No. 17-17486

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

IN RE: FACEBOOK INTERNET TRACKING LITIGATION

PERRIN AIKENS DAVIS; BRIAN K. LENTZ; CYNTHIA D. QUINN; MATTHEW J. VICKERY,

Plaintiffs-Appellants,

v.

FACEBOOK, INC.,

Defendant-Appellee.

On Appeal from the United States District Court
for the Northern District of California
Case No. 5:12-MD-02314-EJD-NC

Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC) in Support of Plaintiffs-Appellants Urging Reversal

Marc Rotenberg
Alan Butler
Natasha Babazadeh
Sam Lester
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

June 26, 2018

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATUTES

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

INTEREST OF THE AMICUS[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* in cases concerning consumer privacy before the United States Supreme Court and federal appellate courts, including the Ninth Circuit. *See, e.g., Smith v. Facebook, Inc.*, No. 17-16206 (9th Cir. filed Sept. 25, 2017) (arguing that Facebook users do not consent to Facebook's collection of medical data from third-party websites); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3rd Cir. 2016) (arguing that unique persistent identifiers are "personally identifiable information" under the Video Privacy Protection Act); *Fraley v. Batman*, 638 Fed. App'x 594 (9th Cir. 2016) (arguing that Facebook's "Sponsored Stories" settlement was not fair or sufficient for class members); *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013) (arguing that interception of Wi-Fi communications from home networks violated the federal Wiretap Act).

[1] Both parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. Counsel for a party did not author this brief, in whole or in part.

EPIC has been one of the most prominent advocates for user privacy and critic of invasive tracking techniques used to monitor individuals' web browsing activities. In 1997, EPIC conducted the first privacy survey of frequently visited web sites and identified the risk that "cookies" would be used to track Internet users. EPIC, *Surfer Beware: Personal Privacy and the Internet* (1997).[2] Following this groundbreaking report, EPIC conducted additional research and uncovered that the Direct Marketing Association and other industry leaders proposed a "self regulatory" model that failed to protect the privacy of users. *See* EPIC, *Surfer Beware II: Notice is Not Enough* (1998); EPIC, *Surfer Beware III: Privacy Policies without Privacy Protection* (1999); EPIC: *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy* (2000).[3] EPIC also filed the first complaint with the Federal Trade Commission against a company engaged in invasive cookie tracking. *See* Complaint and Request for Injunction, Request for Investigation and for Other Relief, *In re DoubleClick Inc.* (2000).[4]

[2] https://www.epic.org/reports/surfer-beware.html.
[3] *Available at* https://www.epic.org/reports/.
[4] *Available at* https://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

SUMMARY OF ARGUMENT

This case concerns an invasive business practice pursued by one of the largest Internet companies in the world: the use of persistent identifiers, commonly called "cookies," to track the private activity of Internet users. Hidden behind the "Like" button embedded in pages across the Internet, Facebook secretly and surreptitiously builds detailed profiles on users even when they are no longer using the service. Not only are users unaware of Facebook's conduct, they have no meaningful ability to limit the collection of their personal data. This is precisely the type of invasive business practice that privacy laws were enacted to limit.

Users expect that their web browsing history will remain private—no one imagines a marketing executive standing over their shoulder and taking notes as they use the Internet—but the lower court improperly assumed otherwise, a clear error at the motion to dismiss stage. The court also misunderstood the purpose of privacy law, theorizing that users have an obligation to adopt complex, technological measures to assert privacy claims. That is what people do in the absence of law. That is why laws are enacted. The lower court should not have dismissed the statutory and common law claims.

ARGUMENT

Over the last two decades, the persistent tracking of Internet users has grown more sophisticated and more secretive. A technique that was originally developed

to assist users complete purchases on a particular website has been transformed into a method for tagging, tracking, and monitoring people as they move across the network. Even technology experts with access to sophisticated privacy tools lack the ability to limit many of these new tracking techniques. It is unreasonable, unfair, and inefficient to place the burden on the typical Internet user to hide from all of this. Users do not "like" being tracked.[5]

I. Internet users cannot reasonably avoid Facebook's secret, post-log out web tracking practices.

A. "Cookies" no longer serve the interests of users and are now deployed to tag, track, and monitor users across the Internet.

The original purpose of the persistent identifier known as a "magic cookie" (from the UNIX world) or simply "cookie" was to solve the problem that the HTTP protocol, which enabled a connection between a web client and a web server was "stateless," i.e. each connection lacked information about prior connections, including prior actions. For the client or "user," this would have made it virtually impossible to purchase products on a commercial website because the server would

[5] According to a recent survey by the Pew Research Center, "people struggle to understand the nature and scope of the data collected about them. Just 9% believe they have 'a lot of control' over the information that is collected about them." Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, Pew Res. Ctr. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/. Of all the entities, public and private, identified in the Pew survey, U.S. adults express the lowest level of confidence in social media sites.

not link discrete acts. Each time the user returned to the shopping cart it would be empty.

The problem was solved with the cookie. A "cookie" is a "text-only string that gets entered into the memory of your browser." David Whalen, *The Unofficial Cookie FAQ* 1.1 (2002).[6] Cookies were developed in the mid-1990s by Lou Montulli, one of the founding engineers of the web browser Netscape. Paul Bonner, *What Is A Cookie?*, CNET Builder (Nov. 18, 1997);[7] *see also*, Letter from Peter F. Hartley, Global Public Policy Counsel, Netscape, to the Fed. Trade Comm'n (Apr. 16, 1997).[8] *See* Bonner, *supra*. "The purpose of cookies is to help sites overcome the fact that HTTP, the file transfer protocol that drives the Web, is fundamentally stateless, with absolutely no concept of sessions. In other words, users are strangers to your Web site every time they access a page." *Id*. So, for example, browser cookies made it possible for a web site to recognize users who are "logged in" or to keep items in a "shopping cart" as the user browses different

[6] http://www.cookiecentral.com/faq/.
[7] *Available at* https://web.archive.org/web/20000610185244/http://www.builder.com/Programming/Cookies/?st.bl.pr.10.feat.1140. According to Montulli, "cookie" was a "a well-known computer science term that is used when describing an opaque piece of data held by an intermediary." *Id*.
[8] *Available at* https://web.archive.org/web/20110213111145/https://www.ftc.gov/bcp/privacy/wkshp97/comments2/netsc067.htm.

pages on the site. *Id*. In the early days of the web, browser cookies served an intuitive function for both users and for website operators.

But problems began when cookies were used not simply to assist users at websites but to track their movements across the Internet. EPIC first identified the growing risk of cookie tracking in a 1997 report. As EPIC explained:

> There has been a great deal of controversy about the cookies feature in browser software. On the one hand, cookies make it possible for a web server to "recognize" a web client and enables certain features that are useful for surfing and on-line commerce, such as retaining screen preferences, storing passwords, and creating virtual shopping carts. . . . At the same time, cookies also enable the surreptitious collection of information from the user.

EPIC, *Surfer Beware: Personal Privacy and the Internet* (1997).[9]

In the report, EPIC surveyed the Top 100 websites and found that 24 enabled cookies. "The cookies feature is often used for registration and password storing, but may also be used to create logs of user interests and preferences (for instance, tracking particular articles that a user accesses at an on-line news site*)."* *Id.* EPIC also found that "it was noteworthy that none of the sites that enabled cookies told the user that information about the user was being placed on the user's system. We think that more could be done to make such transactions 'transparent'—that is to say, readily apparent to the user." *Id.* In subsequent

[9] https://www.epic.org/reports/surfer-beware.html.

reports, EPIC found that the use of cookies was growing though they were still used primarily to enhance the user experience at a particular web site.[10]

By 2000 the Federal Trade Commission ("FTC") reported that advertisers had begun to use cookies and other "Web bugs" to track browsing activity of users across the web. Fed. Trade Comm'n, *Online Tracking: A Report to Congress* (2000).[11] As the Commission explained, "[a]lthough network advertisers and their profiling activities are nearly ubiquitous, they are most often invisible to consumers." *Id*.

Consumers at that time were already deeply troubled by cookie tracking. The FTC found that "89% of consumers are not comfortable having their browsing habits and shopping patterns merged into a profile that is linked to their real name and identity," and "91% of consumers say that they are not comfortable with Web sites sharing information so that they can be tracked across multiple Web sites." *Id*. The FTC remarked that "the cumulation over time of vast numbers of seemingly minor details about an individual produces a portrait that is quite comprehensive and, to many, inherently intrusive." *Id*.

---

[10] EPIC, *Surfer Beware II: Notice Is Not Enough* (1998), https://www.epic.org/reports/surfer-beware2.html; EPIC, *Surfer Beware III: Privacy Policies without Privacy Protection* (1999), https://www.epic.org/reports/surfer-beware3.html.

[11] https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf.

In the almost-two decades since, consumer tracking and profiling have proliferated in ways that would have been unimaginable to consumers at the time. Methods of web tracking have evolved beyond simple cookie tracking; companies now employ browser "fingerprinting," use invisible images called "pixel tags" or "web beacons," collect unique device identifiers associated with users' computers and phones, and use e-mail addresses and other persistent identifiers to profile users. *See* Fed. Trade Comm'n, *Online Tracking* (2016).[12] Moreover, companies now track users across multiple websites and across multiple devices, even following them into the offline world. *See*, *e.g.* Fed. Trade Comm'n., *Cross-Device Tracking, Staff Report* (2017).[13]

In practice, web tracking is almost impossible for consumers to avoid and even commonly used browser settings that offer a "private" browsing experience do not prevent tracking. For example, the FTC found that, "private browsing may not be effective in stopping third parties from using techniques such as fingerprinting to track your web activity." FTC, *Online Tracking* (2016), *supra*. The Commission has also found that while "the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA) offer tools for opting out of

[12] https://www.consumer.ftc.gov/articles/0042-online-tracking.
[13] https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

targeted advertising," these tools actually require the placement of cookies and, therefore, if a user "delete[s] all cookies, you'll also delete the cookies that indicate your preference to opt out of targeted ads." *Id*. Users who activate the "Do Not Track" feature—"a setting in most internet browsers that allows you to express your preference not to be tracked"—are likely unaware that, "most tracking companies today have not committed to honoring users' Do Not Track preferences." *Id*.

In response to efforts by users to delete cookies, companies now deploy browser cookies that cannot be deleted by the user. Companies have developed so-called "supercookies" that are very difficult to detect and, if removed, may secretly reinstall themselves. *See* Ashkan Soltani et al., *Flash Cookies and Privacy 2: Now with HTML5 and ETag Respawning* (2011).[14] Supercookies are designed to evade cookie-blocking features in web browsers and browser ad-ons. *Id*. Erasing traditional cookies, clearing history, erasing the cache, or even using a browser's "private browsing" mode will not prevent these supercookies from transmitting details about your browsing history. Ashkan Soltani et al., *Flash Cookies and Privacy 1* (2009).[15] Even when a user takes the steps to disable cookies, companies find other ways to track their browsing history, including by installing "seemingly

[14] *Available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390.
[15] *Available* at http://ssrn.com/abstract=1446862.

innocuous software that allows for detailed tracking." Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 Wake Forest L. Rev. 433, 438 (2014).

This has become an arms race between the few users and developers who have the tools to disable invasive tracking, and the companies that have the resources to circumvent defensive measures. Companies have recently begun using a technique called "fingerprinting." Adam Tanner, *The Web Cookie Is Dying. Here's The Creepier Technology That Comes Next*, Forbes (Jun. 17, 2013).[16] Fingerprinting can identify users based on "unique characteristics of the individual computers people use" under the "assumption that each user operates his or her own hardware, identifying a device is tantamount to identifying the person behind it." Nick Nikiforakis & Günes Acar, *Browser Fingerprinting and the Online-Tracking Arms Race*, IEEE Spectrum (Jul. 25, 2014).[17] These fingerprinting techniques are evolving to the point where they are impossible for users to block. *See* Dan Goodwin, *Now Sites Can Fingerprint You Online Even When You Use Multiple Browsers*, ArsTechnica (Feb. 23, 2017);[18] Julia Angwin, *Meet the Online*

[16] https://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/.
[17] https://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race.
[18] https://arstechnica.com/information-technology/2017/02/now-sites-can-fingerprint-you-online-even-when-you-use-multiple-browsers/.

Tracking Device That Is Virtually Impossible to Block, ProPublica (Jul. 21, 2014) (describing a new technique called "canvas fingerprinting" that identifies a user's device based on the unique way it draws a hidden image).[19]

In most cases, the public would never know about these surreptitious tracking methods if not for testing done by computer scientists. For example, the public only learned that Google was circumventing Safari browser's cookie-blocking feature after it was discovered by a computer researcher in a Ph.D. program at Stanford University. Stacy Cowley, *Google Caught Skirting Safari Privacy Settings*, CNN Money, (Feb. 17, 2012).[20]

Moreover, some cookie-blocking methods have actually *increased*, rather than decreased, the omnipotence of Facebook's web tracking. For instance, in June of 2017, Apple implemented new settings for its Safari browser that blocked third-party tracking cookies after 24 hours. *See* Russell Brandom, *Apple's New Anti-Tracking System Will Make Google and Facebook Even More Powerful*, The Verge (Jun. 6, 2017).[21] The effect of this change was to increase Facebook's dominance of online advertising, as the company could still rely on its ubiquitous "like" button to track users. *Id*.

---

[19] https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block.
[20] http://money.cnn.com/2012/02/17/technology/google_tracking_safari/index.htm.
[21] https://www.theverge.com/2017/6/6/15747300/apple-safari-ad-tracking-cookie-blocker-google-facebook-privacy.

Today, the prospect of Internet users possibly finding ways to escape all of this ubiquitous web tracking has led advertisers to deploy yet another method: email tracking. A recent study revealed that 30% of all emails embed third-party tracking cookies, allowing advertisers to link a user's browsing activity to their email address. Steven Englehardt, Jeffrey Han, & Arvind Narayanan, *I Never Signed Up for This! Privacy Implications of Email Tracking*, 2018 Proc. Privacy Enhancing Tech.[22]

B. It is not reasonable to expect users to protect themselves when Facebook's tracking techniques are designed to escape detection and the company routinely ignores users' privacy preferences.

Over the past decade, Facebook's data collection and tracking tools have spread across the web. During the same period, Facebook has repeatedly deceived users and overrode their privacy settings. As a result of these unfair and deceptive practices, the company settled claims with the FTC back in 2011, following complaints brought by consumer privacy organizations. Press Release, Fed. Trade Comm'n., *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (Nov. 29, 2011) (noting that "Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic

---

22 https://www.ftc.gov/system/files/documents/public_events/1223263/privacycon_emailprivacy_englehardt_0.pdf.

Privacy Information Center and a coalition of consumer groups.").[23] The FTC's Consent Order required Facebook to, among other things, cease misrepresenting its privacy practices, obtain consumers' affirmative express consent before enacting changes that overrode their privacy preferences, and establish a comprehensive privacy program with regular, independent third-party audits of the company's practices. Decision and Order, *In re Facebook*, FTC File No. 092 3184 (Jul. 27, 2012).[24]

But Facebook has repeatedly failed to abide by the terms of its own settlement with the FTC. In March 2018, Facebook was found to have allowed the political data mining firm Cambridge Analytica to access the personal information on 87 million users without their knowledge or consent. Heather Kelly, *Facebook Says Cambridge Analytica May Have Had Data on 87 Million People*, CNN (Apr. 4, 2018).[25] On March 26, 2018, the FTC announced that it was investigating Facebook for violating the terms of the Consent Order by allowing this massive disclosure of personal data. Press Release, Fed. Trade Comm'n, *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported*

---

[23] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
[24] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[25] http://money.cnn.com/2018/04/04/technology/facebook-cambridge-analytica-data-87-million/index.html.

Concerns about Facebook Privacy Practices (Mar. 26, 2018).[26] In June 2018, the New York Times reported that Facebook had overridden users' privacy settings to provide at least 60 device makers with private access to users' personal data. Gabriel J.X. Dance, et. al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends,* N.Y. Times (Jun. 3, 2018).[27] Following the story, Facebook acknowledged these arrangements, which directly contradict Facebook's 2015 statements that it had cut off third-party access to user data. *See* Josh Constine, *Facebook Is Shutting Down Its API For Giving Your Friends' Data to Apps*, TechCrunch (Apr. 28, 2015).[28]

Given these repeated misrepresentations and violations by Facebook, it was unreasonable for the lower court to expect users to both know and to effectively prevent invasive tracking techniques.

II. Courts should not place the burden on users to compete in a technical arms race to protect their privacy.

The lower court's conclusion that consumers cannot assert privacy claims in this case because they "could have taken steps to keep their browsing histories private" is wrong as a matter of fact and as a matter of law. ER20. There is

[26] https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.
[27] https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html.
[28] https://techcrunch.com/2015/04/28/facebook-api-shut-down/.

substantial dispute over the efficacy of the technological "protections" mentioned by the lower court including blocking cookies, using "incognito" or "private" browsing mode, and installing "plugin browser enhancements." A court could resolve these factual disputes at trial based on expert evidence. But, instead, the lower court improperly assumed facts favorable to Facebook at the motion to dismiss stage without actual review of any evidence. And more fundamentally, the lower court's reasoning that individuals cannot assert their rights unless they adopt such measures flips privacy law on its head.

The purpose of privacy law is to protect against invasive and unreasonable practices involving the collection, use, and disclosure of personal information. Placing the burden on users to develop technical measures to protect themselves negates the core purpose of privacy law and would be ineffective for several reasons. First, it is unreasonable to expect the average user to understand the various plug-ins, applications, and complicated settings necessary to prevent advanced tracking techniques. Sophisticated users are frequently overwhelmed by the complexity and pervasiveness of these practices. Second, any user hoping to defeat tracking over time would need to constantly survey the field of emerging tracking techniques and develop new countermeasures. That is economically inefficient and would place the burden on each Internet user to become an expert in security practices. And third, the basic function of tort law is to impose costs on the

parties that are in the best position to avoid harmful behavior (the "least cost avoiders") which, in this case, are the companies that track users' browsing history.

Compared to the significant resources and bandwidth of companies engaging in cookie tracking operations, users have little ability or incentive to invest in a constant digital arms race to avoid tracking. The companies are the ones deploying technological developments in the first place and thus have all of the necessary information. Modern privacy laws allocate the burden on those who are providing the service to ensure privacy protections for users. Such laws would be superfluous if they could only be effectively enforced by computer science PhDs.

A. Privacy laws place responsibilities on data collectors and give rights to data subjects.

Privacy laws allocate rights and responsibilities between the person who provides personal data and the company that maintains the personal data. The allocation is asymmetric. Privacy law establishes the rights of individuals over their personal data and imposes responsibilities on data collectors to limit collection and use of such data. One of the motivating factors behind privacy law is the understanding that privacy protection is essential to establishing user trust in communications platforms.

California has enacted several significant privacy laws to protect consumers. The California Constitution recognizes a consumer's "inalienable right" to pursue and obtain "privacy." Cal. Const. art. 1, § 1. The California Information Practices

Act of 1977 ("CIPA") states that "all individuals have a right of privacy in information pertaining to them." Cal. Civ. Code § 1798.1. CIPA also recognizes that "the right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information" and "the increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information." Cal. Civ. Code § 1798.1(a), (b). Also, to better protect privacy, CIPA emphasizes "it is necessary that the maintenance and dissemination of personal information be subject to strict limits." Cal. Civ. Code § 1798.1(c).

The underlying framework for many of privacy law is the Fair Information Practices, a set of principles that articulate the rights of data subjects and data collectors. U.S. Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* XX-XXIII, at 50 (1973). Its principles include, among others, the individual's right to know which and what personal data is being collected and to prevent the collection and dissemination of data for a secondary purpose without having given consent. EPIC, *The Code of Fair Information Practices* (2018).[29] The Fair Information Practices makes clear

[29] https://epic.org/privacy/consumer/code_fair_info.html.

that privacy laws are to bestow rights on users and responsibilities on data collectors to protect privacy.

At the federal level, the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. 99-508, 100 Stat. 1848, (current version at 18 U.S.C. §§ 2510 *et seq.*), was enacted to protect "the privacy expectations of citizens" in their communications and to impose responsibilities on both service providers and government agencies to protect personal data. *See* H.R. Rep. No. 99-647, at 19 (1986). Congress also sought to support the creation of new technologies by assuring consumers that their personal information would remain safe. *See* S. Rep. No 99-541, at 5 (1986) (noting that legal uncertainty over the privacy of new forms of communication "may unnecessarily discourage potential customers from using innovative communications systems"). Congress emphasized that consumers would not trust such technologies unless privacy was protected. *Id.*; H.R. Rep. No. 99-647, at 19.

The "core purpose" of the Wiretap Act, 18 U.S.C. §§ 2510–2522, is to strictly limit unlawful or unauthorized interception and to "protect the privacy of individuals by banning eavesdropping other than by duly authorized law enforcement officers who complied with the safeguards provided by the law." Edith J. Lapidus, *Eavesdropping on Trial* 7 (1974). The law accomplishes this in three distinct ways: (1) by generally prohibiting unauthorized interception and

providing for civil remedies, 18 U.S.C. §§ 2511, 2520; (2) by criminally sanctioning both unlawful interception and the facilitation of unlawful interception through manufacture and distribution of "intercepting devices," 18 U.S.C. §§ 2511, 2512; and (3) by establishing specific procedures that courts and law enforcement officers must follow in order to be authorized to intercept communications, 18 U.S.C. §§ 2516–18. To ensure enforcement of these rules, Congress provided a full range of remedies: damages, criminal penalties, injunctive relief, and suppression of evidence derived from an unlawful or unauthorized interception. Congress also established an extensive reporting scheme to facilitate public oversight of the use of the Wiretap authority. 18 U.S.C. § 2519. *See generally* EPIC, *Wiretapping* (2018).[30]

Similarly, the Video Privacy Protection Act of 1988 ("VPPA") was passed to protect the personal consumer information obtained by businesses that offer video services. 18 U.S.C. § 2710 (2002). The VPPA provides a general ban on the disclosure of personally identifiable rental information unless the consumer consents specifically and in writing. *Id.* § 2710(b)(2)(B). At the time of enactment, Congress covered every circumstance by which a video service provider could obtain personal information and construed "personal information" broadly to encompass the various ways that identifiers and elements of a person's identity

[30] https://epic.org/privacy/wiretap/.

could be linked to an actual individual. *Id*. § 2710(a)(3). This broad coverage was to ensure companies had full and comprehensive responsibility to protect consumer privacy. The Act currently serves as one of the strongest protections of consumer privacy against a specific form of data collection.

The lower court's holding, however, flipped the structure of law entirely by imposing on users the responsibility for implementing technological protections that might limit the collection of their personal information. Under the lower court's framework, privacy law is superfluous. The law would only protect users so far as they are able to protect themselves; the law would serve no purpose. That cannot be the point of privacy law and the lower court notably does not cite any binding precedent in the 9th Circuit or any other appellate court for this proposition.

B. Consumers expect their browsing habits to remain private.

Users do reasonably expect that their personal information, such as browsing habits, will remain private. Recent surveys show that Americans hold high expectations for privacy in the digital age. According to Pew Research Center, "[m]ost Americans hold strong views about the importance of privacy in their everyday lives." Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy,*

Security and Surveillance, Pew Res. Ctr. (May 20, 2015);[31] *see also* EPIC, *Public Opinion on Privacy* (2018).[32] This is particularly so for the type of personal data collected and who the data is collected for. Madden and Rainie, *supra*. As of 2015, 93 percent of adults believe it is important to have control over who can get information about them. *Id.*

Consumers are increasingly cognizant and protective of their privacy online as the amount of personal information collected and stored online has increased. Individuals between the ages of 18 and 29 are more likely than older adults to try and protect their privacy and have expressed harm as a result of some privacy problem. Lee Rainie, *The State of Privacy in Post-Snowden America*, Pew Res. Ctr. (Sept. 21, 2016).[33] Of those surveyed, 74 percent of individuals between the ages of 18 and 29 express concern about the use of cookie tracking and collection of browser history data. *Id.* But significantly few users had knowledge of how to set up their browser to disable or turn off cookies. *Id.*

Users also maintain an expectation that they are not in a position to control what companies do with their personal data. Research shows that 91 percent of adults believe that consumers have little to no control over how personal data is

---

[31] http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.
[32] https://www.epic.org/privacy/survey/.
[33] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

collected and used by companies. *Id.* Also, very few individuals have altered their behavior in the last several years to avoid being tracked. *Id.* A majority of Americans, however, do believe that privacy laws make a difference and can better protect consumer privacy. Approximately 64 percent of internet users "believe the government should do more to regulate advertisers." *Id.* And this same majority supports more regulation of advertisers and how they handle personal information and collect it through techniques like cookie tracking. *Id.*

While users maintain an expectation of privacy in their online behaviors, very few have the knowledge or resources to implement advanced technological protections. For example, only 10 percent of adults have encrypted their phone calls, text messages or email, and only 9 percent have used services such as a proxy server, Tor software, or virtual personal network to browse the Web anonymously. Madden and Rainie, *supra*. Many Americans have difficulty understanding the nature and scope of the collection and management of their personal data. Rainie 2016, *supra*. Users are also unaware of "robust actions they could take to hide their online activities. *Id.* And even if they did understand, technology experts already predict that "few individuals will have the energy or resources to protect themselves from 'dataveillance' in coming years." *Id.*

C. Companies, not users, are best positioned to limit invasive tracking.

Basic tort principles, which underlie much of modern privacy law, place liability on the party who is in the best position to avoid the harm, the "least-cost avoider." *See* Guido Calabresi, *The Costs of Accidents: A Legal and Economic Analysis* 135 (1970) ("A pure market approach to primary accident cost avoidance would require allocation of accident costs to those acts or activities (or combination of them) which could avoid the accident costs most cheaply."); *see also* Ronald Coase, *The Problem of Social Cost*, 3 J. Law & Econ. 1 (1960) (articulating a theory of cost allocation to promote efficient allocation of property resources).

The least-cost avoider theory is particularly relevant where transaction costs are high, as in the case of one party causing harm to a large and diffuse group of individuals. Calabresi, *supra*, at 135-38; *see* Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. Legal Stud. 13, 27–28 (1972) (arguing that when transaction costs are high, the legal system can "improve the allocation of resources by placing liability on that party who in the usual situation could be expected to avoid the costly interaction most cheaply"). Liability rules that hold a least-cost avoider responsible allocate rights and responsibilities such that privacy rights are protected, and statutory violations are avoided.

Companies, such as Facebook, that engage in cookie tracking practices even when the users are logged out of its services constitutes a high transaction cost, causing harm to the privacy of the large and diffuse group of Facebook users. The least-cost avoider theory makes clear that the burden should be placed on the company, which is the perpetrator of the harm and the party in the position to most effectively redress that harm. On the one hand, under the lower court's model, millions of users will have to take costly and time-consuming steps to maintain their privacy against increasingly intrusive practices. On the other hand, if the burden is imposed on the data collector to limit invasive practices, then a company can simply employ a privacy enhancing technique to limit collection and protect the privacy of all of its users. Imagine a world in which car manufacturers left brake pedals in the trunk with instructions for how they should be installed and another where car manufacturers could not sell a car unless the brake pedals were properly installed. The latter approach not only leads to fewer accidents, but also it is more efficient.

To guarantee user privacy in the first place, it is more efficient and less-costly for the company to employ the privacy safeguard rather than have each individual user continuously implementing new technical measures to avoid being tracked.

* * *

Consumers intend for their browsing history to be private, and this Court should respect their expectations and uphold the purpose of modern privacy laws by enforcing the responsibilities of companies to protect such privacy.

CONCLUSION

EPIC respectfully requests that this Court reverse the lower court's motion to dismiss and remand the case for further consideration in light of the privacy interests of Facebook users and purpose of modern privacy laws.

June 26, 2018

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Alan Butler
Natasha Babazadeh
Sam Lester
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(4) because it contains 5,272 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac in 14-point Times New Roman style.

/s/ Marc Rotenberg

Dated: June 26, 2018 Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on June 26, 2018, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Marc Rotenberg

Dated: June 26, 2018 Marc Rotenberg