No. 17-16873

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

MATTHEW CAMPBELL and MICHAEL HURLEY,
on behalf of themselves and all others similarly situated

Plaintiffs-Appellees,

v.

ANNA ST. JOHN

Objector-Appellant,

v.

FACEBOOK, INC.,

Defendant-Appellee.

On Appeal from the U.S. District Court
for the Northern District of California, No. 4:13-cv-05996-PJH
The Hon. Phyllis J. Hamilton

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF OBJECTOR-APPELLANT

Marc Rotenberg
Counsel of Record
Alan Butler
Sam Lester
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

February 1, 2018

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and 29(c), *amicus curiae* Electronic Privacy Information Center ("EPIC") certifies that it 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 AMICUS

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.[1] EPIC maintains one of the most popular web sites in the world concerning privacy—epic.org—and routinely advocates for consumer privacy in matters before the Federal Trade Commission ("FTC").

EPIC also frequently participates as *amicus curiae* before this Court and other courts in cases concerning the fairness of class action settlements in consumer privacy cases. In particular, EPIC has previously questioned the fairness of settlements that fail to prohibit the underlying conduct that gave rise to the suit. *See*, *e.g.*, Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC), *In re Google Cookie Placement Consumer Privacy Litig.*, 2017 WL 446121 (D. Del. Feb. 2, 2017) *appeal docketed*, No. 17-1480 (3rd Cir. Mar. 7, 2017) (arguing that a class action settlement that awarded only *cy pres* funds and no other relief to the class was unfair); Brief of *Amicus Curiae* EPIC, *Fraley v. Batman*, 638 Fed. App'x 594 (9th. Cir., 2016) (No. 13-17097) (arguing that a class action settlement

[1] Counsel for Objector-Appellants, Defendant-Appellees, and Plaintiffs-Appellees have all consented to the filing of EPIC's *amicus* brief. In accordance with Fed. R. App. P. 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

involving Facebook's "Sponsored Stories" was inadequate because it allowed Facebook to continue the conduct that was the basis for the suit).

EPIC has previously advised district courts about class action settlements in consumer privacy cases that failed to provide meaningful relief to class members. *E.g.* Letter from Marc Rotenberg, Exec. Dir., EPIC, to Hon. J. Davila (Aug. 22, 2013) (docketed in, *In re Google Referrer Header Privacy Litig.*, No. 10-4809)[2]; Letter from Marc Rotenberg, Exec. Dir., EPIC, to Hon. J. Koh (Jul. 11, 2012), (docketed in, *Fraley v. Facebook*, No. 11-01726)[3]; Letter from Marc Rotenberg, Exec. Dir., EPIC, to Hon J. Seeborg, (Aug. 20, 2012) (docketed in, *Fraley*)[4]; Letter from Marc Rotenberg, Exec. Dir., EPIC, to Hon. J. Seeborg, (Jan. 15, 2010) (docketed in, *Lane v. Facebook*, No. 5:08-cv-03845-RS).[5] In particular, EPIC has specifically opposed settlements where the only relief to the class was a vague notice posted in a privacy policy. *See*, *Google Referrer Header* at 2 (arguing that privacy notices "have been widely recognized as ineffective").

EPIC has a particular interest in this case. For almost a decade, EPIC has led efforts to combat privacy violations by Facebook. EPIC's work in 2010 and 2011, regarding changes in the privacy settings of Facebook users, resulted in a 2012 Consent Order between the FTC and Facebook concerning consumer privacy that

[2] https://epic.org/privacy/google/EPIC-et-al-Ltr-Google-Referrer-Header.pdf.
[3] https://epic.org/privacy/facebook/EPIC-Ltr-Koh-Fraley%207-12-12.pdf.
[4] https://epic.org/privacy/facebook/Seeborg-Ltr-8-20-12.pdf.
[5] https://epic.org/privacy/facebook/EPIC_Beacon_Letter.pdf.

could be impacted by this Settlement. *See Facebook, Inc.,* FTC File No. 092-3184, Dkt. No. C-4365, at 3 (July 27, 2012) (Decision and Order).

Finally, EPIC has a strong interest in ensuring that settlements in class actions advance the interests of class members and fulfill the core purposes of privacy laws. EPIC has also proposed objective criteria for courts to consider in determinations about cy pres awards. *See* Marc Rotenberg & David Jacobs, *Enforcing Privacy Rights: Class Action Litigation and the Challenge of Cy Pres,* in *Enforcing Privacy Law, Governance and Technology Series* 307 (David Wright & Paul De Hert eds., 2016). Chief Justice John Roberts expressed concerns similar to those raised by EPIC in *Marek v. Lane*, 134 S. Ct. 8 (2013)—a similar case involving privacy violations by Facebook.

ARGUMENT

A class action settlement should result in a substantial change in business practice. A class action settlement should not permit the continuation of the business practice that provided the basis for the lawsuit. A class action settlement should provide monetary relief to class members. If it is not possible to provide monetary relief to class members, then a *cy pres* award may be appropriate if the award advances the aims of the underlying investigation and is provided to organizations aligned with the interests of class members.

Class action lawsuits serve an important function in the enforcement of privacy laws in the United States. But in order to be effective, these cases must "stop business practices that harm consumers, compensate individuals for injuries suffered and deter future misconduct." Marc Rotenberg & David Jacobs*, Enforcing Privacy Rights: Class Action Litigation and the Challenge of Cy Pres,* in *Enforcing Privacy Law, Governance and Technology Series* 307 (David Wright & Paul De Hert eds., 2016).

Here, the proposed Settlement should not be approved. First, it would permit Facebook to continue scanning private messages, in violation of federal and state privacy law. The Settlement does not prevent Facebook from resuming the practices that provided the basis for this lawsuit. *See* Dkt. No. 192, Class Cert. Order, at 3-4; Dkt. No. 252, Order Approving Class Settlement, at 3. Indeed, the

notice provided by Facebook confirms that related conduct (the scanning of private messages) will continue. The absence of injunctive relief here distinguishes this Settlement from other, similar settlements within this Circuit.

Second, the Settlement allows Facebook to continue to scan private messages simply with the posting of a notice on a Facebook webpage. Such an outcome is contrary to law. A vague notice is not the basis for consent under the Electronic Communications Privacy Act or the California Invasion of Privacy Act.

Finally, where monetary compensation is unavailable, Fed. R. Civ. P. 23(b)(2), the adequacy of the prospective relief is critical. Here, absent Class Members will walk away empty-handed.

I. Class action settlements that fail to produce a substantial and enforceable change in business practices are insufficient.

Settlements that fail to provide either monetary or injunctive relief to the class are insufficient and should not be approved. Brief of *Amicus Curiae* EPIC, *In re Google Cookie Placement Consumer Privacy Litig.*, 2017 WL 446121 (D. Del. Feb. 2, 2017) *appeal docketed*, No. 17-1480 (3rd Cir., Mar. 7, 2017) (involving Google's tracking of Internet users on third-party websites.)[6] The Third Circuit found that Google's practice of "placing tracking cookies on the plaintiffs' web browsers in contravention of their browsers cookie blockers and defendant

[6] https://epic.org/amicus/class-action/google-cookie/EPIC-Amicus-In-re-Google-Cookie.pdf.

Google's own public statements" violated California law. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 130 (3d Cir. 2015). The settlement "fail[ed] to prohibit the underlying unlawful conduct that gave rise to the suit" and provided only *cy pres* funds instead of direct monetary relief to the class. Br. of EPIC, at 10. As EPIC explained, "[d]espite the substantial evidence of Google's wrongdoing, the proposed settlement contains no provision enjoining Google from such conduct in the future." *Id*.

Here, too, the District Court found substantial evidence that Facebook's conduct violated ECPA and CIPA. Order Granting in Part, Denying in Part, Mot. to Dismiss, Dkt. No. 43. Yet the Settlement contains no injunction barring Facebook from engaging in similar unlawful conduct in the future. "It is hard to imagine how a settlement provides a benefit to the Class if the company is allowed to continue the practice that gave rise to the putative class action." Br. of EPIC, at 11. And unlike the *Google* settlement, where monetary relief was awarded in the form of *cy pres* funds to several Internet privacy organizations, here the only relief available to the class was injunctive relief, and yet the Settlement fails to provide any such prospective relief.

EPIC also opposed the settlement in *In re Google Referrer Header Privacy Litigation*, 87 F. Supp. 3d 1122 (N.D. Cal. 2015), which permitted Google to continue to operate its search engine in a way that disclosed personal information

to third parties. There, as here, the only change mandated by the settlement was a modification of Google's privacy policy that would allow the company to continue the disputed practice. *Id*. EPIC argued that "additional notice will provide no meaningful benefit to the class. To the contrary, the revised notice will essentially ratify the company's continuation of the practice that gave rise to this suit." Letter from Marc Rotenberg, Exec. Dir., EPIC, to Hon. J. Davila (Aug. 22, 2013) (docketed in, *In re Google Referrer Header Privacy Litig.*, No. 10-4809).[7]

EPIC also opposes settlements that shield defendants from future claims arising out of the challenged conduct. In *Fraley v. Facebook*, the settlement forced class members who did not opt out to waive all future claims regarding Facebook's use of their name and likeness for its "Sponsored Stories" feature. *Fraley v. Facebook*, 966 F. Supp. 2d 939 (N.D. Cal. 2013). "Through this settlement Facebook will perfect its immunity from all other misappropriation claims arising from the Sponsored Stories program." Brief of *Amicus Curiae* EPIC, *Fraley v. Batman*, 638 Fed. App'x 594 (9th. Cir., 2016) (No. 13-17097).[8] The instant Settlement also requires absent class members to release all claims for injunctive relief that "arise out of, are based on, or relate in any way to the practices and claims that were alleged in, or could have been alleged in, the Action." Dkt. No. 252 at 4.

[7] https://epic.org/privacy/google/EPIC-et-al-Ltr-Google-Referrer-Header.pdf.
[8] https://epic.org/amicus/facebook/fraley/EPIC-Fraley-Amicus.pdf.

In *Marek v. Lane*, Chief Justice Roberts expressed "fundamental concerns" about the fairness of class action settlements that award *cy pres* funds but provide no monetary relief to the class and fail to enjoin the underlying conduct. *Marek v. Lane*, 134 S. Ct. 8 (2013) (Statement of C.J. Roberts respecting denial of cert.). *Lane* involved Facebook's "Beacon" program, which caused a Facebook user's online purchases to be posted on the user's wall for all her friends to see. *Id*. Although the Court denied the Petition for Writ of Certiorari, the Chief Justice wrote separately to express "fundamental concerns" over the fact that "the vast majority of Beacon's victims got neither" damages nor injunctive relief. *Id*. at 9. Roberts emphasized that, "[a]though Facebook promised to discontinue the 'Beacon' program itself . . . nothing in the settlement would preclude Facebook from reinstituting the same program with a new name." *Id*. at 10.

Such is the case here. Although Facebook has acknowledged its cessation of several practices, nothing in the Settlement prohibits Facebook from resuming these practices. Moreover, the changes to Facebook's privacy policy as part of the Settlement affirm that Facebook will continue scanning the content of private messages, notwithstanding the practices it claims to have ceased.

Chief Justice Roberts also found the settlement in *Lane* to be flawed because it barred a large number of Facebook users from bringing future claims:

> To top it off, the parties agreed to expand the settlement class barred from future litigation to include not just those individuals injured by

> Beacon during the brief period in which it was an opt-out program—the class proposed in the original complaint—but also those injured after Facebook had changed the program's default setting to opt in.

134 S. Ct. at 10. Similarly here, a vast amount of Facebook users—anyone who sent a message with a URL at any point between December 30, 2011 and March 1, 2017—are now prohibited from bringing future claims for injunctive relief. Dkt. No. 252 at 3.

EPIC shares Chief Justice Roberts' concerns about the fairness of these types of settlements. As we have explained:

> Settlements also offer defendants the possibility of escaping liability – even for future misconduct – with only superficial changes to their business practices. And class action attorneys will sometimes agree to allow companies to engage in practices that threaten the privacy interests of consumers. Surprisingly, courts have approved settlements where the defendant company is permitted to engage in the practice after settlement that was the reason for the original lawsuit.

Rotenberg & Jacobs, *supra*, at 2. This settlement bears the hallmarks of deficient settlements that EPIC has opposed in the past. Facebook is permitted to continue the conduct that was the basis for the suit, is only required to post a vague notice in its privacy policy, and absent class members are barred from obtaining injunctive relief from such conduct.

II. The proposed settlement does not require Facebook to change its business practices.

A. The proposed settlement sanctions Facebook's continued violations of ECPA.

Under the Settlement, Facebook will continue to scan the content of private messages. Facebook only acknowledges that it has stopped scanning private messages with respect to four discrete practices concerning privately shared URL links. Dkt. No. 252, at 3. But the disclosures mandated by the Settlement make clear that Facebook will continue to scan the content of private messages for other, undisclosed purposes. Facebook's "Data Policy" disclosure states that Facebook collects the "content and other information" that individuals provide when they "message or communicate with others." *Id*. And Facebook's proposed "Help Center" disclosure states, "we use tools to identify and store links shared in messages." *Id*. If Facebook had stopped all scanning of private messages, these disclosures would be unnecessary. And without injunctive relief, Facebook is free to engage in similar unlawful scanning in the future.

By permitting Facebook to continue scanning private messages, the Settlement sanctions conduct that violates the Electronic Communications Privacy Act 18 U.S.C. § 2510 *et seq.* ("ECPA"). At the motion to dismiss stage, the District Court found that Plaintiffs had presented strong evidence that Facebook's practices violated ECPA. In particular, the Court found that Facebook's scanning of private

messages constituted an "interception" under ECPA, and that the "ordinary course of business" and "consent" exceptions did not apply. Dkt. No. 43.

ECPA prohibits private messaging services from intercepting or redirecting the contents of private messages, or from using that information for a purpose beyond what is necessary for, or incidental to, using the service. 18 U.S.C. § 2510(4); *see also In re Google Inc. Privacy Policy Litig.*, No. 12-1382, 2013 WL 6248499 at *11 (N.D. Cal. Dec. 3, 2013) (defining "ordinary course of business" as an interception that "facilitates the transmission of the communication at issue or is incidental to the transmission of such communication"). Facebook used a "web crawler" device to intercept private messages for the purpose of, among other things, providing targeted advertising. The District Court, as well as other lower courts in this Circuit, have made clear that targeted advertising falls outside the "ordinary course of business" exception. Dkt. No. 43 at 8; *Google Privacy Policy*, 2013 WL 6248499 at *11. The District Court also found that Facebook's interception of privately shared URL links for the purpose of increasing the "like" count of websites fell outside the "ordinary course of business." Dkt. 43 at 8.

The District Court stopped short of saying conclusively that Facebook's practices constituted an "interception" within the meaning of ECPA. The Court stated that it had "no evidentiary record regarding the technical details of Facebook's handling of messages." Dkt. No. 43 at 12. ECPA liability, however,

must not turn on such technical details. If that were the case, companies would simply alter the technical specifications of their messaging services. This Court has cautioned that the term "intercepted" should not be given too narrow a meaning. *Noel v. Hall*, 568 F.3d 743, 750 (9th Cir. 2009). This Court explained that ECPA must be construed in light of rapidly changing technology. "ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002).

The First Circuit in *In Re Pharmatrak* rejected the idea that the term "interception" should turn on technical questions of when the message is intercepted. *In re Pharmatrak, Inc*., 329 F.3d 9, 22 (1st Cir. 2003) ("communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously"). Rather, ECPA must be understood within the broader 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. Facebook's use of a device to intercept private messages for the purpose of targeted advertising and increasing the "like" count of webpages is precisely the type of conduct that ECPA was designed to prohibit.

B. Class action settlements in privacy cases routinely require injunctive relief.

The absence of injunctive relief distinguishes this Settlement from other, similar settlements approved by courts within this Circuit. In *Matera v. Google*, the plaintiffs brought similar claims under ECPA and CIPA alleging that Google intercepted private email messages for targeted advertising. The Settlement enjoined Google from "all processing of email content that it applies prior to the point when the Gmail user can retrieve the email . . . that is used for Advertising Purposes." Order Granting Preliminary Approval of Class Action Settlement, *Matera v. Google*, No. 15-4062 (N.D. Cal. Aug. 31, 2017). The settlement also prohibited Google from using any information it previously obtained by scanning email messages for advertising purposes. *Id*. In fact, the court denied approval of the initial settlement agreement because, while it prohibited Google from scanning emails for the *sole* purpose of collecting advertising data, it would have permitted Google to scan emails for the "*dual purpose*" of detecting spam and malware and "obtaining information that would *later* be used for advertising purposes." *Matera v. Google*, No. 15-4062, 2017 WL 1365021, at *2 (N.D. Cal. Mar. 15, 2017) (emphasis in original). The court stated that, "it is not clear that the 'dual purpose' will bring Google into compliance with the Wiretap Act and CIPA." *Id*.

Here, Facebook's proposed changes clearly do not bring the company into compliance with ECPA and CIPA. Facebook's voluntary changes would only

guarantee that Facebook will not intercept private messages for a few, specific purposes. Facebook broadly retains the right to intercept the content of private messages for any other purpose it chooses, so long as it posts a vague notice in its privacy policy.

In *In re Yahoo Mail Litig.*, No. 13-4980, 2016 WL 4474612, (N.D. Cal. Aug. 25, 2016), the plaintiffs, as here, survived a motion to dismiss their claims under CIPA and the Stored Communications Act regarding Yahoo's "interception, storage, reading and scanning of email." Like *Matera*, the settlement provided a three-year injunction prohibiting Yahoo from intercepting, scanning, and analyzing email that is "in transit" for advertising purposes. *Id*. at *3. The court stressed that "Class Members may bring suit against Yahoo if Yahoo fails to carry out these changes or if Yahoo abandons these changes after three years. *Id*. at *5. The Class Members here have no such remedy if Facebook breaks its promises in the Settlement.

In this case Plaintiffs also sought, and the Settlement purports to provide, "declaratory relief." But there is no actual declaration that a single one of Facebook's practices violated ECPA or CIPA. Not only are Facebook's promises not enforced by an injunction, but the "declaratory relief" does not "declare" anything at all. The Settlement merely acknowledges that Facebook has ceased

certain practices—practices it is free to resume at any time—while also sanctioning conduct that was the basis for the suit.

III. Facebook's vague disclaimers buried in its privacy policy cannot provide the basis for consent.

Class Counsel claims that, in light of Facebook's new disclosures, Facebook users will have "consented" to Facebook intercepting their messages:

> Given that consent is a complete defense to Plaintiffs' ECPA and CIPA claims, these disclosures (along with the cessation of the challenged practices and disclosures discussed below) bring Facebook's business practices into compliance with the law, and allow Facebook users to decide whether to consent to allow Facebook to use the URLs they choose to send in Private Messages.

Dkt. No. 244 at 5. This theory of "consent" does not comport with ECPA, nor does it reflect the essential purpose of privacy law. EPIC objected to the settlement in *In Re Google Referrer Header* because there, as here, the parties claimed that Google users would have "consented" to Google's privacy invasions so long as Google posted notice of its practices in its privacy policy. In its prior *amicus* brief before this Court, EPIC explained that "generic notice is insufficient to establish meaningful consent" under ECPA to Facebook's specific practice of tracking Internet users when they visited health care websites and disclosed sensitive medical information. Brief of *Amicus Curiae* EPIC, *Smith v. Facebook*, 262 F. Supp. 3d 943, *appeal docketed*, No. 17-16206 (9th Cir. Jun. 9, 2017).

The issue presented in this case is the same as what EPIC previously addressed in *Smith* and *Google*. As EPIC has previously explained, a vague notice, buried on a web page, does not provide the basis for meaningful consent under ECPA, let alone consent to Facebook's specific message scanning practices that will continue under this settlement.

A. Consent under ECPA must be meaningful and specific.

Consent under ECPA "should not casually be inferred." *In re Google Inc. Gmail Litig.*, No. 13-md-02430-LHK, 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014) (quoting *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990). The defendant bears the burden of demonstrating that the plaintiff consented to the specific interception at issue. *In re Pharmatrak, Inc*., 329 F.3d 9, 19 (1st Cir. 2003). Mere "foreseeability of monitoring is insufficient to infer consent. Rather, the circumstances must indicate that a party to the communication knew that interception was likely and agreed to the monitoring." *United States v. Staves,* 383 F.3d 977, 981 (9th Cir. 2004); *see also Berry v. Funk,* 146 F.3d 1003, 1011 (D.C. Cir. 1998) ("Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."); *Watkins v. L.M. Berry & Co.,* 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the *capability* of monitoring alone cannot be considered implied consent.")

In the *Gmail* case, the district court found that consent to Google's terms of service regarding Google's scanning of emails for one purpose—to exclude objectionable content—did not establish consent for the purpose of "creating user profiles or providing targeted advertising." *In re Google Inc.*, No. 13-md-02430-LHK, 2013 WL 5423918, at *13 (N.D. Cal. Sept. 26, 2013). In addition, the court found that Google's statement that "advertisements may be targeted to the content of information stored on the Services," did not establish consent because it only demonstrated that "Google has the *capacity* to intercept communications, not that it will." *Id*. (emphasis in original).

The generic disclaimers that Google provided are similar to the disclaimers at issue here. For example, one of Google's notices stated that Google collected information for the purposes of "[p]roviding our services to users, including the display of customized content and advertising." 2013 WL 5423918, at *14. The court found that, "[n]othing in the Policies suggests that Google intercepts email communication in transit between users, and in fact, the policies obscure Google's intent to engage in such interceptions." *Id*.

Here, the District Court correctly held at the motion to dismiss stage that "any consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case—that is,

the scanning of message content for use in targeted advertising." Dkt. No. 43 at 16. The District Court remarked that:

> [w]hen asked, at the hearing, which portion of this policy provided notice of Facebook's practice of scanning users' messages, Facebook's counsel pointed to the disclosure that Facebook 'may use the information we received about you' for 'data analysis.' However, this disclosure is not specific enough to establish that users expressly consented to the scanning of the content of their messages—which are described as 'private messages'—for alleged use in targeted advertising.

Id. at 15.

Despite the District Court's findings, the disclosures mandated by the Settlement are no more specific. The "Help Center" notification simply states, "We use tools to identify and store links shared in messages, including a count of the number of times links are shared." Dkt No 252 at 4. And the "Data Policy" disclosure merely indicates that "Facebook collects the 'content and other information' that people provide when they 'message or communicate' with others." *Id*. A Facebook user reading these notifications would have no idea: 1) whether their particular communications will be intercepted, or 2) for what purpose their communications will be used. A Facebook user would only be aware that Facebook "use[s] tools to identify and store links" and collects "content and other information." Under ECPA, general knowledge of a broadly recurring practice is not actual knowledge of a *specific act*. *See Williams v. Poulos*, 11 F.3d 271 (1st Cir. 1993).

In the digital context, it is impossible to infer consent based on vague indications of how and when one's personal data might be processed. Rather, an individual must be presented with clear and particularized information. "Informed consent requires not only that data processors provide the relevant information, but also that individuals are aware of the mode and the extent of data processing to which they are consenting." Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 Harv. J.L. & Tech. 229, 246 (2004). "Freedom of choice in markets requires accurate information about choices and their consequences." Julie Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 Stan. L. Rev. 1373, 1396 (2000).

That is why under ECPA, the generic notice-and-consent model does not work. 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).

The Federal Trade Commission found that "consumers generally lack full understanding of the nature and extent of this collection and use" of their personal information." Fed. Trade Comm'n*, Protecting Consumer Privacy in an Era of Rapid Change* 60 (2012). The Commission concluded that the notice-and-choice model, "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*.

Mere notice is especially inadequate here, given the degree of uncertainty, lack of transparency, and lack of information that Facebook users possess. "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). "Given algorithmic secrecy, it's impossible to know exactly" what companies such as Facebook are doing with personal data. Frank Pasquale, *The Black Box Society* 39 (2015). If Facebook were to describe its practices in sufficient detail to give adequate notice under ECPA, its privacy policy would likely be too long and complex for the average user to comprehend. But at the very least, the parties cannot claim that Facebook has disclaimed liability under ECPA by providing two short, vague notices buried in a privacy policy.

B. A disclaimer buried in a privacy policy is insufficient to provide even general notice.

Even if Facebook's "Help Center" and "Data Policy" disclosures were sufficiently specific, they would still not provide the basis for consent under ECPA. This Court has held in the online false advertising context that disclosures hidden in hyperlinks, privacy policies or "terms and conditions" are insufficient to provide notice. *See FTC v. Cyberspace.com, LLC*, 453 F.3d 1196 (9th Cir. 2006); *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). In *Commerce Planet*, this Court affirmed a lower court's ruling that a disclosure, buried in a privacy policy, appearing at the bottom of the screen, without an affirmative opt-in requirement or a clear and conspicuous representation, was inadequate. *FTC v. Commerce Planet*, 815 F.3d 593 (9th Cir. 2016). 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. *Commerce Planet*, 878 F. Supp. 2d at 1070. The court in *Commerce Planet* relied on an expert who explained 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." *Id*.

The FTC has also endorsed the "net impressions" test adopted by this Circuit. *See* Fed. Trade Comm'n, *Dot Com Disclosures* (2013) (stating, "[t]he key

is the overall net impression of the ad"); *see also FTC v. Gill*, 265 F.3d 944, 956 (9th Cir. 2001) (applying the "net impressions" test). The Commission's guidelines state that disclosures must be presented "clearly and conspicuously" to ensure that an advertisement is not deceptive. *Id.* When evaluating the prominence of the disclosure, the Commission considers the size, color, and graphics of the disclosure, among other factors. *Id.* at 17.

The requirements for online advertising should apply with even more force to privacy policies. Consumers are far less likely to understand the sophisticated techniques behind the scanning of private messages than they are the terms for commercial transactions.

The disclosures mandated by the Settlement, however, follow none of the guidelines set out by this Court and the FTC. The Settlement does not require Facebook to obtain its users' affirmative, opt-in consent. Facebook is not required to give its users the opportunity to opt-out, nor must it display its notification in a clear and conspicuous manner. The Settlement does not even require Facebook to direct its users to view the disclosures when they log on to Facebook's homepage.

Rather, Facebook will merely post disclaimers buried in its Help Center and Data Policy without providing any notice to current Facebook users. To access Facebook's Help Center, users first have to click on a small question mark icon at the top of Facebook's homepage, and then click on another tiny hyperlink labeled

"Help Center."[9] But visiting the Help Center does not even direct users to Facebook's Data Policy. To access that, users have to scroll to the very bottom of the page and click on the tiny "privacy" link in gray font against a white background.[10] Furthermore, the Data Policy disclosure is buried within dozens of paragraphs of densely packed text regarding Facebook's data collection practices.[11] In sum, these disclosures commit almost every cardinal sin commanded by this Court and the FTC.

Facebook's own evidence submitted to this Court demonstrates that hardly anyone will see Facebook's disclosures. Facebook claims that its American Help Center page was visited 369,159 times for half the entire year of 2017. ER51. Compare that with its currently 214 million active users in the United States. *See* Statista, *Number of Facebook Users by Age in the U.S. as of January 2017*.[12] Assuming that every visit to the Facebook Help page was solely for the purpose of determining whether Facebook was scanning email and that each visit was by a unique user, approximately 0.1% of Facebook users would be aware of the practice that will continue under this settlement.

[9] https://www.facebook.com/.
[10] https://www.facebook.com/help/?ref=contextual.
[11] https://www.facebook.com/privacy/explanation.
[12] https://www.statista.com/statistics/398136/us-facebook-user-age-groups/ (last visited Jan. 29, 2018).

Disclosures that almost no Facebook user will read cannot provide the basis for consent under ECPA. This Court should reject a Settlement that provides no injunctive relief to the Class, no basis for Facebook to disclaim liability under ECPA, and no compensation to class members.

CONCLUSION

Amicus respectfully requests this Court vacate the lower court's approval of the settlement.

February 1, 2018

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
Alan Butler
Sam Lester
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Amicus

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULES

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 5,309 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(i). 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 2011 in 14 point Times New Roman.

Dated: February 1, 2018

/s/ Marc Rotenberg
Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on February 1, 2018, I electronically filed the foregoing Brief of *Amici Curiae* Electronic Privacy Information Center Support of Appellant with the Clerk of the United States Court of Appeals for the Ninth Circuit using the CM/ECF system. All parties are to this case will be served via the CM/ECF system.

Dated: February 1, 2018

/s/ Marc Rotenberg
Marc Rotenberg