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 all others similarly situated,

Plaintiffs-Appellants,

v.

FACEBOOK, INC.,

Defendant-Appellee,

and

AMERICAN CANCER SOCIETY, INC.; et al.,

Defendants.

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

APPELLANTS' REPLY BRIEF

Paul R. Kiesel (CA SBN 119854)
Jeffrey A. Koncius (CA SBN 189803)
Nicole Ramirez (CA SBN 279017)
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel.: 310-854-4444

Jay Barnes
Rod Chapel
BARNES & ASSOCIATES
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884

Attorneys for Plaintiffs
(Additional Attorneys Listed on Signature Page)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND REGULATIONS

OTHER AUTHORITIES

TREATISES

I. INTRODUCTION

This Court can only rule in Facebook's favor if it (1) ignores the well-pled facts of the Complaint, and (2) reverses Circuit precedent. Equally important, Facebook's position contradicts its own repeated statements and court filings. In June 2016, Facebook urged Congress to reject proposed legislation permitting the tracking of mere IP addresses without a warrant, arguing that the "information could reveal details about a person's … medical conditions [or] substance abuse history" and that permitting its tracking without a warrant would raise "civil liberties and human rights concerns[.]"[1] Then in August 2017, Facebook implored the Supreme Court in digital privacy cases to recognize that "courts should focus on the sensitivity of the data at issue and the circumstances of its transmission[.]"[2]

Facebook's position in the Supreme Court is correct. Here, however, Facebook asks this Court to do the opposite. The irony, and the great danger, is that if not reversed, the lower court's decision will also apply to and be used as precedent for government actors. If Facebook can claim its users consent to Facebook tracking their communications, regardless of the sensitivity of the communication's source or subject matter, based on a vague disclosure buried

[1] https://www.aclu.org/letter/ectr-coalition-letter

[2] *Carpenter v. United States*, Case No. 16-402, Amicus Brief of Technology Companies, at 12. Available at: http://www.scotusblog.com/wp-content/uploads/2017/08/16-402-ac-technology-companies.pdf

within a form contract no person is ever likely to read and that is contrary to more prominent promises Facebook and its third-party partners made to Plaintiffs, then so too can government agencies obtain "consent" to the same via buried and inconsistent disclosures.

This Court should reject Facebook's argument and uphold the Plaintiffs' fundamental rights to privacy.

II. FACEBOOK IGNORES AND MISREPRESENTS THE RECORD

Facebook's brief ignores or misrepresents the following key facts:

1. Facebook promised Plaintiffs, "Your privacy is very important to us. We designed our Data Policy to make important disclosures about how … we collect and can use your content and information." ER224-25, ¶60.

2. Unbeknownst to Plaintiffs, Facebook knowingly participated in the breach of explicit privacy promises that were made by health care entities that Facebook describes as its "third-party partners" in its SRR and privacy policies.[3] ER237-38, ¶¶ 107-13.

3. Plaintiffs' communications at issue were related to their health conditions, doctors, treatment, and payment for treatment, or, in the case of Plaintiff Jane Doe II, for her husband. ER243, ¶ 147; ER246, ¶161; ER249, ¶ 175.

Instead of addressing these facts, Facebook makes a massive misstatement: this case is not, as Facebook suggests, "about routine data collection and marketing practices that are commonplace on the Internet." AB1. To the contrary, Plaintiffs specifically alleged that the practices at issue are not necessary for websites to

[3] Facebook also takes this position in its briefs.

function and that "Facebook tracking does not occur on most medical websites." ER228, ¶ 79. Further, it is irrelevant whether Facebook's behavior is "routine" or "commonplace" if also based on misleading or fraudulent conduct.

Facebook proceeds with a series of unsupported non-sequiturs. Facebook's claim that it "does not share any names … or other contact information about specific people" (AB1) is neither relevant nor part of the Complaint. The same is true for Facebook's assertion that it "specifically offers users the opportunity to opt out of receiving advertising tailored to their use of websites and apps[.]" AB2.

Facebook's assertion that it "collect[s] information when you visit or use third-party websites and apps that use our Services" (AB10) is also irrelevant and misleading. This does not disclose that Facebook collects information about sensitive or detailed communications, rather, it merely suggests that Facebook receives information about the visited websites in general. Consider the following: https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook. Facebook informs users it may learn they visited Bloomberg.com, but does not disclose that Facebook also collects the exact communication, i.e. "How Rodrigo Duterte Turned Facebook Into a Weapon with a Little Help from Facebook."[4]

[4] *See U.S. v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2007) (explaining privacy distinctions between tracking of IP addresses, i.e. homepage only, and URLs with a full file path).

Facebook's statement that it receives information about "your use of our Services on those websites and apps" (AB10) is also not relevant. Here, Plaintiffs did not use Facebook's services on the websites in question. To the contrary, Plaintiffs were not aware of Facebook's presence and there is nothing in the Complaint to suggest Plaintiffs took any action to engage with Facebook while communicating with the health care websites.

Facebook asks the Court to consider in isolation its statement that it collects "information the developer or publisher of the app or website provides to you or us" (AB10). Such an approach is contrary to longstanding tort and contract law, both of which require alleged consent to be considered under the totality of circumstances, including examination of other clauses of a contract.

Facebook misstates the facts when it claims there is nothing to suggest its actual or constructive knowledge that Plaintiffs were mistaken about the data it was collecting. As detailed below, this unsubstantiated claim contradicts sixty-eight paragraphs of the Complaint.

Finally, Facebook is incorrect when it argues the "complaint alleges no facts to support the conclusion that the information supposedly disclosed to Facebook is personally identifiable, sensitive, or related to plaintiffs' health." AB39. Actually, Plaintiffs alleged their communications were "tracked, intercepted, and acquired by Facebook *connected to personally-identifiable information for each Plaintiff*" that

included "cookies and other identifiers" and explained how those particular identifiers were personally-identifiable to Facebook.[5] The information disclosed is sensitive because it included communications about Plaintiffs' medical providers and treatments including "intestine transplants," "metastatic melanoma," "pain medicine," "melanoma treatment options," and "health insurance and financial assistance" for the treatment of cancer. And Plaintiffs specifically alleged that the data was related to a "past, present, and future physical or mental health condition" of their own, or, in the case of Jane Doe II, her husband.[6] Thus, Facebook's unsubstantiated assertions do not overcome the Complaint's well-pled facts.

III. PLAINTIFFS DID NOT CONSENT TO FACEBOOK TRACKING THEIR HEALTH COMMUNICATIONS WITH ENTITIES THAT INCLUDE PLAINTIFFS' HEALTH CARE PROVIDERS

A. *Theofel* and *Norman-Bloodsaw* Are on Point

Facebook attempts to brush *Theofel* aside with its unsupported claim that, "Nothing in the complaint suggests that Facebook knew that plaintiffs were 'mistaken' about the data it was collecting." AB34, n.17. This assertion is false and misconstrues the law. The Complaint includes at least sixty-eight paragraphs alleging that Facebook knew or should have known that Plaintiffs and any ordinary

[5] ER230-31, ¶ 82; ER233-36, ¶¶ 92-103; ER239, ¶¶ 116, 120; ER242, ¶¶ 134-35; ER243, ¶ 146; ER244, ¶ 150; ER246, ¶ 160; ER247, ¶ 164; ER249-50, ¶¶ 174, 179; ER251, ¶¶ 187, 191; ER253-54, ¶¶ 201, 205.

[6] ER239, ¶ 117; ER241-42, ¶ 132; ER243, ¶ 147; ER246, ¶ 161; ER249, ¶¶ 175-77; ER251, ¶¶ 188-89; ER253, ¶ 202; ER257, ¶ 216(b).

person would be "mistaken as to the nature and quality of the invasion intended" based on the totality of circumstances.

First, Plaintiffs alleged the communications were with trusted health care entities and related to their health conditions and treatment for themselves or, in the case of Jane Doe II, her spouse.[7] Second, Plaintiffs alleged Facebook had actual and constructive knowledge that the trusted health care entities (described by Facebook as third-party partners) specifically promised that the communications would not be disclosed to third-parties like Facebook.[8] Third, Plaintiffs alleged Facebook knowingly acquired the communications in violation of third-party partners' promises of which Facebook was aware.[9] Facebook cannot sweep these sixty-eight paragraphs of the Complaint away with a footnote.[10]

Facebook's assertion also misstates the law. Plaintiffs need not establish that Facebook had actual knowledge. Constructive and imputed knowledge is enough if

---

[7] ER239, ¶ 117; ER246, ¶ 161; ER249, ¶¶ 175-77; ER251, ¶ 188; ER257, ¶ 216(b).

[8] ER231-32, ¶¶ 86-87; ER237-39, ¶¶ 108-14; ER240-41, ¶¶ 123-30; ER242-43, ¶¶ 138-45; ER245-46, ¶¶ 156-59; ER247-49, ¶¶ 169-73; ER249, ¶¶ 175-77; ER250-51, ¶¶ 184-86; ER252-53, ¶¶ 195-99; ER258, ¶¶ 222-24; ER274, ¶ 285.

[9] ER225-26, ¶¶ 65-70; ER239, ¶ 116; ER242, ¶ 134; ER243, ¶ 146; ER247, ¶ 163; ER249, ¶ 174; ER251, ¶ 187; ER253, ¶ 201.

[10] To the extent Facebook claims it lacked actual or constructive knowledge of the promises of its third-party partners, that is an issue of fact and cannot form the basis of the motion granted below.

the circumstances show that the defendant "probably … ought to have known" of the mistake. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004). Whether Facebook "probably ought to have known" is a question of fact.

Similarly, Facebook fails to distinguish *Norman-Bloodsaw v. Lawrence Berkley Lab.*, 135 F.3d 1260 (9th Cir. 1998), for which Facebook explains, "An agreement to a 'general' examination does not constitute consent to physical testing on every conceivable medical condition." AB33. Plaintiffs agree, but the word "general" comes from the *Bloodsaw* opinion, not the consent form at issue. The court described that form as a "written offer[] of employment expressly conditioned upon a 'medical examination,' 'medical approval,' or 'health evaluation.'" *Bloodsaw*, 135 F. 3d at 1264-65.

Nevertheless, this Court imposed a reasonableness requirement on the otherwise limitless contract provision, ruling that it would not construe the provision as consent to sensitive medical testing, but only to a "general examination." *Id*. Here, the facts are worse for Facebook because: (1) Facebook made a contrary promise in a more prominent part of the contract; (2) Facebook's third-party partners explicitly promised not to engage in the activity in question and Facebook was aware of those promises but participated in their breach anyway; and (3) the *Bloodsaw* plaintiffs had at least been expressly apprised that

defendants would be taking some medical information. There were no such details here and, as a result, Facebook's assertion fails.[11]

B. HIPAA and California Civil Code Section 1798.91 Apply

Facebook's argument on HIPAA and California Civil Code section 1798.91 misstates the facts and law.

Facebook misrepresents facts when it claims the Complaint does not allege "that the information supposedly disclosed to Facebook is personally identifiable, sensitive, or related to plaintiffs' health." AB39. To the contrary, Plaintiffs repeatedly alleged their communications and data were "tracked, intercepted, and acquired by Facebook *connected to personally-identifiable information* for each Plaintiff." *See, e.g.*, ER239, ¶ 116; ER243, ¶ 146; ER246, ¶ 160. Plaintiffs specified exactly which information was personally identifiable: cookies, IP address, unique device identifiers, geographic locations, and browser-fingerprinting. ER239, ¶¶ 116, 120; ER242, ¶¶ 134-35; ER243, ¶ 146; ER244, ¶ 150; ER246, ¶ 160; ER247, ¶ 164; ER249-50, ¶¶ 174, 179; ER251, ¶¶ 187, 191;

[11] For examples of government behavior that Facebook would immunize under its false "consent" test, see *Lebanese Agency Turned Android Phones Into Spy Devices*, N.Y. Times, Jan. 19, 2018 (available at https://www.nytimes.com/2018/01/18/technology/lebanese-intelligence-spy-android-phones.html?); and https://www.eff.org/press/releases/eff-and-lookout-uncover-new-malware-espionage-campaign-infecting-thousands-around; ("[A]ll Dark Caracal needed was application permissions that users themselves granted when they downloaded the apps, not realizing that they contained malware. This research shows it's not difficult to create a strategy allowing people and governments to spy on targets around the world.").

ER253-54, ¶¶ 201, 205. Plaintiffs explained how these data points are personally-identifiable and that they are PII as a matter of law under HIPAA. ER230-31, ¶ 82; ER233-36, ¶¶ 92-103. And they specifically alleged that their communications about "intestine transplants," "metastatic melanoma," and "pain medicine," among others, were related to a "past, present, and future physical or mental health condition." ER257, ¶ 216.

Furthermore, Facebook's "accessible to the public" defense is based on the same misrepresentation. AB40. For example, the URL http://my.clevelandclinic.org/search/resultsq=intesting%20transplant is "accessible to the public." But Facebook does not acquire the URL alone. Facebook also acquires PII of the person who made the communication. Under HIPAA, a name is not required. *See* 45 C.F.R. §164.514(b)(2) (prohibiting disclosure of identifiers "of the individual or of relatives[,]" including "geographic subdivisions smaller than a State;" "device identifiers;" URLs, IP addresses and "any other unique identif[ier]" that "could be used alone or in combination with other information to identify an individual."). From its code, Facebook learns the specific identity of the person who sent the communication.

Additionally, whether HIPAA creates a private right of action is not relevant to whether it sets the national standard of consent for disclosure or acquisition of medical information. In *Astra USA, Inc. v. Santa Clara Cty.*, the Court ruled there

could be no claim where the purported "statutory and contractual obligations … are one and the same." 563 U.S. 110, 117-18 (2011).[12] Here, Plaintiffs alleged eight causes of action that are beyond a mere HIPAA violation, i.e. not "one and the same."

Further, Facebook's status as a non-covered entity is not relevant. HIPAA's standards apply to non-covered entities. *See* 42 U.S.C. § 1320d-6(a)(2) (applying consent rules to "any person" who "knowingly" and "in violation of [HIPAA]" "obtains" protected information). If Facebook obtained similar data through the mail, it would not matter that Facebook was not a covered entity. The same is true here.

Facebook fails to specifically respond to California Civil Code section 1798.91, which has a different definition of "medical information" that clearly applies to the type of data acquired by Facebook. Further, section 1798.91 applies to Facebook because it "use[s] personal information for marketing or advertising products, goods, or services directly to individuals."

[12] *Cuyler v. U.S.*, 362 F.3d 949 (7th Cir. 2004), supports Plaintiffs. There, the Court ruled that statutes may "conclusively [] or presumptively establish[] that the violator failed to exercise due care," but ruled against the plaintiffs because the defendant had no duty to the persons injured. *Id*. at 952.

C. Even Absent HIPAA or Section 1798.91, the District Court Applied, and Facebook Urges, the Wrong Test for Consent[13]

The proper test for consent (in the absence of HIPAA or section 1798.91) comes from *Theofel*, *Norman-Bloodsaw*, and the Restatement (Second) of Torts. Consent must be "actual … rather than constructive[.]" *In re: Pharmatrak*, 329 F.3d 9, 19 (1st Cir. 2003). Even "overt manifestation[s] of assent" are not effective "if the defendant knew, or probably if he ought to have known … that the plaintiff was mistaken as to the nature and quality of the invasion intended." *Theofel*, 359 F.3d at 1073. "Even when no restriction is specified the reasonable interpretation of consent may limit it to acts at a reasonable time and place, or those reasonable in other respects." *Restatement (Second) of Torts* § 852A(3), cmt. g.

Here, the test for consent requires the Court to examine: the entirety of any agreements with Facebook; the nature of the entities with which Plaintiffs were exchanging communications; the sensitivity of the information at issue; reasonable expectations of privacy; and any promises concerning those communications –

[13] Contrary to Facebook's brief, Plaintiffs never agreed with its putative test for consent. AB20. Instead, Plaintiffs argued Facebook fails its own test. In order to, as Facebook formulates it, "have understood that Facebook was collecting the information at issue," a reasonable user would have to understand that Facebook was knowingly participating in the breach of explicit privacy promises made to users by Facebook's third-party partner medical websites, including their own providers. Such an understanding would contradict Facebook's primary privacy promise.

particularly promises of which Facebook had actual, constructive, or putative knowledge that came from Facebook's third-party partners.

D. Consent Is a Question of Fact

Facebook claims interpretation of its written statements is a question of law. AB20, n.6 (citing *Pure Wafer Inc. v. City of Prescott*, 845 F.3d 943, 961 (9th Cir. 2017)). But Facebook misrepresents *Pure Wafer*, where the majority found that remand for fact-finding was unnecessary because the District Court had already "considered extensive trial testimony, and made sufficient findings of fact." 845 F.3d at 954. *Pure Wafer* stands for the opposite of Facebook's proposition as here, no such fact-finding has occurred. At this stage, Plaintiffs' allegations must be taken as true and consent was not given.

E. Facebook Is Bound by the Promises of Its Third-Party Partners, Whether It Had Actual, Constructive, Imputed, or No Knowledge at All

Facebook claims it has no obligation to refrain from participating in breaches of promises made to Plaintiffs by Facebook's "third-party partners." AB10. This ignores that Plaintiffs alleged Facebook knew of those confidentiality promises but engaged in the complained of conduct anyway. *See, e.g.*, ER231-32, ¶¶ 86-87; ER274-75, ¶¶ 286-90; ER281, ¶317. Further, Facebook's arguments about its self-described "partners" turns common law on its head:

> By the general law of partnership, the act of each partner, during the continuance of the partnership and within the scope of its objects, binds all

> the others. It is considered the act of each and of all, resulting from a general and mutual delegation of authority. Each partner may, therefore, bind the partnership by his contracts in the partnership business . . . .

Bell v. Morrison, 26 U.S. 351, 370 (1828). Therefore, Facebook can and should be bound by those promises.

F. The District Court's Double-Standard for Facebook and Ordinary Consumers

Despite Plaintiffs' allegations, the District Court's Order imputes knowledge and consent to ordinary consumers based on a disclosure buried within Facebook's Privacy Policy that: (1) conflicts with Facebook's more prominent promises and those of its "third-party partners"; and (2) even the most sophisticated consumer is unlikely to read or understand. *See, e.g.*, Debra Cassens Weiss, Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print, ABA Journal (Oct. 20, 2010) ("Roberts admitted he doesn't usually read the computer jargon that is a condition of accessing websites."); *Berkson v. GoGo, LLC*, 97 F. Supp. 3d 359, 384 (E.D.N.Y. 2015) (referencing empirical studies which found "between 0.05% and 0.22% of online shoppers access online agreements"). At the same time, by ignoring Facebook's privacy promises and those of its partners, the Court below held that Facebook, one of the world's largest and most sophisticated technology companies, is not responsible for understanding and acting in accordance with the explicit privacy promises of its "third-party partners" who utilize Facebook's source code, that Facebook knew about.

Plaintiffs' imputed knowledge and alleged consent to Facebook's conduct is, at best, a legal fiction. But Facebook's knowledge of the privacy promises of its partners is a reality ignored by the District Court.

Plaintiffs ask this Court to adopt a consistent standard for all Internet users – whether ordinary consumers or sophisticated actors like Facebook. If Plaintiffs are to be held to Facebook's buried and contradictory disclosures, then so too must Facebook be held responsible for its knowledge of its own promises and those made by its partners from whom it profits. Here, that means Facebook's disclosures must be considered under the totality of circumstances and read in conjunction with the promises made by Facebook's partners.

G. Tort and Contract Law on Consent Are Consistent

For tort and statutory claims deriving from tort principles, the proper test for consent should be derived from the law of torts. Nevertheless, the test set forth above in Section III.C. is also consistent with contract law.

A contract "must be construed as a whole, with the various individual provisions interpreted together so as to give effect to all, if reasonably possible or practicable." *City of Atascadero v. Merrill Lynch*, 60 Cal. App. 4th 445, 473 (1998). "In deciding what the words of a contract meant to the parties," the fact-finder must "consider the whole contract, not just isolated parts" and "use each part to help … interpret the others, so that all the parts make sense when taken

together." CACI No. 317. Here, the trial court completely ignored Facebook's more prominent privacy promise to Plaintiffs that "Privacy is very important" and that the Data Policy was designed to "make important disclosures about … how we collect and can use your … information." Plaintiffs specifically referred to those promises for their good faith and fair dealing claim. ER289-90, ¶¶ 354-55.

"[W]ords in a contract are to be construed according to their plain, ordinary, popular or legal meaning, as the case may be." *Hayter Trucking Inc. v. Shell Western E & P, Inc.*, 18 Cal. App. 4th 1, 15 (1993). Where there is a dispute over the meaning of a particular contract term, the fact-finder may consider not just "the usual and ordinary meaning of the language used in the contract," but also "the circumstances surrounding the making of the contract." CACI No. 314; *see also City of Hope Nat'l Med. Ctr. v. Genentech, Inc.*, 43 Cal. 4th 375, 395 (2008). If the fact-finder still cannot discern the meaning of a term, it "must be interpreted most strongly against the party who prepared it," a rule that is "applied with particular force in the case of adhesion contracts[.]" *Badie v. Bank of America*, 67 Cal. App. 4th 779, 801 (1998).

Here, the parties dispute the meaning of Facebook's prominent "Your privacy is important" promise. Facebook asserts it is not "important" to disclose that it: (a) intercepts communications with its partners in violation of those partners' promises; (b) intercepts communications with medical websites,

including HIPAA-covered providers; and (c) records medical communications and information for direct marketing purposes. ER290, ¶ 355. Plaintiffs disagree. Under California law, under which Facebook's contract is to be interpreted (ER211, ¶ 20), the fact-finder may look beyond the contract itself to "the circumstances surrounding" its making. Here, those circumstances are such that, even under contract interpretation, this Court should rule as a matter of law that Plaintiffs did not agree to a contract that would permit Facebook to knowingly violate Plaintiffs' privacy when communicating with Facebook's third-party medical website partners.

The District Court also erred in failing to consider those terms in light of the covenant of good faith and fair dealing. "In the case of a contradictory and ambiguous contract, however, the implied covenant may be applied to aid in construction." *April Enters. v. KTTV*, 147 Cal. App. 3d 805, 816 (1983). In *April Enterprises*, the court refused to give effect to an unambiguous term that gave the defendant the unfettered right to delete videotapes, finding that it must reconcile "conflicting terms of the contract" and could only do so by placing a reasonable limitation on the seemingly unrestrained clause in question.

Here, interpretation of Facebook's disclosures must also be construed in light of the covenant. Facebook claims it has the absolute right to acquire data about its users regardless of the sensitivity of source or subject, but contract law

imposes an obligation of good faith and fair dealing. Facebook's more prominent privacy promises and the totality of the circumstances surrounding the activity in question lead to only one conclusion: Facebook's buried term is not an unconditional license to participate with its third-party partners in the breach of privacy promises made to Facebook users in violation of Facebook's first privacy promise. Neither does it permit Facebook to track users' communications with medical websites, nor to use their medical data for marketing.

Finally, there is a contract law corollary to Restatement (Second) of Torts section 892B. "Unilateral mistake is ground for relief where the mistake is due to the fault of the other party or the other party knows or has reason to know of the mistake." *Architects & Contractors Est. Svc., Inc. v. Smith*, 164 Cal. App. 3d 1001, 1007-08 (1985). Plaintiffs repeatedly alleged they had no knowledge of Facebook's predatory scheme and that Facebook knew, or should have known, the same.

IV. PLAINTIFFS ADEQUATELY PLED CLAIMS[14]

A. The ECPA Claim Is Proper

1. Facebook is not a party to Plaintiffs' communications with health care entities

Facebook does not offer a definition of "party to the communication." To do so would expose the absurdity – for the definition to be gleaned from Facebook's brief is that a "party to the communication" is "anyone who receives data directly *from the device* of the alleged victim." AB44-49.

Facebook's logic creates a wiretap tautology that even *Google Cookie* recognized. "Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient. As the intended recipient of a communication is necessarily one of its parties, and the defendants were the intended recipients of the GET requests acquired here, the defendants were parties to the transmissions at issue in this case." *In re: Google Cookie*, 806 F.3d 125, 143 (3d Cir. 2015). Here, Facebook was not an intended recipient of any communication that Plaintiffs sent or received to or from their health care institutions.

[14] Facebook mistakenly argues that "Plaintiffs' opening brief does not address the claims they brought against Facebook for negligence per se and quantum meruit." AB15 n.4. In fact, Plaintiffs made clear that the court below wholly failed to address those claims. OB12 (noting "The Order is devoid of analysis relating to Plaintiffs' claims for: (1) negligence per se; (2) breach of the duty of good faith and fair dealing; (3) fraud; and (4) quantum meruit."). And this is despite Plaintiffs fully briefing those claims below. ER140-46.

Facebook's fundamental error is that it conflates the Plaintiffs (people) with the things (devices and/or software) that they use for communications. Plaintiffs never sent any communication to Facebook. Instead, their browser was commandeered by Facebook code, which works as an automatic routing program, without Plaintiffs' knowledge, consent, or action. ER222, ¶ 52. Automatic routing programs are interceptors under the ECPA. *In re: Pharmatrak, Inc.*, 329 F.3d at 22 ("NETcompare was effectively an automatic routing program," i.e. "code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak).").

If Facebook is right, Plaintiffs cannot think of a single wiretap scenario involving a communications device that would be protected by the Wiretap Act because every interception of a communication sent via telephone or computer must start with the victim's chosen device and end with the interceptor. A ruling in Facebook's favor effectively repeals the Wiretap Act.

Facebook further claims as dispositive that its "acquisition" occurred through "a separate channel than the path of the actual communication[s]" between Plaintiffs and the health care entities. AB45. Again, Facebook argues for an exception that would swallow the statute. If Facebook is right, it would be impossible to violate the Wiretap Act: every interception occurs through a separate channel than the path of the communications between the known parties to the

communication, otherwise it would not be an interception. *See Pharmatrak*, 329 F.3d at 22 (rejecting argument that "there was no interception because 'there were always two separate communications: one between the Web user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak.'").

Contra Facebook's brief, *Konop* holds that a communication is intercepted where it is "*acquired during transmission.*" *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). This is "consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival," but does not require stoppage, seizure, or interruption "in progress or course" because that is not how wiretaps work. There is no stoppage, seizure, or interruption of communications between wiretap victims and their co-communicants. Instead, the original line of communication continues unabated – and the interception occurs whenever contents of a communication are diverted through a separate path contemporaneous to their transmission between the known participating parties. Here, Plaintiffs alleged Facebook acquired the contents of their sensitive communications contemporaneous to, and in the middle of, the communications Plaintiffs exchanged with the health care entities. This passes the *Konop* test.[15]

[15] *Konop* is factually distinct. The *Konop* defendant gained unauthorized access to a 'secure' website where the contents of the plaintiffs' communications had been stored on a website bulletin board on a server for an unspecified period of time, but

Facebook's claim that it did not "bug" the communications in question because "it received a separate communication from the plaintiffs' own *browser*" (AB48) ignores that Facebook only acquired the communication because its computer code commandeered Plaintiffs' devices without their knowledge or consent.[16]

The law enforcement impersonator cases, such as *U.S. v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964), are inapposite. There, the alleged victim knew they were having a conversation with someone and purposefully speaking directly to the alleged wiretapper. The fact that the recipient had disguised who they were did not negate that the alleged victim had purposefully communicated with them. Here, Plaintiffs had no knowledge that Facebook (or anyone else) was acquiring information about their communications with the health care entities.

Finally, Facebook's argument works an absurd result that is contrary to the ECPA's purpose and plain language. The "paramount objective of the [ECPA] is to protect effectively the privacy of communications." *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013). The ECPA "extend[ed] to data and electronic transmissions

---

far longer than milliseconds. Here, Facebook's acquisition occurred contemporaneous to the communications and, in fact, before the communications between plaintiffs and the health care entities were complete. ER270-71, ¶ 267.

[16] For real-world examples of the danger of Facebook's argument, see *How Spy Tech Firms Let Governments See Everything on a Smartphone*, N.Y. Times, Sept. 2, 2016; https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?.

the same protection already afforded to oral and wire communications." *Pharmatrak*, 329 F.3d at 18.

Where the ECPA does not specifically define a phrase, this Circuit "must give the term its ordinary meaning." *Joffe*, 746 F.3d at 927. In *Joffe*, this Circuit rejected Google's "technical definition" of an undefined term in the ECPA because it "d[id] not conform with the common understanding held contemporaneous with the enacting Congress" and was "in tension with how Congress – and virtually everyone else – uses the phrase." *Id*. at 927-28. Likewise here, the communications were between Plaintiffs and health care entities, and no ordinary person would say that Facebook was a "party" to those communications.

2. Facebook's actions had tortious intent

The fact that Facebook wished to profit from its conduct does not absolve it of tortious intent. Theft and misappropriation are employed for profit – and are tortious. If Facebook acquired the same data through some other means without authorization and then sold advertising based on that information, Plaintiffs would still have a claim. Accordingly, Facebook's conduct pulls it within the "tortious intent" section of the Wiretap Act.

3. Facebook acquired content

Content includes "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). "'[C]ontents' refers to the

intended message conveyed by the communication[.]" *In re: Zynga Privacy Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014). In *Zynga*, the plaintiffs had only alleged interception of Facebook profile URLs that revealed a username or group name. For example, www.facebook.com/nytimes or www.facebook.com/bedelman.[17] Accordingly, a Facebook group or username was not enough to constitute "content." However, *Zynga* pointed out "search term[s] and similar communication[s]" made by a user contain content.[18] This is such a case.

Further, Facebook wrongly suggests that because URLs may contain some location information, that they are mutually exclusive to content. AB50. In a *Declassified Opinion*, the NSA took a similar position to Facebook, but the Foreign Intelligence Surveillance Court rejected the NSA/Facebook argument, holding that "DRAS and content are not mutually exclusive categories." *See* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf at 31-32 (explaining DRAS and "content" are not "mutually exclusive categories."). Legislative history shows Congress expressly disagreed with Facebook. *See H.Rep. 107-236* at 53 (PATRIOT Act history explaining, "the portion of a URL specifying Web search terms or the name of a requested file or article" is content under the

[17] AB8-9, n.7.

[18] Facebook's argument that Plaintiffs "miss[] the point" by insisting the information includes content in the form of "search queries" (AB50) is contrary to *Zynga*.

ECPA.)[19] Accordingly, this Circuit should reject Facebook's request to expand the PATRIOT Act beyond that which Congress and the Executive Branch deemed necessary (or constitutional) just one month after the attacks of September 11.

4. Plaintiffs adequately alleged use of a device

Facebook wrongly claims that *Carrier IQ* did not consider whether software is a "device" (AB51 n.27). *See In re: Carrier IQ*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) ("[T]he Carrier IQ Software is a '[d]evice' for [p]urposes of the Wiretap Act."). Further, *Szymuszkiewicz* is not inconsistent with any binding precedent from this Circuit, and *Crowley* and *Potter* are inapposite. *See U. S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001); *Potter v. Havlicek*, 2008 U.S. Dist. LEXIS 122211 (S.D. Ohio June 23, 2008). In *Crowley*, Amazon was not an interceptor where the communications occurred at Amazon.com because it "acted as no more than the second party to a communication[.]" 166 F. Supp. 2d at 1266. Here, the interceptions did not occur while Plaintiffs were on the Facebook.com website. In *Potter*, the court rejected the defendant ex-husband's attempted interpleading of a company that designed the software he used to spy on his spouse. 2008 U.S. Dist. LEXIS 122211, 23-24. The court concluded that "computer software alone" is not

[19] To this point, Congresswoman Zoe Lofgren explained that in discussions "with the Justice Department and the [Bush] White House, they made it very clear that they agreed with this, and this is not an argument. It is just a clarification[.]" *See H.Rep. 107-236* at 294-95.

a "device" because the ECPA "does not contemplate imposing civil liability on software manufacturers and distributors for the activities of third parties[.]" *Id.* Similar to its other assertions, if Facebook prevails with its arguments that the types of tools used here are not "devices," then it has effectively repealed the ECPA for the Internet.

B. Plaintiffs Stated CIPA Claims

1. California Penal Code section 631(a)

Plaintiffs re-assert their arguments in their opening brief regarding "content" and "party to the communication." For "device" under CIPA, Facebook again misstates the facts. Plaintiffs alleged seven devices, not just cookies and, further, CIPA never mentions "device" but instead prohibits interceptions "by means of any machine, instrument, or contrivance, or in any other manner." Facebook's citation to the rule that "general words must be construed as restricted to things of the same type as those specifically enumerated" does not apply here, but does not change the result even if it did. The hardware and software alleged as devices by Plaintiffs are "things of the same type" as "machines, instruments, or contrivances" in that they are items designed to acquire communications in real-time.

2. California Penal Code section 632

Under section 632(c), "confidential communication means any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but

excludes a communication … in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." California courts holding that Internet communications are not confidential have done so in much different circumstances than here. In *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010), the court rejected the child predator's section 632 defense where: (1) "the Yahoo! Privacy policy indicated that chat dialogues may be shared for the purpose of investigating or preventing illegal activities"; (2) "defendant was communicating online with a person whom he did not know"; and (3) "defendant expressed concern that [the victim's] mother would discover their communications[.]" No such circumstances are present here. Instead, Plaintiffs communicated with health care entities that expressly promised not to disclose their information.

The correct ruling here is that Facebook is not a party to the communications in question so section 632 does not apply. However, if the Court deems Facebook a "party" despite the absence of Plaintiffs' knowledge of Facebook's presence, it must then also conclude that Plaintiffs had a reasonable expectation that Facebook (a "party" of which they were not even aware) would not record these communications.[20]

[20] Plaintiffs' device discussion applies with equal authority here. In addition, Facebook's servers on which it records the communications undoubtedly qualify under section 632(b) as a "recording device."

C. Intrusion Upon Seclusion / Constitutional Invasion of Privacy

1. Plaintiffs had a reasonable expectation of privacy in the data

Facebook's claim that "Internet users have no expectation of privacy in [the identities of] … the websites they visit" is wrong[21] and irrelevant. AB55 (citing *Forrester*, 512 F.3d at 510). Here, the Complaint is not based on tracking websites Plaintiffs visited but, instead, on Facebook's unauthorized acquisition of the full details of Plaintiffs' communications with medical websites. *Forrester* itself points out the difference. 512 F.3d at 510 n.5-6.[22] Other sources of Plaintiffs' reasonable expectations of privacy are alleged in the Complaint and their Opening Brief, including state and federal statutes protecting the communications and information at issue; Facebook's prominent privacy promise; and the explicit promises of Facebook's partner medical websites.

[21] Facebook is correct that the legal standards that apply to a pen register device (i.e. one that records phone numbers dialed or IP addresses visited) falls short of the Fourth Amendment's reasonable expectation of privacy test. Nevertheless, Americans retain a reasonable expectation of privacy that a private party will not install a pen register on their communication devices without consent. *See* 18 U.S.C. § 3121 (prohibiting use of pen register except in limited circumstances that do not apply here).

[22] Regarding other sources of Plaintiffs' reasonable expectation of privacy, *see Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("[C]ertain types of data are also qualitatively different. An Internet search and browsing history … could reveal an individual's private interests or concerns – perhaps a search for symptoms of disease, coupled with frequent visits to WebMD.").

Facebook's claim that Plaintiffs "failed to take the available measures to safeguard their information" is fictional. In reality, there were no "available measures" short of not communicating with their health care entities. And, that would require knowledge that Facebook would engage in the activity if Plaintiffs failed to take action. Plaintiffs had no such knowledge.

2. Highly offensive / serious invasion is a question of fact

The cases cited by Facebook are of no moment. Other than the other Facebook case on appeal from the same District Court, the cited cases only involved disclosure or use of names or zip codes. *See Low v. LinkedIn*, 900 F. Supp. 2d 1010, 1028 (N.D. Cal. 2012) (involving disclosure of LinkedIn ID and URL of LinkedIn profile page); *Google Privacy Policy Litig.*, 58 F. Supp. 3d 968, 980, 987 (N.D. Cal. 2014) (involving defendant who disclosed 'a few bytes of name, email address, and zip code information' to third-parties); *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (involving defendant who asked plaintiff for zip code at brick-and-mortar checkout for marketing).

Additionally, Facebook's "legitimate business reasons" defense (AB57) is misplaced. *See Campbell v. Facebook*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014) (finding defendant "cannot simply adopt any revenue-generating practice and deem it 'ordinary' by its own subjective standard."); *Matera v. Google*, 2016 U.S. Dist. LEXIS 107918, *44 (N.D. Cal. Aug. 12, 2016); *Opperman v. Path*, 87 F. Supp. 3d

1018, 1061 (N.D. Cal. 2014) ("[T]he Court does not believe that the surreptitious theft of personal contact information … has come to be qualified as 'routine commercial behavior.'").

No court has ever held that activity like Facebook's here is not highly offensive. To the contrary, the trend is clear: unauthorized access to, or negligent disclosure of, this type of data is actionable. Indeed, allegations involving less offensive conduct have been allowed to proceed. *See In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3d Cir. 2016) (disclosure of videos viewed on children's website); *Opperman*, 87 F. Supp. 3d 1018 (disclosure of contact lists). Moreover, other digital privacy intrusion cases have proceeded which are offensive in scope, but not necessarily specific. *See In re: Google Cookie*, 806 F.3d 125 (broad tracking of communications on Internet); *Ung v. Facebook, Inc.*, Case No. 1-12-cv-217245 (Santa Clara Cty Jul. 2, 2012) (same). Here, the data is as sensitive as it gets – and its unauthorized acquisition and use is both highly offensive and a serious invasion of privacy.

3. Plaintiffs' claim for breach of the implied covenant is appropriate

Breach of the implied covenant of good faith and fair dealing can be based on conduct that does not technically violate the contract's express terms. *See Waller v. Truck Ins. Exch.*, 11 Cal. 4th 1, 36 (1995) ("[W]here a contracting party had an obligation to deal fairly with its contracting partner in calculating license

fees, it violated that duty by using a method that unfairly undervalued fees owed even if there was no express contractual obligation to calculate them differently."); *Ladd v. Warner Bros. Entm't, Inc.*, 184 Cal. App. 4th 1298, 1308 (2010). Further, a claim for breach of the implied covenant is not duplicative of a contract claim where the defendant acted in bad faith to frustrate a contract's benefits. *Celador Internat'l Ltd. v. The Walt Disney Co.*, 347 F. Supp. 2d 846, 853 (C.D. Cal. 2004); *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990). Here, Plaintiffs alleged that Facebook acted in bad faith to frustrate its contract with Plaintiffs. ER 288-91, ¶¶ 348-62.

4. Fraud is adequately pled

Facebook made a misrepresentation in its privacy promise and omitted material fact when, having promised that privacy was important and to make important disclosures, it failed to disclose the alleged activity. Plaintiffs alleged the misrepresentation and omissions were made with "intent to deceive" or "to induce him to enter into the contract." *See* ER291, ¶¶ 364-66. Plaintiffs also alleged reliance. *See* ER292, ¶ 366. For damages, Plaintiffs adequately alleged unjust enrichment (ER292, ¶ 368), the existence of a market for, and lost value of PII (ER222-23, ¶¶ 53-57; ER291, ¶ 362), and general damages for invasion of their privacy (ER279, ¶ 304). *See In re: Facebook Privacy Litig.*, 572 Fed.App'x 494 (9th Cir. 2014) (unpublished) (dissemination of personal information and lost sales

value adequate allegation of damages for contract and fraud claims) cited by *In re: Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d 953, 993-95 (N.D. Cal. 2016); *In re: Anthem II*, 2016 U.S. Dist. LEXIS 70594, at *129 (N.D. Cal. May 27, 2016).

V. CONCLUSION

It is respectfully submitted based on the foregoing, and the arguments set out in Plaintiffs' opening brief, that the order appealed from be reversed.

DATED: January 22, 2018

Respectfully,

KIESEL LAW LLP

By: */s/ Jeffrey A. Koncius*

Paul R. Kiesel
kiesel@kiesel.law
Jeffrey A. Koncius
koncius@kiesel.law
Nicole Ramirez
ramirez@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Tel.: 310-854-4444
Fax: 310-854-0812

THE GORNY LAW FIRM, LC

Stephen M. Gorny
steve@gornylawfirm.com
Chris Dandurand
chris@gornylawfirm.com
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

BARNES & ASSOCIATES

Jay Barnes
jaybarnes5@zoho.com
Rod Chapel
rod.chapel@gmail.com
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

EICHEN CRUTCHLOW ZASLOW & McELROY

Barry. R. Eichen
beichen@njadvocates.com
Evan J. Rosenberg
erosenberg@njadvocates.com
Ashley A. Smith
asmith@njadvocates.com
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

THE SIMON LAW FIRM, P.C.

Amy Gunn
agunn@simonlawpc.com
800 Market St., Ste. 1700
St. Louis, MO 63101
Tel.: 314-241-2929
Fax: 314-241-2029

BERGMANIS LAW FIRM, L.L.C.

Andrew Lyskowski
alyskowski@ozarklawcenter.com
380 W. Hwy. 54, Ste. 201
Camdenton, MO 65020
Tel.: 573-346-2111
Fax: 573-346-5885

CERTIFICATE OF SERVICE

I hereby certify that on January 22, 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 appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

DATED: January 22, 2018 **KIESEL LAW LLP**

By: */s/ Jeffrey A. Koncius*
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

Form 8. Certificate of Compliance Pursuant to 9th Circuit Rules 28.1-1(f), 29-2(c)(2) and (3), 32-1, 32-2 or 32-4 for Case Number 17-16206

Note: This form must be signed by the attorney or unrepresented litigant *and attached to the end of the brief.*

I certify that (*check appropriate option*):

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 28.1-1.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☒ This brief complies with the length limits permitted by Ninth Circuit Rule 32-1.
The brief is [6,997] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 32-2(b).
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable, and is filed by (1) ☐ separately represented parties; (2) ☐ a party or parties filing a single brief in response to multiple briefs; or (3) ☐ a party or parties filing a single brief in response to a longer joint brief filed under Rule 32-2(b). The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the longer length limit authorized by court order dated [ ]
The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable.

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 32-2 (a) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32 (f), if applicable. The brief's type size and type face comply with Fed. R .App. P. 32(a)(5) and (6).

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 29-2 (c)(2) or (3) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits set forth at Ninth Circuit Rule 32-4.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Signature of Attorney or Unrepresented Litigant: /s/ Jeffrey A. Koncius

Date: Jan 22, 2018

("s/" plus typed name is acceptable for electronically-filed documents)