No. 17-16206

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

WINSTON SMITH; JANE DOE I; AND JANE DOE II, on behalf of themselves and others similarly situated

Plaintiffs-Appellants,

v.

FACEBOOK, INC.,

Defendant-Appellee,

and

AMERICAN CANCER SOCIETY, INC.; et al.,

Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California
Case No. 5:16-cv-01282-EJD
Honorable Edward J. Davilla

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

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

Counsel for Amicus Curiae

September 26, 2017

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

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICUS[1]

The Electronic Privacy Information Center ("EPIC")[2] 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* before the United States Supreme Court, federal circuit courts, and state appellate courts in cases concerning consumer privacy and medical record privacy. *See In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3d Cir. 2016) (arguing that unique persistent identifiers disclosed in connection with online video viewing records constituted "personally identifiable information" under the Video Privacy Protection Act); *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013) (arguing that interception of private Wi-Fi data from home networks violated the Wiretap Act); *Fraley v. Batman*, 638 Fed. App'x 594 (9th Cir. 2016) (arguing that Facebook's proposed settlement of privacy claims arising from "Sponsored Stories" advertisements was not fair or sufficient for class members).

---

[1] The plaintiffs consent to the filing of this brief. Pursuant to Circuit Rule 29-3, EPIC endeavored to obtain consent of the defendants, but the defendants did not respond. 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.

[2] EPIC Fellows Christine Bannan and Samuel Lester contributed to this brief.

ARGUMENT

According to the lower court, Facebook may surreptitiously collect the personal data of Internet users even when the sites they visit state that their personal data will not be disclosed to others. That cannot be correct. "Consent" is not an acid rinse that dissolves common sense. And it most certainly does not dissolve a 2012 consent order between the company and the Federal Trade Commission that governs the company's data collection practices. The decision of the lower court should be reversed.

Nearly two-thirds of Americans use Facebook,[3] yet hardly anyone reads the privacy policies. Kimberlee Morrison, *Survey: Many Users Never Read Social Networking Terms of Service Agreements*, Adweek (May 27, 2015).[4] Why should they? Facebook announces boldly "your privacy is very important to us." Facebook, *Statement of Rights and Responsibilities* (2015) ("1. Privacy").[5] That should provide a reasonable assurance that the company will not engage in deceptive practices to track users or obtain their data.

---

[3] As of 2017, 64% of all Americans use Facebook. Edison Research, *The Infinite Dial 2016* (May 10, 2016), http://www.edisonresearch.com/the-infinite-dial-2016/.
[4] http://www.adweek.com/digital/survey-many-users-never-read-social-networking-terms-of-service-agreements/.
[5] https://www.facebook.com/terms.php.

Yet in this case, the lower court sided with Facebook and found that users had consented to tracking, even when they went to web sites such as cancer.net, to obtain sensitive personal information about their medical conditions.

I. Notice does not constitute consent.

Privacy law evolves with new technology and new business practices. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890) (proposing a new tort of privacy following "[r]ecent inventions and business methods" such as "instantaneous photograph[y]"). In *Riley v. California*, Chief Justice Roberts writing for the Court stated "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

The challenges to privacy are many. Today, courts also confront a variety of techniques intended to take away legal protections to safeguard personal data. These include privacy policies that do not protect privacy, and notices that disclaim conduct that cannot be disclaimed.

Rather than apply federal and state privacy laws to the facts of this case, the lower court adopted an overly broad and formalistic view of consent. Such a sweeping exception to privacy law is out of step with current reality and undermines the rule of law. As Professor Julie Cohen has explained, "consent-

based dismissals of information privacy claims constitute a powerful statement of institutional disengagement from the conditions of contemporary commercial life." *See* Julie E. Cohen, *Information Privacy Litigation As Bellwether for Institutional Change*, 66 DePaul L. Rev. 535, 561 (2017).

According to the lower court, if a company indicates somewhere, on some web page far below its assurance that "privacy is very important," that it will collect personal data—even when the user has every reason to believe otherwise—then privacy laws no longer apply. Such an outcome is "clearly at odds with the general aim of privacy law in both the United States and Europe," which is "to limit the collection and use of personal data." Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1, ¶ 30. As Professor Cohen further explains, "the expansive scope afforded for practices of notice-and-waiver in the information privacy context is unlike that in any other area of substantive law." Cohen, *supra*, at 558.

In order to establish that an individual has meaningfully consented to the collection or disclosure of their personal information, a court should consider (1) their degree of awareness (including both time and content-specific awareness) of the tracking, (2) their ability to control the scope of the collection or disclosure (e.g. whether they can opt-in or opt-out of the tracking), and (3) any conflicting or contradictory representations regarding tracking. In this case, the lower court

ignored a variety of facts, including explicit statements that the personal data at issue would not be disclosed, and instead selected certain phrases in Facebook's terms of service to conclude that consent had been obtained. The Court should not adopt such a broad waiver of users' rights based on a few words stashed in a privacy policy.

A. Generic notice is insufficient to establish meaningful consent to the detailed tracking of users' web browsing history.

According to the Federal Trade Commission, the collection of personal data online is "ubiquitous and often invisible to consumers." Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* 60 (2012) (hereinafter "FTC Report").[6] The FTC found that "consumers generally lack full understanding of the nature and extent of this collection and use" of their personal information. *Id.* The Commission concluded that the "notice-and-choice" model of privacy protection, "which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand." *Id*.

This is particularly true of Facebook. Examinations of Facebook's privacy settings have found that they regularly fail to allow consumers to achieve their privacy preferences. One study reported that "privacy settings match users'

[6] http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected." Yabing Liu, et al., *Analyzing Facebook Privacy Settings: User Expectations vs. Reality*, Proc. 2011 ACM SIGCOMM Conf. on Int. Mgmt. 61, 61 (2011). The ability of Facebook to exploit users' lack of awareness is most evident with third-party tracking: the collection of personal data occurs not when the user is on Facebook and may be thinking about Facebook's privacy settings, but while the user is browsing other websites and may be quite reasonably relying on the privacy representations of that site.

In fact, that is precisely what happened in this case. Users could point to explicit statements on the medical websites they visited which said their personal data would not be disclosed to others. Yet, Facebook pointed to language, buried deep in its privacy policy, which said that it nonetheless could collect the data, and the lower court sided with Facebook. In such a world, how can users possibly make sense of privacy statements?

Furthermore, studies have found that individuals tend to follow default settings, even when given the chance to change those settings. Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (2008). Facebook and other companies with an interest in obtaining personal information design their privacy settings in ways that maximize data collection. As Professor Ryan Calo explained, "entities have an interest in, and

have developed expertise in, exploiting behavioral and psychological processes to promote disclosure." Ryan Calo, *Digital Market Manipulation.* 82 Geo. Wash. L. Rev. 995, 1304 (2014). Facebook has a long history of designing its platform to encourage users to simply accept its default privacy settings. *See* Molly Wood, *How Facebook Is Putting Its Users Last*, CNET (Apr. 23, 2010).[7]

Moreover, concerns regarding "long, incomprehensible privacy policies" that the FTC identified in its report are particularly acute here, given the complex nature of third-party tracking. Either the privacy statement must be impossibly long and complex, or it must omit material information to be presented in a way that consumers can understand. As Professor Helen Nissenbaum has explained, "summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used." Helen Nissenbaum, *A Contextual Approach to Privacy Online,* 140 Dædalus 32, 35 (2011).

Facebook has exploited its status as the most widely-used social networking service by presenting users with take-it-or-leave-it settings regarding its third-party tracking practices. As the FTC states, "a 'take it or leave it' approach is

[7] http://news.cnet.com/8301-31322_3- 20003185-256.html.

problematic from a privacy perspective, in markets for important services where consumers have few options." FTC Report at 48. It is not a reasonable option in today's world to simply opt-out of Facebook. Facebook has an unparalleled reach and influence. Julia Boorstin, *Forget 25 Years—Facebook Changed Our Lives In 10*, CNBC (Feb. 6, 2014).[8] Therefore, even if the lower court was correct in construing Facebook's terms as a contract, the court erred when it failed to construe ambiguous terms against the drafter (Facebook), as is required in contracts of adhesion. *See Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1224 (9th Cir. 2015). Under California law, contracts of adhesion are also considered unconscionable where they waive statutory rights. *See Iskanian v. CLS Transp. Los Angeles, LLC*, 59 Cal. 4th 348 (2014).

In sum, it is simply unrealistic to find that plaintiffs meaningfully consented to Facebook's third-party tracking practices based on notice alone. Meaningful consent implies that consumers are exercising freedom of choice in a marketplace, and as Professor Nissenbaum describes, the concept of "free choice" is incompatible with the realities of online privacy:

> That almost all privacy policies are long, abstruse, and legalistic adds to the unrealistic burden of checking the respective policies of the websites we visit, the services we consider and use, and the content we absorb. Compounding the burden is an entity's right to change its

[8] https://www.cnbc.com/2014/02/06/forget-25-yearsfacebook-changed-our-lives-in-10.html.

> policy at will, giving due notice of such change, ironically, within the policy itself and therefore requiring interested individuals to read it not once but repeatedly. Unsurprisingly, ample evidence reveals that people do not read privacy policies, do not understand them when they do, and realistically could not read them even if they wanted to.

Nissenbaum, *supra*, at 35. Mere notice is especially inadequate given the degree of uncertainty, lack of transparency, and lack of information that users face in the online context. "Advancements in information technology have made the collection and usage of personal data often invisible." Alessandro Acquisti, Laura Brandimarte, & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 Science 509, 509 (2015).

Facebook's third-party tracking practices reflect precisely what Professor Nissenbaum is describing. Facebook has implemented this practice surreptitiously without giving its users due notice or an opportunity to opt-out. Users are unlikely to read Facebook's privacy policies, even when they do receive notice, and, moreover, they are unlikely to understand these policies even if they do read them. It is misguided to apply a contractual standard of consent where Facebook's surveillance invades a relationship between users and third-party websites—a relationship in which those users had a clear and explicit expectation of privacy.

B. Consent to collection of health data cannot be presumed when the healthcare websites expressly prohibit such disclosures.

The users in this case had every reason to expect privacy in their browsing of healthcare websites—a context where they were disclosing highly sensitive,

health-related information. Studies show that context is critical to expectations of privacy, and the healthcare websites at issue in this case had explicitly promised not to disclose their users' personal data. For example, Melanoma.org stated, "We do not sell or share your Personal Data with Third Party Companies." ER371. Cleveland Clinic promised, "Cleveland Clinic does not share any personally identifiable information of any individual with any third-party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization." ER397.

Contextual factors, such as how that information will be used, are profoundly important in determining whether users will disclose personal data to others. *See* Kirsten Martin, Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 Colum. Sci. & Tech. L. Rev. 176 (2016). While some individuals may be willing to disclose personal data in one context, they may not be so willing in another context, particularly where the information they are disclosing is highly sensitive. The FTC has stressed the importance of a respect for context in regards to online privacy, stating, "Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business." FTC Report, *supra*, at 27.

Here, the users were communicating with their healthcare providers and disclosing information about their doctors and treatment options. ER246, ¶ 161. And they did so with the explicit assurance from the websites they were visiting that their personal information would not be disclosed to others. Given the sensitivity of this information—which is given heightened protection under federal law[9]—the plaintiffs had the right to expect privacy.

C. This Court's "net impressions" analysis should apply to the interpretation of privacy policies.

This Court has also made clear in the online false advertising context that truthful disclosures buried in fine print or in a hyperlink are insufficient to correct a consumer's misleading "net impression." As this Court explained in *FTC v. Cyberspace.com, LLC*, 453 F.3d 1196 (9th Cir. 2006), "[a] solicitation may be likely to mislead by virtue of the net impression it creates even though the solicitation also contains truthful disclosures." 453 F.3d at 1200. It is similarly inadequate to bury a disclosure with other "densely packed information and legalese," or present it in vague terms that are not clearly defined. In *FTC v. Commerce Planet*, 878 F. Supp. 2d 1048 (C.D. Cal. 2012), *aff'd in part, vacated in part, and remanded on other grounds*, 815 F.3d 593 (9th Cir. 2016), the court observed:

---

[9] *See* Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 1320d-1320d-8.

> District courts consider the overall, common sense "net impression" of the representation or act as a whole to determine whether it is misleading. See *FTC v. Gill*, 265 F.3d 944, 956 (9th Cir. 2001) (holding that defendant failed to counter the FTC's substantial showing that he made statements and created an overall "net impression" of a misleading representation regarding the ability to remove negative information from consumers' credit report, "even if the information was accurate, complete, and not obsolete")

878 F. Supp. 2d at 1065. *See also FTC v. Johnson*, 96 F. Supp. 3d 1110, 1148 (D. Nev. 2015).

Facebook's assurance that "your privacy is very important to us" along with the healthcare websites' explicit promises not to disclose personal data to third-parties created the net impression that the plaintiffs would not be tracked while visiting the healthcare websites. In order to review the "notice" of third-party tracking at issue in this case, the plaintiffs would have had to click on a series of hyperlinks to locate Facebook's "Data Policy" and "Cookie Policy." In *Commerce Planet*, this Court affirmed the lower court's holding that a disclosure, buried in a privacy policy, without an affirmative opt-in option or a clear and conspicuous representation, was inadequate. *Commerce Planet*, 815 F.3d 593. The court in *Commerce Planet* relied on expert testimony that "as soon as you put the word 'privacy policy' in front of a consumer, they completely tune out. They're one of the most unread components of a web page." 878 F. Supp. 2d at 1070. Here, Facebook disclosed its third-party tracking practices within a series of hyperlinks buried *within* its privacy policy. This disclosure was therefore wholly inadequate to

cure the plaintiffs' net impression that they had privacy while they browsed the healthcare websites.

The "net impressions" analysis that this Court has applied to online advertising should apply with even more force to privacy policies because consumers are far less likely to understand the techniques for online tracking than they are the terms for commercial transactions. *See* FTC Report, *supra*, at 60.

II. Consent is also limited by the scope of Facebook's settlement with the FTC in 2012.

In 2012, Facebook entered into a settlement with the FTC governing its privacy practices for a twenty-year period. *Facebook, Inc.,* FTC File No. 092-3184, Dkt. No. C-4365, at 3 (July 27, 2012) (Decision and Order).[10] Facebook agreed that it "shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information." Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises* (Nov. 29, 2011) (announcing the

[10] Under this agreement "covered information" includes but is not limited to: "(a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above."

proposed 2012 Decision and Order).[11] This includes representations about (1) Facebook's collection or disclosure of information; (2) the extent to which a user can control the privacy of covered information and steps that must be taken to implement controls; and (3) the extent to which Facebook discloses covered information to third-parties both while a user is active and after a user has deactivated or terminated her account. *Id*. at 3–4. Prior to "any sharing of a user's nonpublic user information with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s)," Facebook is required to make a "clear and prominent" disclosure—separate from the privacy policy—specifically identifying the third-parties and obtain the user's express affirmative consent. *Id*. at 4.

But 2014 marked a dramatic shift in Facebook's business practices to make its tracking ubiquitous across the internet. Facebook announced that it would expand its use of cookies and pixel tags on Facebook.com and Facebook apps to track user activity on non-Facebook websites for use in targeted advertising. The Trans-Atlantic Consumer Dialogue wrote a letter to the FTC commissioners asking them to investigate Facebook's new business practices as a possible violation of the 2012 consent decree. Letter from the Trans Atlantic Consumer Dialogue to

[11] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

Chairwoman Edith Ramirez, Fed. Trade Comm'n, and Commissioner Billy Hawkes, Data Protection Comm'nr, Ireland (July 29, 2014).[12]

The tracking techniques at issue in this case are even more expansive. Beyond cookies, Facebook is using browser fingerprinting and colleting IP addresses to track users across the internet. Here, Facebook's terms do not give a full disclosure of the company's tracking activities. Facebook's policies do not state that it intercepts communications on websites without social plugins. ER211, ¶ 20. The company appears to imply that there is a difference between websites with those plugins and websites displaying a simple Facebook icon. Therefore, even after reading the privacy policy, users would not have a full understanding of Facebook's business practices. ER225, ¶ 66. Furthermore, Facebook has already committed to a higher standard under the FTC Consent Decree—disclosure separate from their privacy policy and obtaining users express affirmative consent. Both are missing here.

III. The more precise representations in the healthcare website statements supersede the general disclaimer in the Facebook privacy policy.

Assuming that users do indeed read privacy policies, Facebook users in this case confronted two conflicting statements: a vague and general disclaimer buried in the Facebook privacy policy and prominent, precise statements from medical

[12] http://tacd.org/wp-content/uploads/2014/07/TACDletter-to-FTC-and-Irish-Data-Protection-Commissioner-re-Facebook-data-collection.pdf.

websites that they would not disclose personal data to third-parties. An essential rule of textual interpretation is that the specific controls the general—*generalia specialibus non derogant*. *See Nitro-Lift Technologies, L.L.C. v. Howard*, 568 U.S. 17, 21 (2012). Similarly, in contract interpretation, specific terms control over general ones when provisions are inconsistent. *S. Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 891 (9th Cir. 2003). As this Court recently explained, the "canon provides that a 'narrow, precise, and specific' statutory provision is not overridden by another provision 'covering a more generalized spectrum' of issues." *Perez-Guzman v. Lynch*, 835 F.3d 1066 (9th Cir. 2016) (quoting *Radzanower v. Touche Ross & Co.,* 426 U.S. 148, 153–54 (1976)).

Consider the statements. The Facebook statement is very broad:

> We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

ER12.

The lower court put great weight on the phrases "we collect information," "third party websites," and "when they offer our like buttons." ER13 (emphasis in original). But of course, the phrase "we collect information" provides no information whatsoever about the information collected. The description "third-party website" describes every website on the Internet other than Facebook's. And

Facebook's plug-ins cover 55 percent of the most popular websites in the world. *See* Priya Kumar, *When Was the Last Time You Read a Privacy Policy?*, Slate (Jan. 27, 2016).[13]

It would be difficult to draft a more general policy concerning the collection and use of personal data than the one Facebook presented to users. But the policies of the health care websites that users visited are quite precise.

- "We do not sell or share your Personal Data with Third Party Companies." (Melanoma.org) ER371.
- "Cleveland Clinic does not share any personally identifiable information of any individual with any third-party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization." ER397.

Even assuming that Facebook users consented to the collection of their personal data by third-party websites as a general proposition (which EPIC does not concede), isn't it equally reasonable to assume that these users understood that Facebook would not collect their data when they visited medical websites because of the very precise representations made by those third-party sites? In this instance, the cannon of statutory construction tracks the common sense understanding that consent is bounded where there is an explicit statement that disclosure will not occur.

[13] http://www.slate.com/articles/technology/future_tense/2016/01/tech_company_privacy_policies_don_t_cover_everything_they_should.html.

Regardless of whether the lower court had jurisdiction to consider the claims against the medical websites, it should not have ignored the representations that those sites made to Facebook users. It is ultimately the absence of user consent and not Facebook's terms that determine the outcome in this case.

CONCLUSION

EPIC respectfully requests that this Court vacate the lower court's order and remand for further consideration of Plaintiffs' claims.

September 26, 2017

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Alan Butler
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 3,981 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: September 26, 2017 Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on September 26, 2017, 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: September 26, 2017 Marc Rotenberg