(2)(d).
[70] *See Cookie Policy*, MCKINSEY, https://www.mckinsey.com/cookie-policy#; *Cookies and similar technology*, ACCENTURE, https://www.accenture.com/us-en/support/company-cookies-similar-technology.
[71] *See Free Cookies Policy Generator*, PRIVACY POLICIES, https://www.privacypolicies.com/cookies-policy-generator/
[72] In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014).
[73] Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983).

Northern District of California adopted a "reasonable user" standard in determining whether Yahoo obtained consent.[74] In establishing that accepting Yahoo's terms of service provided explicit consent, the court noted that the contract acknowledged its cookie and data monitoring practice in clear language. By agreeing to the terms of service, the plaintiffs therefore consented to the conduct. The *Yahoo* case demonstrates the uphill battle plaintiffs can face when arguing that they did not consent to the companies' conduct, a battle that continues to be fought as data harvesting practices have only increased.

Ultimately, while the authors of the original Wiretap Act, and its amendments, could not have possibly anticipated these exact usages in the twenty-first century, courts have spent considerable time analyzing them in light of new and invasive technological developments.

Part III: New Cases

This section will discuss the *Google* and *Facebook* cases that have created a circuit split on the party exception to the Act. In recent years, as cookies have become increasingly prevalent, companies have found themselves on the receiving end of litigation challenging their invasive data harvesting strategies.[75] Two cases out of the Third and Ninth Circuits have heightened the inter-circuit divide, largely because they both concern a similar issue surrounding the unauthorized duplication of "GET" requests.

A GET request is an HTTP, or Hypertext Transfer Protocol, request technique that retrieves whatever information or data is requested from a particular source, likely a browser, to the server it is attempting to access on behalf of a user.[76] Third-party cookies placed on internet browsers use these GET requests to determine what web sites a user is visiting, and advertising

---

[74] In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014).
[75] *See generally* Mount v. PulsePoint, Inc., 684 F. App'x 32 (2d Cir. 2017); Stokes v. Price, 2020 U.S. Dist. LEXIS 194032 (D.N.J. Oct. 20, 2020); Zak v. Bose Corp, 2020 U.S. Dist. LEXIS 96753 (N.D. Ill. May 27, 2020).
[76] *GET – What is the GET Method*, LAST CALL: THE RAPID API BLOG, https://rapidapi.com/blog/api-glossary/get/; *see also HTTP Requests*, CODE ACADEMY, https://www.codecademy.com/articles/http-requests.

companies can then use the results to create targeted advertisements that companies will pay to feature on their site.[77]

Though both courts consider unauthorized duplication of GET requests to be an interception, the Ninth Circuit (the "Facebook" court) has held that the party exception does not apply, but the Third Circuit (the "Google" court) considers the third party companies to be parties within the exception.[78] Therefore, the Third Circuit has held that such interceptions are lawful,[79] while the Ninth Circuit has held that they are unlawful, and the companies using such practices are therefore not shielded from liability under the Act.[80]

Google was the first circuit case to consider the unauthorized duplication of GET requests in the context of the Wiretap Act. A report in February 2012 exposed Google and other defendants' practice of exploiting loopholes in Safari and Internet Explorer's cookie blocker software.[81] A covert form placed on websites with Google's advertisements triggered an exception to the browsers' cookie blockers and allowed the defendants to place cookies on the browser.[82] This violated Google's specific assurances to visitors that Safari's default settings, which blocked cookies from third parties and advertisers, would remain intact.[83] Plaintiffs filed a putative class action asserting claims under the Act and other federal laws, in addition to various state law claims. [84]

---

[77] *Online Tracking*, FEDERAL TRADE COMMISSION (June 2016), https://www.consumer.ftc.gov/articles/0042-online-tracking.
[78] *See infra* Section III.
[79] *Google*, 806 F.3d at 142–43.
[80] *Facebook*, 956 F.3d at 608.
[81] Jonathan Mayer, *Safari Trackers*, Web Policy Blog (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/.
[82] *Google*, 806 F.3d at 131–32.
[83] *Id.*
[84] *Id.* at 133.

The Third Circuit first considered routing information to be "content" under the Wiretap Act, and adopted the position of the Surveillance Court[85] that queried URLs can contain both routing and content information.[86] The Third Circuit explained that "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's [i]nternet activity."[87] The Third Circuit then considered the defendants' argument that they were the intended recipients, and therefore a party under the "party exception." [88]

The court first reviewed the plaintiff's complaint, which details a process in which defendants allegedly intercepted the communication between the user's browser and first-party website which the user was accessing.[89] Crucially, the complaint alleged that:

> "[u]pon receiving a []GET[] request from a user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, instructing the browser to send a []GET[] request to the third-party company charged with serving the advertisements for that particular webpage.' As to Google specifically, the complaint likewise pleads that 'the server hosting the publisher's webpage . . . instructs the user's web browser to send a GET request to Google to display the relevant advertising information for the space on the page for which Google has agreed to sell display advertisements."[90]

Therefore, the issue was twofold: because of the cookie Google inserted in the user's browser, the website the user accessed would send a GET request to a third-party advertising company, and the browser would duplicate the user's initial GET request and send it to Google for advertising purposes.[91]

---

[85] The Foreign Intelligence Surveillance Court provides "judicial oversight of Intelligence Community activities in a classified setting." *Foreign Intelligence Surveillance Court*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/surveillance/fisa/fisc/.
[86] *Google*, 806 F.3d at 138.
[87] *Id.* (quoting United States v. Forrester, 512 F.3d 500, 510 n.6 (9th Cir. 2008)).
[88] *Id.* at 140.
[89] *Id.*
[90] *Id.*
[91] *Id.*

The Third Circuit reasoned that the users' browsers are directly communicating with defendants regarding accessing a website, and that therefore the defendants are not obtaining the GET requests from transmissions "to which they are not a party."[92] This indicates the underlying view that, regardless of what Google does with the GET requests or whether the user intended that his information be used for advertising purposes, if the user employed the browser with the modified data to access his intended site, then Google was a "party" to the communication.

This seems particularly surprising considering that users did not even consent to this modified code exploiting a loophole in the browser's cookie blocker. The Third Circuit stated that, although it was troubled by the defendants' covert circumvention of the cookie blocker, it does not affect whether an entity falls under the "party exception."[93] Looking to cases from the 1960s, it reasoned that a wiretapping statute would likely allow for a party to surreptitiously participate in a conversation.[94] The Third Circuit continued in this vein by noting that the defendants acquired the information in the "ordinary course," implying that the court interpreted this duplication as a natural result of the user using Google to access a separate web site. [95] It concluded that the plaintiffs' browsers sent the GET requests directly to the defendant's servers, and were therefore the intended recipients of the transmissions.[96] Because of this, they fell under the party exception of the Act and the interception was lawful.[97]

The Ninth Circuit, however, took the opposite approach. In *Facebook*, plaintiffs brought suit against Facebook's practice of tracking user's browsing histories and compiling them into profiles which would be sold to advertisers.[98] Facebook did not dispute that it engaged in this

---

[92] *Google*, 806 F.3d at 140–41.
[93] *Id.* at 143.
[94] *Id.*
[95] *Id.* at 141.
[96] *Id.* at 142–43.
[97] *Google*, 806 F.3d at 142–43.
[98] *Facebook*, 956 F.3d at 589, 596.

practice, even after users logged out of the site. The company did this through embedding third-party plug-ins, such as the Facebook "Like" button, on third-party websites.[99] These plug-ins contain pieces of Facebook code that were able to replicate and transmit the user's GET requests to Facebook without the user knowing.[100] Facebook collected the user's URL and the third-party page's Internet Protocol ("IP") address.[101] While Facebook executives were aware of the tracking of logged-out users, they stopped this practice only after a blogger published an expose.[102]

Plaintiffs then filed a putative class action, alleging various federal and state causes of action, including claims under the Act and Stored Communications Act.[103] Like the defendants in *Google*, Facebook also claimed that it was acting under the protection of the party exception.[104] The Ninth Circuit specifically noted Facebook's variation on the normal process of using a GET request to transmit the referer header, containing the URL with personally identifiable information, from the browser to the webpage. Crucially, on sites with the Facebook plug-in, the code "directs the user's browser to copy the referer header from the GET request and *then send a separate but identical GET request* and its associated referer header to Facebook's server."[105]

The court continued that the First and Seventh Circuit held that the party exception would not shield entities from liability for the unauthorized duplication of communications, in the software and email context, respectively.[106] The court also noted the factual similarity to *Google* and its contrary ruling before ultimately adopting the reasoning of the First and Seventh

---

[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.* at 596–97.
[103] *Id.* at 597.
[104] *Facebook*, 956 F.3d at 607.
[105] *Id.*(emphasis added).
[106] *Id.*; *see Pharmatrak*, 329 F.3d at 22, United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010).

Circuits.[107] In doing so, the court considered the legislative intent of the Act, which is ultimately to protect communication privacy and the desire to prevent unauthorized third parties from accessing the contents of the communication.[108] It also recognized that a contrary ruling in line with *Google* would "[allow] the exception to swallow the rule" by permitting a wide variety of intrusions.[109] Therefore, Facebook was not shielded from liability under the party exception to the rule.[110] Facebook's petition for rehearing was denied by the full Ninth Circuit, indicating that the court did not consider the inter-circuit split to be of "exceptional importance" such that it needed to be heard en banc.[111]

A. How did the Courts Diverge?

With largely analogous facts and a similar process of obtaining user's information, Google and Facebook experienced different outcomes based on how different circuit courts interpreted the party exception. While both courts considered their inquiries to be highly fact-specific, the Third Circuit based its reasoning almost entirely on the process alleged in the complaint and the plain meaning of the "party" exception.[112] The most obvious example of this was when the court noted that, because the *browser* was the entity accessing the GET request and covertly duplicating it, and the user accessed the third-party site, then the browser is a party to the communication.[113]

In coming to this conclusion, the Third Circuit relied on older cases from the Fifth,[114] Sixth,[115] and Seventh[116] Circuits which together hold that "one who impersonates the intended

---

[107] *Id.* at 608.
[108] *Id.*
[109] *Id.*
[110] *Facebook*, 956 F.3d at 608.
[111] Fed. R. Civ. P. 35.
[112] *Google*, 806 F.3d at 140–46.
[113] *Id.* at 140–141.
[114] United States v. Campagnuolo, 592 F.2d 852, 863 (5th Cir. 1979).
[115] Clemons v. Waller, 82 Fed. App'x 436, 442 (6th Cir. 2003).
[116] United States v. Pasha, 332 F.2d 193, 198 (7th Cir. 1964).

receiver of a communication may still be a party to that communication for the purposes of the federal wiretap statute and that such conduct is not proscribed by the statute."[117] These cases were decided prior to the passage of the ECPA and concerned wire and oral communications where law enforcement aimed to shield its conduct from liability under the party exception.

The Ninth Circuit relied less on a "textualist" reading of what it means to be a party, and instead considered the overall intent of the Act, which is to prevent duplicitous access to communications.[118] It also seemed concerned with the power the party exception could have over future electronic transmissions if it interpreted the legislation similar to the *Google* court, since this could open the gates for significantly more unauthorized access to these communications. Finally, the court primarily relied on newer cases concerning electronic communications,[119] as opposed to earlier cases that dealt with wire communications, in coming to its conclusion. With this reading, it seems clear that the unauthorized duplication of GET requests and transmission to a third-party advertiser would not shield an entity from liability under the party exception, regardless of whether the user knowingly used the entity's services for a different purpose.

The Ninth Circuit decision is not entirely unprecedented. In 2014, the court held that Google's Street View cars, which were collecting personal data like emails, videos, and documents over unencrypted Wi-Fi networks, could be held liable for an interception under the Wiretap Act.[120] Google attempted to shield itself from liability by arguing that it was exempt from liability under the "general public" exception,[121] which exempts radio communication interceptions by any station "for use of the general public."[122] The court adopted a broad

---

[117] *Google*, 806 F.3d at 144 (quoting *Clemons*, 82 Fed. App'x at 442).
[118] *Facebook*, 956 F.3d at 608.
[119] *Pharmatrak*, 329 F.3d at 22, *Szymuszkiewicz*, 622 F.3d at 706.
[120] Joffe v. Google, Inc., 729 F.3d 1262, 1264 (9th Cir. 2014).
[121] *Id.* at 1266.
[122] 18 U.S.C. § 2511(2)(g)(ii)(I) – (IV).

reading of the exception, but ultimately concluded that "radio communication" does not encompass the type of data Google was collecting.[123] In doing so, the court considered the exception in the context of the remainder of the legislation, congressional intent, and the common sense meaning of the word "radio."[124] While the exception was not the one claimed in *Facebook*, the case offers an interesting lens into how the circuit interpreted the Act that provided a similar framework to what was applied in *Facebook*.[125]

While both the *Google* and *Facebook* decisions relied on interpreting prior circuit decisions in light of a changing landscape, such divergent opinions will ultimately create massive confusion for internet sites and users alike. Therefore, the United States must have a unified philosophy to address these practices.

Part V: Recommendations

The recommendations of this comment are categorized into three buckets. While the first focuses on judicial solutions, namely in interpreting the Act, the second and third center on external and legislative solutions, looking to the European Union's recently passed data privacy legislation (GDPR), and on actions that the general public should take in putting public pressure on search browsers and internet companies.

A. Judicial Interpretation

The most straightforward judicial solution is to interpret the Act to narrow the definition of "party" to entities that are the intended recipient for the reasonably intended use. A court could generally ascertain the understanding of all parties from terms and conditions, statements of consent, and the reasonableness of the user's respective beliefs as to the privacy of their communications. In *Google*, this analysis centered on the court's careful reading of the

[123] *Joffe*, 729 F.3d at 1267–68.
[124] *Id.* at 1267–77.
[125] *See generally Facebook*, 956 F.3d 589.

Plaintiff's complaint and how the technology worked, ultimately concluding that the "direct transmissions" between plaintiffs and defendants, regardless of the intentions behind the transmissions, were enough to establish that defendants were parties to the communications.[126] Similarly, in *Facebook*, this analysis centered on the technical context of the allegations and congressional intent in holding that Facebook was not a "party" to the communication as it pertained to the unknown duplication of GET requests.[127]

This comment strongly advocates for a broad adoption of the position of the Ninth Circuit, building on First[128] and Seventh[129] Circuit decisions, which held that, regardless of the recipient intended by the party sending out the communication, "simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception."[130] Companies would therefore have to obtain approval from the initial user for both transmitting the GET request to the server and for duplicating this request and communicating it to other companies and advertising agencies. The Third Circuit's interpretation had to rely on older cases that did not take into account the ECPA's amendments, and in particular on *United States v. Pasha*, where the plaintiffs did not bring a cause of action under the Act and the intercepting party was a law enforcement officer.[131] Crucially, even when focusing on the scope of the word "intercept," the Third Circuit did not focus on, or even consider, the difference between the needs of a law enforcement officer, operating in the scope of his duties, and a private company looking to harvest user's data for profit.

Additionally, *Pasha* did not discuss the Act's exceptions at all, but rather whether the communication was "intercepted" to begin with, and therefore has limited applicability to cases

---

[126] *Google*, 806 F.3d at 141.
[127] *Facebook*, 956 F.3d at 608.
[128] *Pharmatrak*, 329 F.3d 9 at 22.
[129] *Szymuszkiewicz*, 622 F.3d at 701.
[130] *Facebook*, 956 F.3d at 608.
[131] *Pasha*, 332 F.2d at 198.

where often times the fact that a communication was "intercepted" is not disputed.[132] While Congress likely could not have predicted these practices in 1986, a closer inspection would have likely led the Third Circuit to an interpretation of the Act more in line with the Ninth Circuit's, largely because the *Facebook* court's cited cases all dealt with electronic interceptions by private entities. Interpreting the party exception such that the users must know and intend, not only the recipient, but what the recipient plans to do with the user's data, is additionally in line with the high standard of data privacy in the European Union.[133]

Critics of this approach will likely have several counterarguments. First, this would result in a broad expansion of the protections granted by the Act, since now an entity could only be considered a party if it was both privy to the communication and the user consented to any of the entity's transmissions related to this initial communication. As the Third Circuit decision notes, this would add an additional qualifier to the definition of "party." It could also seem duplicative when read in tandem with the consent exception, which permits an interception where prior consent had been given.[134] Yet the plain language of the consent exception only concerns the initial interception, not how the entity uses the information extracted from this interception.[135]

Therefore, interpreting legislation should be done in light of the rapidly evolving technological landscape. In this case, the legislative intent of both the Act and ECPA. The Act was enacted to balance the increased need for information privacy with the demands of law enforcement, and the ECPA augmented this because there was growing concern regarding the

---

[132] *Id.*
[133] *What is GDPR, the EU's new data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/; *see infra* Part V.C.
[134] 18 U.S.C. § (2)(c).
[135] *Id.*

issues raised by new digital technologies.[136] While legislative history does not provide ironclad authority when considering differing statutory interpretations, both the Third and Ninth Circuit relied on it in their holdings. If one takes into account the historical context and intent behind passage of the legislation, the Ninth Circuit's interpretation of the Act and ECPA is much closer to the original congressional intent.

Second, the Ninth Circuit's decision goes against existing precedent. In addition to differing from *Google*, *Facebook* arguably is in tension with the Ninth Circuit's previous decision in *Konop v. Hawaiian Airlines*.[137] While the technology at issue in *Konop* was different than the GET request duplication in *Google* and *Facebook*, the case posed a similar question of whether unauthorized access to a password protected website constituted an "interception" under the Wiretap Act.[138] While the court did not delve into the party exception, it applied a narrow definition of interception to electronic communications and held that they must be acquired during transmission, without taking into account the unauthorized access to the original communication.[139] Although this goes to the "interception" element of proving a prima facie case under the Act, it still implies that whether an entity's conduct is unlawful does not turn on whether the access or transmission of user data was authorized. The *Facebook* court distinguished this by noting that *Konop* concerned "items viewed on a private website," as opposed to external plug-ins that covertly duplicated and transmitted GET requests.[140]

B. External Solutions

---

[136] *ECPA Reform and the Revolution in Cloud Computing: Hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee on the Judiciary, House of Representatives*, 111th Cong. 2 (2010) ("ECPA was enacted into law in 1986 to address the issues being raised by new digital technologies.").
[137] Konop v. Hawaiian Airlines, 302 F.3d 868, 872 (9th Cir. 2002).
[138] *Id.* at 872–76.
[139] *Id.* at 878-79.
[140] *Facebook*, 956 F.3d at 608 n.9.

A second, external solution is to pressure social media and web browsing companies to begin phasing cookies out of their search engines. There is some hope that companies are understanding the negative implications of excessive cookie use and are adjusting their browsing policies accordingly.[141] For example, Google recently announced that it will begin a two-year process of phasing cookies out of its Chrome web browser.[142] The company has also proposed data monitoring technology that would be less invasive than cookies, making it easier to target advertisements to certain demographics without identifying specific people.[143] Google will now join Safari and Firefox, which have taken similar stances against data and internet tracking.[144] This could help with more anonymized tracking. While users would therefore receive slightly less tailored ads, it would be with the knowledge that their specific, identifiable data is not being sold to third parties. Additionally, users could pressure companies to block third-party cookies by default, and users would have to opt into these persistent cookies, a model that has already been adopted by Apple, through its browsing tool Safari, and Firefox. [145]

There is greater variance in how companies handle blocking first-party cookies: some technology companies identify which cookies are used for tracking, and block those by default, some create mandatory expiration dates for third-party persistent cookies, and some simply do not block them by default. [146] Users could use similar public pressure to achieve uniformity between various companies in a way that balances the legitimate functions of first-party cookies with a greater emphasis on user privacy.

---

[141] *See infra* notes 142, 144.
[142] Dieter Bohn, *Google to 'phase out' third-party cookies in Chrome, but not for two years*, THE VERGE (Jan. 14, 2020), https://www.theverge.com/2020/1/14/21064698/google-third-party-cookies-chrome-two-years-privacy-safari-firefox.
[143] *Id.*
[144] Michael Wlosik, *How Different Browsers Handle First-Party and Third-Party Cookies*, CLEARCODE, https://clearcode.cc/blog/browsers-first-third-party-cookies/.
[145] *Id.*
[146] *Id.*

Google has countered this narrative by surprisingly stating that blocking cookies is bad for privacy, as it will lead companies to engage in even more invasive practices such as "fingerprinting."[147] This technique allows a site to build a unique "fingerprint" to identify a user's browser based on features such as the browser version, screen size, and fonts installed.[148] However, other privacy advocates, including Jonathan Mayer, who authored the original expose about Google's surveillance practices, have strongly opposed Google's argument, calling it "privacy gaslighting."[149] They continued that it was a defeatist approach, because it was attempting to persuade users that "an obvious privacy protection—already adopted by Google's competitors—isn't actually a privacy protection."[150] They additionally stated that there has been little evidence to suggest the superior value of targeted advertising, noting that when the New York Times did not experience a decrease in advertising revenue after shifting to contextual and geographic ads.[151]

Google has also argued that increased data privacy measures would reduce funding for advertising agencies and web site publishers, "jeopardiz[ing] the future of the vibrant web."[152] However, while this business practice is profitable, Google's argument that these profits should be placed above protecting user privacy implies that the company knows more about what makes a "vibrant web" than users.

C. Legislative Solutions

In crafting a legislative solution, United States legislators could take inspiration from the efforts being made in the European Union to combat the impacts on data privacy. The level of

---

[147] Justin Schuh, *Building a more private web*, GOOGLE: THE KEYWORD (Aug. 22, 2019), https://www.blog.google/products/chrome/building-a-more-private-web/.
[148] *Id*.
[149] Jonathan Mayer and Arvind Narayanan, *Deconstructing Google's excuses on tracking protection, Freedom to Tinker* (Aug. 23, 2019), https://freedom-to-tinker.com/2019/08/23/deconstructing-googles-excuses-on-tracking-protection/.
[150] *Id*.
[151] *Id*.
[152] *Id*.

consent advocated for in this paper is not unprecedented on the global stage, as it is mirrored by the protections offered in the General Data Protection Regulation ("GDPR"), including requiring a user's explicit consent before an entity can track his or her web site habits.[153] The GDPR, which passed the European Parliament in 2016, replaced the European Union Data Protection Directive, which already provided people living in the European Union with the highest level of data protection in the world.[154] The European Union Data Protection Directive, which created minimum data privacy and security standards, was consistently updated based on a constantly morphing technological landscape.[155] However, the GDPR augments these protections in a few key ways.

First, it now applies to companies that are not based in the European Union, in addition to those that are, if they offer goods or services, or monitor the behavior, for people in the EU for example through offering goods in an EU currency or using an EU national language in the course of doing business.[156] Additionally, the GDPR raised the minimum level of consent a user must provide to a company for online advertising.[157] It is currently defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[158] Crucially, consent must be given by affirmative action such that a user would have to opt-in to online advertising, as opposed to under previous laws, which many interpreted as an "opt-out" model of consent.[159] Finally, if a company previous obtained a user's

---

[153] *What is GDPR, supra* note 133.
[154] *How the GDPR Impacts Online Advertising*, TERMSFEED (May 23, 2019), https://www.termsfeed.com/blog/gdpr-online-advertising/.
[155] *What is GDPR,, supra* note 133.
[156] *How the GDPR Impacts Online Advertising*, *supra* note 154.
[157] *Id.*
[158] 2016 O.J. (L. 119) 34.
[159] *Id.*

consent in a way which was not compliant with the GDPR, the company would have to remove that user from their marketing emails or re-request consent.

A recent study found that only twenty percent of businesses believed they were GDPR compliant after the May 25, 2018 compliance deadline had passed, while fifty-three percent were still implementing these policies and twenty-seven percent had yet to start implementation.[160] While these figures clearly demonstrate progress, they also show that the process of improving data privacy protections for companies is lengthy.

Regardless, the United States should look to adopt similar legislation surrounding data privacy and protection. Of course, the differing governing systems will likely make this less likely in the United States on a federal level. California has passed privacy legislation that provides stricter limits on personal data that can be shared. Under the CCPA, California residents can ask businesses to turn over any personal information that the business has on them and how they use that information.[161] Residents also have the right to be notified before or after businesses collect their personal information and can request that businesses stop selling their personal information (the "opt-out" model).[162] While this is not as comprehensive as the GDPR's "opt-in" model, it still offers more protection than any federal legislation at this point. Additionally, California Proposition 24, which passed in the November 2020 election, further enhances data privacy laws, namely by (1) prohibiting businesses from sharing personal information and (2) correcting false personal information.[163] However, comprehensive federal data privacy legislation did not pass on the federal level in 2019 or 2020.[164]

---

[160] *GDPR Compliance Status*, TRUSTARC (July 2018).
[161] *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa (Office of the Attorney General).
[162] *Id*.
[163] *2020 Consumer Data Privacy Protection*, National Conference of State Legislatures, https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx; Cameron F. Kerry and Caitlin Chin, *By passing Proposition 24, California voters up the ante on federal privacy law*, BROOKINGS (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/.
[164] *Id*.

There are a few critiques of the GDPR that also surround similar legislation people aim to enact in the United States. First, it is likely to increase the cost of certain services that consumers now access for free, because they compensate for these services by providing their browsing information.[165] However, a clear counterargument is that companies can simply provide the option to consumers, as opposed to removing their agency entirely. A second critique once again centers on less targeted advertisements, or ads with a "looser fit" than the extremely narrowly tailored ads users often experience today, and often sharing the data enhances the experience for the user.[166] Once again, this argument minimizes the lack of agency users have in determining whether their private information is shared or not. As seen in this comment, the harvesting of their search habits and browsing histories is often done without their consent or understanding.

D. Amending the Wiretap Act

More narrowly, the United States could look to amend the Act to add additional clarity surrounding the party exception. This is not unprecedented, as the ECPA was an amendment to the Act extending its protections beyond wire and oral communications to electronic communications as well, in response to growing concern among legislators that these communications were not adequately protected.[167] Similarly, as the bounds of technology expand, Congress should look to provide additional protections in light of the original purpose of the legislation, which was to promote private citizen's privacy expectations in balance with the needs of law enforcement.[168] Even as early as the early 2000s, circuit courts were acknowledging that because "the ECPA was written prior to the advent of the Internet and the

---

[165] Niam Yaraghi, *A case against the General Data Protection Regulation*, BROOKINGS (June 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/.
[166] *Id*.
[167] Dorothy Higdon Murphy, *United States v. Councilman and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?*, 6 N.C. J. L. & TECH. 437, 443 (2005).
[168] Electronic Communications Privacy Act (ECPA), ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/ecpa/#:~:text=Introduction%20to%20ECPA&text=It%20was%20enacted%20to%20create,personal%20information%20would%20remain%20safe.

World Wide Web … the existing statutory framework is ill-suited to address modern forms of communication… ."[169] Since its original passage, there have been no substantive changes to the Act or ECPA in terms of its fundamental pillars or the party or consent exceptions.[170]

An amendment to the existing Act could be as simple as defining "party" in the Wiretap Act to fall in line with the holdings from the First, Seventh, and Ninth Circuits, and defining "consent" in line with the stringent GDPR definition. Any amendment could include language requiring the initial user have knowledge of what the parties would use the transmission for, or consenting to distributing any information to third parties.

In a 2010 congressional hearing on amending the ECPA, Richard Salgado, the senior counsel of law enforcement and information security at Google, noted that "[he has] seen large gaps grow between the technological assumptions of that earlier era and the reality of how electronic communication works today."[171] As a result, several technology companies created a coalition to support "common sense" amendments to the ECPA.[172] While most of these centered on balancing government access to data with internet privacy, the amendments demonstrate that technology companies are increasingly aware of the importance users place on privacy protections.[173] Interestingly, just as the ECPA helped create greater public enthusiasm around the creation of new technologies because people felt more secure with their data,[174] strong electronic protections around data privacy could actually be a boon for both websites and advertisers.

---

[169] *Konop*, 302 F.3d at 874.
[170] ECPA Reform, CENTER FOR DEMOCRACY & TECHNOLOGY, https://cdt.org/area-of-focus/government-surveillance/ecpa-reform/.
[171] ECPA Reform, *supra* note 170, at 19–23.
[172] *Id.*
[173] *Id.*
[174] Electronic Communications Privacy Act (ECPA), *supra* note 170.

To summarize, this comment advocates for one of three pathways for reform: a unified judicial interpretation across all circuits in line with the Ninth Circuit's holding in *Facebook*, external solutions like placing pressure on the search engines themselves to install cookie blockers, and legislative solutions such as enacting a domestic version of the GDPR or amending the Wiretap Act. While these solutions all have critiques and counterarguments, they are weaker than the underlying rationale for enacting some iteration of these solutions to ensure a more unified approach that emphasizes data privacy.

Conclusion

It is clear that with the advent of new technology comes the rise of increasingly complicated questions. In this case, these questions center on how to interpret older statutes in light of shifting regulation, rapidly developing electronic infrastructure, and business models that rely on highly personalized data. Since the ECPA has not kept pace with these advances, many times it falls to courts to determine how to best interpret older legislation in light of these issues. The divide that has been created as a result will lead to forum shopping and confusion among both companies and users alike. The common sense reforms, such as the ones proposed above, could help reinstate some of the trust that has been lost between these two groups.