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' OPENING 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

RULES

STATUTES

REGULATIONS

TREATISES

OTHER AUTHORITIES

JURISDICTIONAL STATEMENT

The United States District Court for the Northern District of California properly exercised jurisdiction under 28 U.S.C. section 1331 because this case arises in part under the laws of the United States, including 18 U.S.C. section 2520. The District Court exercised supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. section 1367 because they are related to and arise out of the same case and controversy as the federal claims. The Ninth Circuit has jurisdiction over this appeal. 28 U.S.C. § 1291. This appeal is from a May 9, 2017 order granting Defendants' motion to dismiss without leave to amend. ER002. The appeal as to Defendant Facebook, Inc., only, was timely filed on June 8, 2017. ER018; Fed. R. App. P. 4(a).

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

1. Did the District Court err in dismissing all of Plaintiffs' claims based on a factual finding that they consented to Facebook's interception, acquisition, and use of their communications with health care websites when, in fact, Plaintiffs specifically alleged that they did not consent?
2. Did the District Court err in determining that communications Plaintiffs exchanged with their own health care providers (or, in the case of Jane Doe II, her husband's providers) which relate to their past, present, and/or future physical health and condition are not protected by law under the Health

Insurance Portability and Accountability Act of 1996, 42 U.S.C. section 1320d, et seq. ("HIPAA"), California Civil Code section 1798.91, custom, or enforceable duty based on promises made by the health care providers?

3. Did the District Court err in dismissing Plaintiffs' claims against Facebook for breach of the duty of good faith and fair dealing?

4. Did the District Court err in dismissing Plaintiffs' claims against Facebook for fraud under California Civil Code sections 1572 and 1573?

5. Did the District Court err in not permitting Plaintiffs' claims to proceed against Facebook for violations of the Electronic Communications Privacy Act of 1986, 18 U.S.C. section 2510, *et seq*. ("ECPA"), violations of the California Invasion of Privacy Act, California Penal Code section 630, *et seq*. ("CIPA"), intrusion upon seclusion, and invasion of privacy?

STATEMENT OF THE CASE

I. INTRODUCTION

This case presents important questions about the future of privacy: Is there any legal limit to the data that a social networking company is permitted to acquire about its users' communications outside of the social network's website? Can a social networking company, via computer code designed by the social networking company and from which it profits, legally obtain information about users' confidential communications with health care providers in knowing violation of

the privacy promises those websites have made to its users? Plaintiffs submit that there are limits which when exceeded are actionable, contrary to the court's holding below.

II. BASIC FACTS OF THE CASE

A. Overview

Plaintiffs exchanged communications with trusted health care entities about their medical conditions, doctors, treatment, and finances. The health care entities, including some of the Plaintiffs' own health care providers, each explicitly promised not to disclose Plaintiffs' personally identifiable information ("PII") to third parties. Facebook had actual or constructive knowledge of those privacy promises, yet, Facebook knowingly participated in their breach by acquiring PII and the substance of Plaintiffs' communications with the health care websites contemporaneous to their making. Facebook then used the data acquired to sell advertising targeted by medical interests.

B. The Privacy Promises Made by Health Care Providers and Non-Profit Organizations Plaintiffs Communicated With

When read in context, no one would have understood that Facebook and the health care entities were exchanging PII about the Plaintiffs because the disclosures included specific promises not to do so (and Facebook knew about those promises). For example:

- MD Anderson explicitly promised, "Under no circumstances will we ever disclose (to a third party) personal information about individual medical conditions or interests, except when we believe in good faith that the law requires it." ER400-03.

- Cancer.org promised, "Your health-related information is privileged and confidential and will not be shared or released to any organization or business entity other than those affiliated with or working in conjunction with ACS as follows: [listing non-applicable circumstances]," and "We do not disclose personally identifiable information to those operating linked sites." ER347-53.

- Cancer.net. promised, "ASCO will only disclose your PII to third-parties under the following circumstances [listing non-applicable circumstances]." ER354-67.

- Melanoma.org promised, "We do not sell or share your Personal Data with Third Party Companies." ER368-73.

- Shawnee Mission promised, "As a general rule, we will not disclose your personally identifiable information to any unaffiliated third party, except when we have your permission or under special circumstances[.]" ER374-82.

- 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." ER396-99.

- Barnes Jewish Hospital's "Privacy Policy" assured users that it complies with HIPAA and that it is "required by law to protect the privacy of your protected health information." ER383-95.

C. Specific Allegations of Plaintiff Jane Doe I

Plaintiff Jane Doe I exchanged communications with her health care provider (Shawnee Mission Hospital) about her doctor (Dr. Ashcraft) and

treatment (pain management and spine treatment) via her health care provider's website. ER246, ¶¶ 161-62. These communications "relat[ed] to pain management and her particular doctor" and were "related to [her] 'past, present, and future physical or mental health or condition.'" ER246, ¶ 161; ER257, ¶ 216(b). Shawnee Mission Hospital specifically "promise[d] not to share personally-identifiable information of its patients and website users with third-parties" like Facebook, and Facebook had "actual and constructive knowledge" of this promise. ER232, ¶ 87; ER245-46, ¶¶ 156-59. Despite her health care provider's explicit promise and Facebook's knowledge of it, Plaintiff Jane Doe I's health-related communications with Shawnee Mission Hospital were "disclosed to, tracked, intercepted, and acquired by Facebook" connected to her PII. ER246, ¶ 160.

D. Specific Allegations of Plaintiff Jane Doe II

Plaintiff Jane Doe II exchanged communications with her husband's health care providers (BJC Healthcare and Cleveland Clinic) about his doctors (Drs. Hunt and Jain) and treatments (intestine transplant). ER249, ¶¶ 175-76; ER251, ¶¶ 188-89. These communications "relat[ed] to a sensitive medical condition and her husband's doctor," "relat[ed] to her family's health care treatment and their doctors," and related to "past, present, and future physical or mental health or condition[s]." ER249, ¶¶ 175-77; ER251, ¶¶ 188-89; ER257, ¶ 216(b). These health care providers specifically promised not to share PII about their patients or

website users with third parties like Facebook. BJC further assured users on its website that it complied with HIPAA. ER247-48, ¶¶ 169-71.

Likewise, Cleveland Clinic promised that it "does not share any personally identifiable information of any individual with any third party unrelated to Cleveland Clinic, except in situations where [it] must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization." ER250, ¶ 184.

Defendant Facebook has "actual and constructive knowledge" of these promises. ER232, ¶ 87; ER249, ¶¶ 172-73; ER251, ¶¶ 185-86. Yet, despite these promises and Facebook's knowledge of them, Jane Doe II's health-related communications were "disclosed to, tracked, intercepted, and acquired by Facebook" connected to information that personally identified her to Facebook. ER249, ¶ 174; ER251, ¶ 187.

E. Specific Allegations of Plaintiff Winston Smith

Plaintiff Winston Smith exchanged communications with health care providers and trusted health care non-profit organizations about cancer and cancer treatment – in particular, melanoma. ER239, ¶ 117; ER241-42, ¶ 132; ER243, ¶ 147; ER253, ¶ 202. These communications related to a "past, present, and future physical or mental health or condition" of Plaintiff Smith. ER257, ¶ 216(b). The providers and non-profit organizations with which Smith communicated

specifically promised not to share PII about users (including patients and potential patients) with third parties like Facebook. ER237-38, ¶¶ 108-12; ER240-41, ¶¶ 123-28; ER242-43, ¶¶ 138-43; ER252-53, ¶¶ 195-97. Facebook had actual and constructive knowledge of these promises. ER232, ¶ 87; ER238-39, ¶¶ 113-14; ER241, ¶¶ 129-30; ER243, ¶¶ 144-45; ER253, ¶¶ 198-99. Despite these promises and Facebook's knowledge of them, Winston Smith's health-related communications were "disclosed to, tracked, intercepted, and acquired by Facebook" connected to information that personally identified him to Facebook. ER239, ¶ 119; ER242, ¶ 134; ER243, ¶ 146; ER253, ¶ 201.

F. Plaintiffs' Relationships with Facebook

Plaintiffs are registered users of Facebook who completed Facebook's registration upon sign-up for the social network. ER210, ¶¶ 6-8; ER224, ¶¶ 58-59. The very first paragraph of Facebook's Statement of Rights and Responsibilities ("SRR") makes the following promise to registered users:

> *Your privacy is very important to us*. We designed our Data Policy to make *important disclosures* about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.

ER224-25, ¶ 60 (emphasis added).

Despite promising that user privacy is "very important" to Facebook and that it will "make important disclosures" about how it collects and can use user content

and information, Facebook fails to disclose that it tracks, collects, and intercepts sensitive communications in violation of explicit promises that health care entities, including providers, make to maintain confidentiality and prevent the disclosure of communications to third parties like Facebook. ER225-26, ¶¶ 65-69. Facebook further fails to disclose that it uses these intercepted communications "for direct marketing purposes, placing users into tranches of medically sensitive categories for sale to advertisers." ER226, ¶ 70. Plaintiffs specifically alleged that Facebook's failure to make these important disclosures and its suppression of key facts were done "with the intent to deceive its users." ER291-92, ¶ 366.

The District Court's Order relied on a statement contained within Facebook's "Data Policy" about general activity and information Facebook collects on third-party websites:

> 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).[1] 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.

ER225, ¶ 62. The District Court further referenced general disclosures that Facebook makes about its use of Internet cookies that were included in its "Cookie

[1] To the extent this provision is even relevant, Plaintiffs did not allege that Facebook's conduct occurred through Plaintiffs' use of the Facebook "Like" button, Log In, or its "measurement and advertising services[.]"

Policy." ER315-16. Neither the "Data Policy" nor the "Cookie Policy" are contained directly within Facebook's SRR. Instead, they may only be viewed by users after clicking a series of links.

Plaintiffs pled the existence of a contract generally, but disputed the meaning of certain contractual provisions and expressly and repeatedly denied consent to Facebook's acquisition of their communications with their own health care providers that themselves had explicitly promised not to disclose such information (and which Facebook knew made such promises). ER209, ¶ 3; ER220-21, ¶ 50(e)-(f); ER224, ¶ 59; ER237-54, ¶¶ 110-206.

Plaintiffs expressly pled that Facebook purposefully deceived users and that Facebook's conduct is "objectively unreasonable," "evades the spirit of the bargain made between Facebook and the plaintiffs," and "abuses its power to specify terms in the contracts it has with its users." ER290-91, ¶¶ 357-62.

Plaintiffs also pled fraud with particularity – alleging "actual fraud [by Facebook], through its suppression, with the intent to deceive its users, of the facts that it (a) tracks and intercepts user communications in violation of other websites' privacy policies, (b) tracks and intercepts user communications with health-care related websites, including the websites of medical providers subject to HIPAA, and (c) tracks, takes, and records users' medical communications and information

for purposes of placing users into medical categories for direct marketing purposes." ER291-92, ¶ 366.

After compiling data from HIPAA-covered entities and other health care organizations in violation of explicit privacy promises made to users and those users' reasonable expectations of privacy, Facebook uses the data to sell targeted advertising based on sensitive medical topics and interests that include, but are not limited to: substance abuse, HIV/AIDS, bipolar disorder, ovarian cancer, colorectal cancer, Hepatitis C, binge eating disorder, bladder cancer, cervical cancer, melanoma, rectal prolapse, incontinence, erectile dysfunction, eclampsia, chlamydia, and ectopic pregnancy. *See* ER333-346.

III. PLAINTIFFS' CLAIMS AGAINST FACEBOOK

Plaintiffs alleged eight claims against Facebook: (1) violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; (2) violation of the California Invasion of Privacy Act, Cal. Civ. Code §§ 630, *et seq.*; (3) intrusion upon seclusion; (4) invasion of privacy under the California constitution; (5) negligence per se; (6) breach of the duty of good faith and fair dealing; (7) fraud under Cal. Civ. Code §§ 1572 and 1573; and (8) quantum meruit.

IV. THE DISTRICT COURT'S ORDER

Facebook and the health care defendants filed a consolidated motion to dismiss. On May 9, 2017, the District Court dismissed the claims against Facebook

with prejudice and on the merits, and dismissed the claims against the health care defendants based on lack of personal jurisdiction. Plaintiffs have appealed as to Facebook only.

In ruling in Facebook's favor, the District Court overlooked Plaintiffs' well-pled allegations that Facebook knowingly violated the explicit privacy promises of the health care entities that were using computer code supplied by Facebook; that Facebook's conduct occurred without Plaintiffs' knowledge or consent; that Facebook abused its power to define the terms of its agreement with Plaintiffs; and that Facebook's conduct constituted fraud. Instead, the District Court relied upon a general assertion in Facebook's Data Policy and disclosures on other parts of the Facebook website regarding cookies[2] to make an incorrect factual determination that "Facebook's Data Policy discloses the precise conduct at issue in this case: 'We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button).'" ER013, Order at 12, citing Compl. Ex. A at 2.[3]

Indeed, the very first paragraph of Facebook's SRR promises users that their privacy is "very important" and that it would make "important disclosures" about

[2] The Order's focus on cookies ignores that "Internet Tracking is Not Anonymous for Facebook Even If Cookies Were Not Present." *See* ER233-36, ¶¶ 92-103.

[3] The Order's focus on the "Like" button is error. This case is not about the Like button. *See* ER228, ¶ 78; ER239, ¶ 115; ER241, ¶ 131; ER274, ¶ 284 (alleging disclosures occur on pages not containing a "Like" or "Share" button).

how Facebook collects information so that users can make "informed decisions." However, the District Court did not take into account that Facebook fails to disclose that it tracks users on health care websites in knowing violation of the specific privacy promises made by health care entities that make use of Facebook source code. For the reasons set forth below, it is respectfully submitted that the District Court's ruling on consent misconstrued the facts of the Complaint, misstated the law, and misapplied the law to Plaintiffs' allegations.

The District Court further ruled that the heightened authorization standards of HIPAA and California Civil Code section 1798.91 did not apply by finding that "nothing about [the communications at issue] relates 'to the past, present, or future physical or mental health or condition of an individual.'" ER014-15, Order at 13-14 (citing 45 C.F.R. § 160.103). Like the Court's ruling on consent, this finding also missed the mark because it ignored well-pled facts about the Plaintiffs, misstated the law, and misapplied the law to Plaintiffs' allegations.

The District Court used its consent ruling to justify dismissal of Plaintiffs' claims for (1) violation of ECPA; (2) violation of CIPA; (3) intrusion upon seclusion; and (4) invasion of privacy under the California Constitution. ER015, Order at 14. 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.

SUMMARY OF ARGUMENT

Privacy is not dead. General privacy principles still exist and apply to Internet communications. Long-standing constitutional, statutory, regulatory, contractual, and common law rules place important limits on intrusion into private matters, particularly involving one's own health. These limits apply to social networking companies just as much as anyone else. For reasons explained below, Facebook's conduct here far exceeded these limits.

GENERAL STANDARD OF REVIEW

This court conducts de novo review of Rule 12(b)(6) dismissals. *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 989 (9th Cir. 2009). The court "accept[s] as true all material allegations in the complaint, as well as any reasonable inferences to be drawn from them." *Broam v. Bogan*, 320 F.3d 1023, 1028 (9th Cir. 2003). It also construes all allegations "in the light most favorable to plaintiffs." *Zucco*, 552 F.3d at 989. To survive a 12(b)(6) motion, a complaint need only contain sufficient factual matter to "state a claim to relief that is plausible on its face." *Id*. Further, where a district court dismisses a complaint without leave to amend, such dismissal "is improper unless it is clear that the complaint could not be saved by any amendment." *Id*.

ARGUMENT

V. PLAINTIFFS DID NOT CONSENT

The Order is based on an erroneous finding of consent to the specific conduct at issue when, in fact, no such consent was given, nor was it pled.[4] To the contrary, Plaintiffs specifically pled that they did not consent. ER219-22, ¶ 50; ER258, ¶ 221; ER261-62, ¶ 234; ER269-70, ¶ 266; ER277, ¶ 300; ER281, ¶ 316; ER285-87, ¶ 333. As explained below, the heightened consent requirements of HIPAA and California Civil Code section 1798.91 apply to this case. But even if they did not, Facebook did not show that Plaintiffs consented to the conduct complained of.

A. Consent Is a Question of Fact and it Must Be Found to Be Reasonably Given

The "validity of [a party's] consent is a question of fact, and its resolution depends upon the totality of the circumstances." *United States v. Cormier*, 220 F.3d 1103, 1112 (9th Cir. 2000); *accord In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 U.S. Dist. LEXIS 36957, at *57 (N.D. Cal. Mar. 18, 2014). For claims under the ECPA, "[c]onsent may be explicit or implied, but it must be actual consent rather than constructive consent." *In re Pharmatrak*, 329 F.3d at 19. The "precise scope" of consent is "'normally for the trier of fact to determine.'"

[4] Defendants bear the burden of proving the affirmative defense of consent. *See Blumofe v. Pharmatrak, Inc. (In re Pharmatrak, Inc. Privacy Litig.)*, 329 F.3d 9, 19 (1st Cir. 2003).

Tsao v. Desert Palace, Inc., 698 F.3d 1128, 1149 (9th Cir. 2012) (quoting *Restatement (Second) of Torts* § 892A cmt. d); *see also Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983).

For example, in *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260 (9th Cir. 1998), this court ruled that the plaintiffs' express consent to general "periodic health examinations" that included questions about venereal disease, sickle cell anemia, and menstrual problems and also involved the taking of "blood and urine samples" was not enough to find that consent to testing those same blood samples for "syphilis, sickle cell trait, and pregnancy." *Id*. at 1264-65. This court concluded the lower court erred as a matter of law in holding that the plaintiffs knew or had reason to know of the nature of the tests performed, explaining, "the question of what testing, if any, plaintiffs had reason to expect turn[ed] on material factual issues *that can only be resolved at trial*[.]" *Id*. at 1268 (emphasis added).

Further, even where the facts appear to evince express consent, this Circuit grants "no refuge" to defendants who gain consent through mistake that the defendant knew or, in the exercise of reasonable care, ought to have known about and that relate to the "essential nature" of the claim. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004). *Theofel* instructs that even "overt manifestation[s] of assent" are not effective "if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the

nature and quality of the invasion intended." *Id.*; *see also Tsao*, 698 F.3d at 1151 n.18. Accordingly, consent is invalid where there is a mistake about "the essential character of the act itself," i.e., "that which makes it harmful or offensive[.]" *Theofel*, 359 F. 3d at 1073 (quoting W. Page Keeton et al., Prosser & Keeton on the Law of Torts § 18, at 120 (5th ed. 1984)). Where "the mistake is known" to the defendant or "induced by … misrepresentation, the consent is not effective for the unexpected invasion or harm." *Restatement (Second) of Torts* § 892B(2).[5] Determining whether an "invited mistake" goes to the "essential nature of the invasion" turns "on the extent to which the intrusion" impacts the specific interests that the claim seeks to protect. *Theofel* at 1073. In *Theofel*, even clear and express consent was held invalid when the defendant "had at least constructive knowledge" of the invited mistake and the access resulting therefrom "effected an 'invasion . . . of the specific interest that the [ECPA] seeks to protect.'" *Id*. at 1074.[6]

The rule goes beyond fraud and misrepresentation. It also imposes a reasonableness requirement on alleged consent. For example, Prosser & Keeton,

---

[5] *See also* § 892B(2), cmt. h, "[t]he mistake having been produced by the misrepresentation of the actor, he will normally be aware of its existence, but his knowledge of the mistake is not necessary."

[6] *See also J.H. Desnick v. Am. Broad. Cos.*, 44 F.3d 1345, 1351 (7th Cir. 1995); *Leleux v. United States*, 178 F.3d 750, 755-56 (5th Cir. 1999) ("fraudulent procurement of consent eliminates the witting agreement."); *Food Lion, Inc. v. Capital Cities / ABC, Inc.*, 194 F.3d 505, 519 (4th Cir. 1999); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1060 (N.D. Cal. 2014).

cited extensively by *Theofel*, states that a boxer "consent[s] to the defendant's striking at him" even "if death unexpectedly results," but does not "consent to being hit with brass knuckles, which is the same invasion by an act of a different character." Keeton, *supra,* § 18, at 118. Similarly, courts have consistently held that consent to sex is vitiated where the defendant knows that he or she has an STD and fails to inform their partner. *See Johnson v. Jones*, 344 P.3d 89, 95 (Ore. Ct. App. 2015) ("Consent produced by material nondisclosure is no consent at all."). Likewise, in *Sanchez-Scott v. Alza Pharms.*, a California court held that the plaintiff stated a claim for intrusion upon seclusion even when the defendant's conduct in observing her breast exam took place in full view of the plaintiff and the plaintiff did not object. *Sanchez-Scott v. Alza Pharms.*, 86 Cal. App. 4th 365 (2001). The court explained that privacy "is not a binary, all-or-nothing characteristic." *Id*. at 370 (citing *Sanders v. Am. Broad. Cos*., 20 Cal. 4th 907 (1999)). Instead, the concepts of privacy and seclusion are "relative" and "[t]he mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone." *Id*. at 374-75.

The common theme, therefore, is that the law imposes a reasonableness requirement on the affirmative defense of express or implied consent. "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. "For example, a landowner's permission for a picnic on his land will not normally be taken to give consent to a picnic at three o'clock in the morning or to a drunken brawl." *Id*.

B. The Errors of the District Court

1. The District Court Failed to Consider the Precise Scope of the Alleged Consent, the Totality of Circumstances, and the Plaintiffs' Allegations that Facebook Abused Its Power and Deceived Its Users Through Omission

The Order read Facebook's consent provisions in isolation. But consent is multi-faceted, and its scope and validity are factual questions that depend upon a review of the totality of the circumstances. Even where no limitation is stated, the law implies and imposes a reasonableness requirement on the parties. This is particularly true where the defendant knew or ought to have known that the plaintiff was mistaken as to the quality or nature of the specific invasion at issue. In short, context and reasonable expectations matter – regardless of how express or broad a party's alleged consent appears when read in isolation.

Here, the District Court did not consider the precise scope of the alleged consent and the totality of the circumstances. Taken in full, the facts alleged establish that no reasonable person would have believed that the specific data at issue was being disclosed to, tracked, acquired and sold by Facebook. To the contrary:

- Plaintiffs specifically and repeatedly alleged that they lacked knowledge of and did not authorize Facebook's acquisition of the data at issue. ER219-22, ¶ 50; ER258, ¶ 221; ER261-62, ¶ 234; ER269-70, ¶ 266; ER277, ¶ 300; ER281, ¶ 316; ER285-87, ¶ 333.
- The communications at issue were with trusted health care entities and related to health conditions, doctors, treatment, or financing for themselves or, for Jane Doe II, her spouse. ER239, ¶ 117; ER246, ¶ 161; ER249, ¶¶ 175-77; ER251, ¶ 188; ER257, ¶ 216(b).
- Plaintiffs were specifically promised that the communications would not be disclosed to third-parties like Facebook. ER237, ¶¶ 108-12; ER240-41, ¶¶ 123-28; ER242-43, ¶¶ 138-43; ER245-46, ¶¶ 156-59; ER247-48, ¶¶ 169-71; ER249, ¶¶ 175-77; ER250-51, ¶¶ 184-86; ER252-53, ¶¶ 195-97; ER347-403.
- Facebook had actual and constructive knowledge of these promises. ER231-32, ¶¶ 86-87; ER238-39, ¶¶ 113-14; ER241, ¶¶ 129-30; ER243, ¶¶ 144-45; ER246, ¶¶ 158-59; ER249, ¶¶ 172-73; ER251, ¶¶ 185-86; ER253, ¶¶ 198-99; ER258, ¶¶ 222-24; ER274, ¶ 285.
- Facebook knowingly acquired the data at issue in violation of these promises. ER225-26, ¶¶ 65-70; ER239, ¶ 116; ER242, ¶ 134; ER243, ¶ 146; ER247, ¶ 163; ER249, ¶ 174; ER251, ¶ 187; ER253, ¶ 201.

- Facebook promised to make "important disclosures," but engaged in fraudulent "suppression, with the intent to deceive its users, of the facts that it (a) tracks and intercepts user communications in violation of other websites' privacy policies, (b) tracks and intercepts user communications with health care related websites, including the websites of medical providers subject to HIPAA, and (c) tracks, takes, and records users' medical communications and information for purposes of placing users in medical categories for direct marketing purposes." ER 224-25, ¶ 60; ER291-92, ¶ 366.
- Plaintiffs enjoyed "several specific legally protected privacy interests" in the communications at issue, including actual and reasonable expectations of privacy. ER282-84, ¶¶ 325-26; ER285-87, ¶¶ 333-35; ER290, ¶¶ 356-57.
- Facebook tracking does not occur on all medical websites and is not necessary for a website to utilize some Facebook functionality. For example, MayoClinic.org and HopkinsMedicine.org "include a small Facebook icon on nearly every page," but Facebook did not acquire PII about its users from those pages. ER228-29, ¶ 79.

Considering the totality of circumstances, the District Court should have rejected Facebook's affirmative defense of consent because its actions knowingly violated explicit privacy promises made to the Plaintiffs and their reasonable

expectations of privacy. Further, Facebook knew or should have known that Plaintiffs were unaware of the essential character of the invasions at issue here.

2. The District Court's Erroneous Test for Consent

The District Court cited three cases in support of its consent finding.[7] However, these cases illustrate the deficiencies of the alleged consent here.

First, in *Mortensen v. Bresnan Commc'n*, the court found that the plaintiffs had consented to monitoring of their Internet communications by their own Internet Service Provider and the forwarding of the same to a company called NebuAd where: (1) the ISP clearly disclosed that it would do so; (2) "gave Plaintiffs specific notice of when the NebuAd Appliance trial would commence"; and (3) "provided a link for its customers to opt out of the NebuAd Appliance if they so chose." *Mortensen v. Bresnan Commc'n*, No. CV 10-13-BLG-RFC, 2010 U.S. Dist. LEXIS 131419, at *10 (D. Mont. Dec. 13, 2010). In contrast, here: (1) Plaintiffs were explicitly promised that the communications at issue would remain

[7] It bears noting by examining Facebook's general statements about its privacy policies in isolation, the District Court's Order goes further than the Defendants' briefs on its motion, where they suggested the following test for consent: "Would a reasonable user who viewed [the defendants'] disclosures have understood that [Facebook] was collecting [the information at issue?]" ER172, Def's Mot. to Dismiss, Dkt. # 96 at 16, citing *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014). This proposed test uses the plural possessive, directing the court to examine more than any single provision in isolation. In response, Plaintiffs' argued first that the correct test for consent in this case is set forth in HIPAA and California Civil Code section 1798.91. Plaintiffs maintain the same position in this appeal.

private and Facebook knew about those promises; (2) Facebook failed to give specific notice that it would collect information from trusted health care websites in violation of explicit privacy promises; and (3) Facebook did not provide its users with the ability to opt-out of its tracking on health care websites that promised not to disclose their PII.

Next, in *Del Vecchio v. Amazon.com, Inc*., the court punted on "the issue of authorization," instead ordering further briefing. *Del Vecchio v. Amazon.com, Inc*., No. C11-366RSL, 2012 U.S. Dist. LEXIS76536, at *25 (W.D. Wash. June 1, 2012).[8] The case is also factually inapposite because it involved cookie tracking by the defendant on its own website. Here, Plaintiffs are not challenging Facebook's legal ability to track users on Facebook.com. Likewise, *Del Vecchio* did not involve any countervailing promise of secrecy. Nor did it involve communications with trusted health care entities, including the plaintiffs' own providers. Instead, it appears to have been about "pet supplies." *Del Vecchio v. Amazon.com, Inc*., No. C11-366-RSL, 2011 U.S. Dist. LEXIS 138314 (W.D. Wash. Nov. 30, 2011).

Finally, in *Perkins v. LinkedIn*, the defendant's disclosure "was not, as is often the case, … buried in a Terms of Service or Privacy Policy that may never be

[8] *Del Vecchio* did evince skepticism about plaintiff's claims, stating that the defendant's Privacy Policy "appear[ed] to notify visitors that it will take the very actions about which Plaintiffs now complain[.]" *Del Vecchio,* 2012 U.S. Dist. LEXIS 76536 at *19. Such notice is absent in this case.

viewed or if viewed at all on a wholly separate page disconnected from the processes that led to the alleged wrongful conduct." *Perkins*, 53 F. Supp. 3d at 1212. "Even more significant[]," *Perkins* explains, "is the fact that alongside the disclosure is an express opt out opportunity in the form of the 'No thanks' button." *Id*. at 1212-13. *Perkins* determined it was only "[i]n light of the clarity of the disclosure, the proximity of the disclosure to the wrongful conduct, and the ability to opt out" that the plaintiffs had authorized the conduct at issue. *Id*. at 1213. But none of the key facts from *Perkins* are present here. Instead, Facebook's alleged disclosures are general in nature and contradicted by other explicit promises about the privacy of the specific data at issue, of which Facebook is aware. Facebook's alleged disclosure is also "buried … in a Privacy Policy … on a wholly separate page disconnected from the processes that led to the alleged wrongful conduct," and there is no "express opt-out opportunity." *See id.* at 1212-13.

C. Applying the Law of Consent to the Facts of this Case

Plaintiffs here were not using the Internet to play time-wasters or look at pictures of cats. Instead, they exchanged communications about their health conditions, treatment, and financing with trusted health care entities (including providers) under explicit promises, of which Facebook was aware, to keep the information private.

In *Riley v. California*, the Supreme Court unanimously held that Americans have a reasonable expectation of privacy in the data contained within their smartphones based on the fact that such data is "qualitatively different." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). For example, "An Internet search and browsing history. . . could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Id*. Similarly, in *Norman-Bloodsaw*, this court observed:

> In all, the information obtained as the result of the testing was qualitatively different from the information that plaintiffs provided in their answers to the questions, and was highly invasive. That one has consented to a general medical examination does not abolish one's privacy right not to be tested for intimate, personal matters involving one's health – nor does consenting to giving blood or urine samples, or filling out a questionnaire.

Norman-Bloodsaw, 135 F.3d at 1270. Even though they had consented to the drawing of their blood for testing, this court found that "the question of what testing, if any, plaintiffs had reason to expect turn[ed] on material factual issues that can only be resolved at trial[.]" *Id*. at 1268.

Here, Plaintiffs do not challenge Facebook's general tracking of consumers on the Internet. Instead, they challenge Facebook's tracking of their communications about medical conditions, treatment, and financing with health care entities that Facebook knows explicitly promise not to share such "qualitatively different" information. In the phrasing of *Norman-Bloodsaw*, "That

one has consented to a general [tracking] does not abolish one's privacy right not to be [tracked] for intimate, personal matters involving one's health." *See id.* at 1270. Indeed, the facts here are more compelling for the plaintiffs than *Norman-Bloodsaw*, where the alleged consent expressly related to the plaintiff's health and the information was obtained from the party's employer. Here, the alleged general consent does not mention health at all and the data is obtained by a social networking company.

Accordingly, Plaintiffs respectfully request that the trial court be reversed on multiple grounds. Consent is an issue of fact to be determined by the trier of fact only after considering the totality of the circumstances. Here, the totality of the circumstances alleged, taken as true, show that Plaintiffs did not consent to Facebook's conduct which itself was not reasonable in time, place, or any other respect. Facebook's claim of consent further fails because it was based on a theory of constructive consent from a broad, vague term buried within a Privacy Policy that no user was likely to read or understand; did not provide users with an opportunity to opt-out; and, for the specifics in this case, conflicted with explicit promises made to the Plaintiffs regarding the data at issue and of which Facebook had actual or constructive knowledge. And, even if Facebook's claim of constructive consent was based on language that was set apart from the Privacy Policy and adequately presented to each user, no reasonable user who viewed

Facebook's and the health care entities' disclosures would have understood that Facebook was collecting the information at issue. As such, any alleged consent is invalid.

VI. HIPAA AND CALIFORNIA CIVIL CODE SECTION 1798.91 APPLY TO THIS CASE AND REQUIRE THAT FACEBOOK OBTAIN EXPRESS, KNOWING, AND WRITTEN CONSENT TO OBTAIN THE INFORMATION AT ISSUE

A. HIPAA Protects Data that Is: (1) Created by a Covered Entity; (2) Relates to the Health or Condition of an Individual; and (3) Is Tied to an Identifier of the Individual, or Their Relatives, Employers, or Household Members.

The District Court erred in determining, as a matter of law, that Plaintiffs' communications with their health care providers in this case did not relate "to the past, present, or future physical or mental health or condition of an individual." ER015, Order at 14, citing 45 C.F.R. § 160.103.[9] This, however, is a question of fact, and the Order ignores the well-pled facts of the Complaint:

- Jane Doe I exchanged communications with her health care provider about her specific doctor and treatment (pain management and spine treatment). ER246, ¶¶ 161-62.

[9] The Order further erred when it made the factual determination that "the same information is transmitted to Facebook every time a user visits any page on the internet that contains a Facebook button." However, Facebook tracking does not occur on most medical websites and it is possible for a website to "include a small Facebook icon on nearly every page" without Facebook acquiring PII about its users. ER228-29, ¶ 79.

- Jane Doe II exchanged communications with her husband's health care providers (BJC and Cleveland Clinic) about his doctors (Drs. Hunt and Jain) and his treatments (intestine transplant). ER249, ¶¶ 175-76.[10]
- Winston Smith exchanged communications with health care providers and trusted health care non-profit organizations about cancer and cancer treatment – in particular, melanoma. ER239, ¶ 117; ER241-42, ¶ 132; ER243, ¶ 147; ER253, ¶ 202.

To state what should be obvious, Jane Doe I suffered from pain that stemmed from back problems, Jane Doe II's husband underwent an intestine transplant, and Winston Smith had melanoma. Facebook acquired the content of these health-related communications attached to PII about the plaintiffs.[11] But the Order simply ignored the facts, and ruled that communications are not protected if they also "contain general health information that is accessible to the public[.]" ER014, Order at 13.

First, this conclusion overlooks that the data is attached to PII about the Plaintiffs. The URL

[10] The HIPAA "de-identification standard" prohibits disclosures of a patient's "relatives, employers, or household members." 45 C.F.R. § 164.514(b)(2)(i).

[11] The Order's holding that the identifiers disclosed to Facebook (browser, IP address, cookies) do not "relate[] specifically to Plaintiffs' health" (ER014, Order at 13) makes no sense because such identifiers connect health information to an identifiable person.

http://my.clevelandclinic.org/search/results?q=intestine%20transplant is "accessible to the public," but the fact that Jane Doe II sent it is not. Second, the Order cites no authority for this determination. To the contrary, nothing in HIPAA's statutes or regulations suggests such a limitation.

Consider the brick-and-mortar equivalent of Facebook's conduct here: imagine the providers maintain toll-free numbers through which individuals can communicate to learn more information about their treatment. A person calls the number and is given a list of options. Next, they dial a code for their doctor or condition. Would it violate HIPAA if Facebook acquired the doctor and treatment codes dialed by callers?[12] Of course it would, and there is no qualitative difference here. The only difference is technological: the Internet has made communications more efficient. Accordingly, Plaintiffs respectfully request that this Court find that the data at issue in this case was protected by HIPAA, thereby prohibiting Facebook from acquiring such data in the absence of signed, informed, written consent pursuant to HIPAA.

B. Facebook's Conduct Is Subject to California Civil Code Section 1798.91

California Civil Code section 1798.91 provides that a business "may not request in writing medical information directly from an individual regardless of

[12] HIPAA also authorizes sanctions against knowing recipients of protected information. *See* 42 U.S.C. § 1320d-6(a)(2).

whether the information pertains to the individual or not, and use, share, or otherwise disclose that information for direct marketing purposes" unless it first "disclos[es] in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual" and "obtain[s] the written consent of the individual to whom the information pertains[.]" Cal. Civ. Code § 1798.91(c). "Medical information" means "any individually identifiable information … regarding the individual's medical history, or medical treatment or diagnosis by a health care professional" and "individually identifiable" means the information contains "any element[s] of [PII] sufficient to allow identification of the individual[.]" Cal. Civ. Code § 1798.91(a)(2).

Facebook is subject to this provision of California law because: (1) it is a business engaged in direct marketing;[13] (2) the communications at issue are "medical information" because (a) they contain individually identifiable information in electronic form[14] and (b) regard Plaintiffs' medical histories and/or treatment and diagnoses by health care professionals;[15] and (3) Facebook used the information for direct marketing without obtaining sufficient consent under the statute. Accordingly, Plaintiffs respectfully request this Court find that data at issue

[13] ER232, ¶¶ 88-91; ER259, ¶¶ 227-28; ER333-46, Ex. E.

[14] ER230-31, ¶ 82; ER235-36, ¶¶ 99-103; ER253, ¶ 200.

[15] ER246, ¶ 161; ER249, ¶¶ 175-77; ER257, ¶ 216(b).

was protected by California Civil Code section 1798.91, thereby prohibiting Facebook from using the data for direct marketing purposes in the absence of a "clear and conspicuous" consent form that complies with California law.

VII. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' CLAIMS AGAINST FACEBOOK FOR BREACH OF THE DUTY OF GOOD FAITH AND FAIR DEALING

Facebook's relationship with the plaintiffs is governed by California law. *See* ER300, ¶ 15. In California, "every contract calls for the highest degree of good faith and honest dealing between the parties." *Nelson v. Abraham*, 29 Cal. 2d 745, 750 (1947). The duty of good faith and fair dealing "is implied as a supplement to the express contractual covenants, to prevent a contracting party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party's rights to the benefits of the contract." *Racine & Laramie, Ltd. v. Dept. of Parks & Recreation*, 11 Cal. App. 4th 1026, 1031-32 (1992). "A party violates the covenant if it subjectively lacks belief in the validity of its act or if its conduct is objectively unreasonable." *Carma Developers (Cal.), Inc. v. Marathon Dev. California, Inc.*, 2 Cal. 4th 342, 372 (1992).

The duty "finds particular application . . . where one party is invested with a discretionary power affecting the rights of another." *Id.* Though there is no "rule of all-encompassing generality [for such claims], a few principles have emerged." *Id.* at 373. First, "breach of a specific provision of the contract is not a necessary

prerequisite." *Id.* "Nor is it necessary that the party's conduct be dishonest . . . the covenant of good faith can be breached for objectively unreasonable conduct, regardless of the actor's motive." *Id*. "Subterfuges and evasions violate the obligation of good faith in performance even though the actor believes his conduct to be justified." *R.J. Kuhl Corp. v. Sullivan*, 13 Cal. App. 4th 1589, 1602 (1993). "[B]ad faith may be overt or may consist of inaction, and fair dealing may require more than honesty." *Id.* There is no complete catalogue of the types of bad faith, but courts have recognized "evasion of the spirit of the bargain" and "abuse of a power to specify terms," among other things. *Id*.

The District Court wholly failed to analyze Plaintiffs' claim for breach of the duty of good faith and fair dealing. Nevertheless, plaintiffs have alleged facts sufficient to proceed on such a claim. First, a contract exists. ER289, ¶ 351. Second, "Facebook is invested with discretionary power affecting the rights of its users." ER289, ¶ 353; *Carma Developers,* 2 Cal. 4th at 372. Third, Plaintiffs point to a specific provision of the contract upon which they base their good faith and fair dealing claim: the first paragraph of Facebook's SRR promises users that their privacy is "very important" and Facebook will "make important disclosures" to "help" users "make informed decisions." ER289, ¶ 354. With this promise, Facebook has retained for itself the discretionary power to determine which disclosures are "important" for users to "make informed decisions."

Fourth, Plaintiffs specifically alleged that Facebook "abuses its power to specify terms – in particular, Facebook's vague disclosures of its tracking which fail to disclose that it "tracks and intercepts communications in violation of other websites' privacy policies and tracks and intercepts communications with health-care related websites, including medical providers." ER290-91, ¶ 361. Facebook also fails to disclose that it "records users' medical communications and information for purposes of placing users into medical categories for direct marketing purposes[.]" ER290, ¶ 355.

Fifth, Facebook's conduct is "objectively unreasonable" when it engages in the medical tracking at issue in this case. ER290, ¶¶ 356-58. Sixth, Facebook's conduct "evades the spirit of the bargain made between Facebook and the plaintiffs." ER290, ¶¶ 359-60. In particular, it evades the spirit of Facebook's promise that privacy is "very important" and that it would make all "important disclosures" about how it collects and uses the content of its users' information.

Seventh, the particular provisions relied upon by the District Court do not encompass the activity at issue in this case. This case is broader than the "Like button or Facebook Log In or [Facebook's] measurement and advertising services." *Id.* Plaintiffs specifically alleged, "In fact … Facebook does track users on pages lacking a Like button." ER228, ¶ 78.

"Whether the implied covenant of good faith and fair dealing has been breached is ordinarily 'a question of fact unless only one inference can be drawn from the evidence,'" *Hicks v. E.T. Legg & Assocs.*, 89 Cal. App. 4th 496, 509 (2001). Here, it was error for the District Court to dismiss Plaintiffs' claim for breach of the duty of good faith and fair dealing.

VIII. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' CALIFORNIA COMMON LAW CLAIMS AGAINST FACEBOOK

To state an action for fraud, a plaintiff must plead with specificity an intentional misrepresentation of material fact with knowledge of its falsity and intent to induce reliance, actual reliance, and damages proximately caused by the reliance. *Gonsalves v. Hodgson*, 38 Cal. 2d 91, 100-01 (1951). Under California Civil Code section 1572, "actual fraud" may consist of "[t]he suppression of that which is true, by one having knowledge or belief of the fact" or "[a]ny other act fitted to deceive." Cal. Civ. Code § 1572. Under California Civil Code section 1573, a plaintiff can establish "constructive fraud" where there has been a breach of duty "without an actually fraudulent intent" and the breaching party "gains an advantage." Cal. Civ. Code § 1573. Here, Plaintiffs alleged the "who" (Facebook and its employees), the "what" (tracking on medical websites in violation of explicit privacy promises), the "when" (during the Class period), the "where" (in interactions with the health care websites and Plaintiffs), and the "how." *See*

ER219-22, ¶ 50 (explaining how the disclosures occur); ER298, ¶ 1 (Facebook's promise to make "important disclosures").

The District Court wholly failed to analyze these claims. Nevertheless, Plaintiffs have alleged facts sufficient to proceed on such a claim and respectfully request that the Order be reversed.

IX. THE DISTRICT COURT ERRED IN NOT PERMITTING PLAINTIFFS' CLAIMS TO PROCEED AGAINST FACEBOOK UNDER THE ECPA, CIPA, INTRUSION UPON SECLUSION, AND INVASION OF PRIVACY

The District Court declined to address the substantive merits of the Plaintiffs' claims under the ECPA and CIPA, as well as claims for Intrusion upon Seclusion and Invasion of Privacy, finding instead that due to Plaintiffs' consent, they were barred. ER015, Order at 14. However, for the reasons stated herein, Plaintiffs did not consent and have alleged facts sufficient to proceed on each cause of action.

A. The Wiretap Act

To state a claim under the Wiretap Act, a plaintiff must allege an (1) intentional, (2) interception, (3) of the contents, (4) of an electronic communication, (5) without authorization,[16] (6) through the use of a device. *In re*

[16] Even where there is authorization, the Act contains an exception for interceptions that are made "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d).

Pharmatrak, 329 F.3d at 18; *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-78 (9th Cir. 2002); 18 U.S.C. § 2511.

Here, plaintiffs have satisfied the elements.

1. Intentional – Facebook designed the computer code through which plaintiffs' browsers are commandeered for Facebook to acquire the content of their communications. ER260, ¶ 231, ER266, ¶ 253.

2. Interception – The ECPA defines "intercept" as the "acquisition of the contents of any . . . electronic . . . communication[.]" 18 U.S.C. § 2510(4). It is not necessary for the acquisition to be made via the same communication. *In re Pharmatrak*, 329 F.3d at 22. Instead, the "contents" of the protected communication need only "be acquired during transmission, not while it is in electronic storage." *Konop*, 302 F.3d at 878. In *Pharmatrak*, the First Circuit ruled that a third-party cookies company (like Facebook) had "intercepted" communications through computer code that "was effectively an automatic routing program . . . that *automatically duplicated part of the communication* between a user and a [medical website] and sent this information to a third-party (Pharmatrak)." 329 F.3d at 22 (emphasis added). "Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement[s]" under the Wiretap Act. *Id.*; *see also United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). Here, Facebook's acquisition was also contemporaneous to, and in the

middle of, the communications Plaintiffs exchanged with the health care entities. ER219-22, ¶ 50; ER222, ¶ 52; ER239, ¶ 119; ER242, ¶ 134; ER244, ¶ 149; ER247, ¶ 163; ER249, ¶ 178; ER251, ¶ 190; ER253, ¶ 204; ER266, ¶ 254; ER270-71, ¶ 267.

3. Content – "Content" is defined to "include[] any information concerning the substance, purport, or meaning of [a] communication[.]" 18 U.S.C. § 2510(8). Here, the Complaint details fifteen instances in which Facebook acquired information concerning the substance, purport, or meaning of a communication. ER239-40, ¶¶ 117-21; ER241-42, ¶¶ 132-36; ER243-44, ¶¶ 147-51; ER246-47, ¶¶ 161-65; ER249, ¶¶ 175-76; ER251-52, ¶¶ 188-92; ER253-54, ¶¶ 202-06; ER271-73, ¶¶ 268-70.

For example, Facebook acquired communications between Winston Smith and MD Anderson relating to "Metastatic Melanoma" via a GET request that included the following: cancerwise/2012/06-metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis.html. *Id*. at ER253-54, ¶¶ 202-06; ER272, ¶ 269(g). The phrase "metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis" is content because it includes information concerning the "substance, purport, and meaning" of the communication that Winston Smith sent to MD Anderson. It also is "content" of the response communication that MD Anderson sent back to Winston Smith. ER272-73, ¶ 270.

No court has ever ruled that GET requests and URLs as specific as these are not protected by the ECPA. Case law, legislative history, and plain logic on this point overwhelmingly support Plaintiffs. In *In re Zynga Privacy Litigation*, this court explained that URLs contain content where they include "search term[s] or similar communication[s] made by the user[.]" *Graf v. Zynga Game Network (In re Zynga Privacy Litig.)*, 750 F.3d 1098, 1109 (9th Cir. 2014). Similarly, in *United States v. Forrester*, this court pointed out that URLs, unlike mere IP addresses "reveal[] much more information" about a user's activity, including articles viewed. *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008). In *In re Google Inc.*, the Third Circuit explained:

> post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user . . . between the information revealed by highly detailed URLs and their functional parallels to post-cut-through digits, we are persuaded that – at a minimum – some queried URLs qualify as content.

In re Google Inc., 806 F.3d 125, 139 (3d Cir. 2015); *In re U.S. for an Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 50 (D. Mass. 2005) ("contents" include URL "subject lines, application commands, search queries, requested file names, and file paths"); H.R. Rep. No. 107-236, at 53, 294-96 (2001).

4. Electronic Communication – The ECPA defines "electronic communication" broadly to mean "any transfer of signs, signals, writing, images,

sounds, data, or intelligence of any nature[.]" 18 U.S.C. § 2510(12). The data exchanged between Plaintiffs and the health care entities are "communications." *See* ER267, ¶ 257. This includes GET requests that Plaintiffs sent to the health care entities and the responses from the health care entities back to Plaintiffs. ER273, ¶¶ 271-76.

5. Without Authorization

The ECPA creates an exception to liability for interceptions that occur either with the consent of a party to the communication or by a "party to the communication." 18 U.S.C. § 2511(2)(c). Even then, however, an exception to these exceptions exists where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d).

a. Consent

For the reasons discussed above, Plaintiffs did not consent to Facebook's acquisition of the communications at issue. Plaintiffs stated they were "without knowledge" of whether the health care entities knew of Facebook's conduct. ER236, ¶ 105.

b. Facebook Is not a Party to the Communication

The Wiretap Act does not define "party to the communication." 18 U.S.C. § 2511(c)-(d). Therefore, this Court must give the term its ordinary meaning. *Joffe*

v. Google, *Inc.*, 729 F.3d 1262, 1268 (9th Cir. 2013). Here, no ordinary person would agree that Facebook is a party to any communication exchanged between a patient and their health care provider. If the communications at issue had occurred by telephone and Facebook had placed a bug on the plaintiffs' phones without their knowledge (and then received the data directly from the phones), Facebook's claim to be a "party to the communications" between the plaintiffs and the health care providers would be easily recognized as absurd. The fact that the subterfuge in this case occurred through the use of modern technology should not change the result.

Courts have split on whether a defendant may create its own exemption under the Wiretap Act via conduct that causes the data at issue to be transferred to itself directly from the communication device utilized by the victim. In *Pharmatrak*, the First Circuit held that the Wiretap Act applied to the acquisition of data by cookie companies that track users on other websites. *In re Pharmatrak,* 329 F.3d at 22. Even though the interception involved separate transmissions of data, *Pharmatrak* explained that "separate, but simultaneous . . . communications" are actionable under the ECPA. *Id*. Likewise, in *United States v. Szymuszkiewicz*, the Seventh Circuit found that the defendant had violated the Wiretap Act after he had set up an email forwarding rule in the victim's email inbox that caused every message to be automatically forwarded from the victim's email inbox to the defendant. *Szymuszkiewicz*, 622 F.3d at 707. In *In re iPhone Application*

Litigation, the court rejected the "party to the communication" defense and held that a defendant "cannot manufacture a statutory exception through its own accused conduct[.]" *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012).

The Third Circuit has taken both sides of the issue. In *In re Google Inc.*, it ruled that a third-party cookie company defendant transformed itself into "a party to the conversation . . . by deceiving the plaintiffs' *browsers into thinking* the cookie-setting entity was a first-party website."[17] *In re Google Inc.*, 806 F.3d at 143 (emphasis added). *In re Nickelodeon Consumer Privacy Litigation* followed. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3d Cir. 2016). Then, in *United States v. Eady*, the Third Circuit adopted a contradictory rule. In *Eady*, the defendant had surreptitiously used software that caused communications that started with the victim's phone to be sent directly to the defendant's phone. *United States v. Eady*, 648 F. App'x 118, 190 (3d Cir. 2016). Per the Third Circuit, a "party" under the ECPA "is a participant whose presence is known to the other parties contemporaneously with the communication." *Id*. at 191. Further, one "does

[17] The District Court had ruled that the cookie company was not a party to the communication because "plaintiffs' browsers sent different information in response to targeted advertising than would have been sent without the setting of third-party cookies." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 988 F. Supp. 2d 434, 443 (D. Del. 2013). Here, Plaintiffs alleged the sending of different information. *Compare* ER220, ¶ 50d (communication to American Cancer Society) with ER220-21, ¶ 50f (data transmission to Facebook).

not actually participate in a conversation unless his presence is known to the other participants." *Id*. at 192.

Here, the District Court has also taken both sides. In *In re Facebook Internet Tracking Litig.*, the District Court squarely rejected Facebook's claim that it was a party, explaining that such a "characterization of the allegations is incomplete because Plaintiffs allege they were unaware that Facebook was surreptitiously tracking them." *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 936 (N.D. Cal. 2015). Thus, the court held, "while it is true that a Facebook server was involved, there are no allegations . . . which demonstrate that Plaintiffs knew that fact while their browsing activity was being tracked and collected." *Id*. at 936-37. The court ruled against the plaintiffs on other grounds with leave to amend. *Id*. at 937. In June 2017, however, the District Court reversed itself, holding that Facebook is a party to the communication when tracking users on other websites. *In re Facebook Internet Tracking Litig.*, No. 5:12-md-02314-EJD, 2017 U.S. Dist. LEXIS 102464 (N.D. Cal. June 30, 2017).

Here, there are two communications at issue with each exchange between Plaintiffs and the health care entities. The first communication begins with the user either typing the full URL into their browser or employing a technological shortcut, i.e., clicking on a hyperlink. ER219-20, ¶ 50(b). The Complaint provides the example: www.cancer.org/cancer/stomachcancer/detailedguide/stomach-

cancer-diagnosis. To send the communication, the user consciously decides to hit their "Enter" key or click their mouse. ER267-68, ¶ 259. This is a communication of a sentient human being. Immediately upon the user hitting "Enter" or clicking their mouse, the user's web browser sends a GET request to the American Cancer's Society's server requesting the particular content included in the request. ER220, ¶ 50(d). In this example, the GET request is "GET/cancer/stomachcancer/detailedguide/stomach-cancer-diagnosis." ER220, ¶ 50(d).

The second communication is the health care entity's response. For this example, the American Cancer Society sends a return communication that includes a lengthy essay on how stomach cancer is diagnosed. ER221-22, ¶ 50(g). Like the user's original communication, the response involves sentient thought by a human being because it is an explanation composed by a human being for human beings – as a response to likely inquiries from users. It is more than mere computer code directing software or hardware to take an action. ER221-22, ¶ 50(g).

Unbeknownst to the user (and in the middle of the exchange of communications), Facebook code on the American Cancer Society website commandeers the user's web browser for Facebook's own purposes – "commanding the user's *browser* to send a separate but simultaneous 'GET' request to Facebook that is attached to an exact duplicate of the user's

communication to the American Cancer Society." ER220, ¶ 50(e) (emphasis added). This transmission of data between the browser and Facebook is not a communication of a human being. Instead, it is a transmission of data that is accomplished without the user's knowledge or consent. The cookies that Facebook uses to associate user communications acquired via this process with users are commonly called "third-party cookies" for a reason – they are set by website servers other than the website or server with which the user intends to exchange communications. ER217, ¶ 42(b)(ii).

Plaintiffs respectfully submit that the Third Circuit's opinion in *In re Google Inc.* (the basis of the other cases determining that third-party cookie companies are immune from ECPA liability) is fundamentally flawed. In ruling that a third-party cookie company can become a "party to the conversation … by deceiving the plaintiffs' browsers into thinking" the user has knowledge of or has consented to the third-party's presence, the court conflated the actual parties to the communication with the instruments through which those communications are made. *See In re Google Inc.*, 806 F.3d at 143.

Browsers do not "think." Browsers are inanimate software controlled by computer code and human instructions. Accordingly, browsers did not create or make the communications at issue in this case; rather, the browsers are simply a tool through which communications flow. If a hacker's success in deceiving

software or hardware is enough to make an interceptor a "party" to a communication, then the Wiretap Act no longer applies to the Internet – and may not even apply to the traditional phone wiretap.

To understand the absurdity of a holding that one who deceives a communication device is actually a party to an intercepted communication, apply the same logic to an interception that occurs where a police officer inserts a monitoring device into the telephone line of a suspected criminal. The officer who inserted the device can then listen to the suspect's conversations. Neither the suspect nor the people with whom he is communicating are aware that a secret listener is on the line. The communication begins with the victim, and the monitoring device tricks the phone into sending the communication directly to the officer. By the logic of the *In re Google Inc.* panel, this conduct does not violate the Wiretap Act because the information is sent directly from the victim's device of choice (a phone) to the officer.

If courts continue to follow the logic of *In re Google Inc.* the Wiretap Act will be eviscerated. Plaintiffs urge this Court to remand this case to the District Court and ensure that the ECPA remains effective for Internet communications by adopting the logic of the *In re iPhone Application* case that a defendant "cannot manufacture their own exemption" and the Third Circuit's statement in *Eady* that a defendant who acquires the content of a communication is not a party unless their

"presence is known to the other parties contemporaneously with the communication[.]"

c. Regardless of Authorization, Facebook's Acquisition of the Content Had a Criminal and Tortious Purpose

In *Sussman v. ABC*, this Court explained that this exception to the affirmative defense of authorization applies where the underlying act is criminal or tortious regardless of the particular means through which the act was carried out:

> Under section 2511, "the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception – its intended use – was criminal or tortious." . . . Where the taping is legal, but is done for the purpose of facilitating some further impropriety . . . section 2511 applies.

Sussman v. ABC, 186 F.3d 1200, 1202 (9th Cir. 1999). Likewise, in *Deteresa v. American Broadcasting Companies*, this Court explained that section 2511 would apply where the plaintiff came "forward with evidence to show that [defendant] taped the conversation for the purpose of violating Cal. Penal Code § 632, for the purpose of invading her privacy, for the purpose of defrauding her, or for the purpose of committing unfair business practices." *Deteresa v. Am. Broad. Cos.*, 121 F.3d 460, 467 n.4 (9th Cir. 1997).[18]

[18] The *Deteresa* court's interpretation is consistent with the legislative history. *See* H.R. Rep. No. 99-647, at 39-40 (1986) (explaining ECPA struck the phrase "or for the purpose of committing any other injurious act" and left "for a criminal or tortious purpose" in order to "remove only the shadow of finding that section 2511 has been violated by interceptions made in the course of otherwise responsible news gathering.").

Plaintiffs' allegations satisfy section 2511. Applying *Deteresa*, Plaintiffs allege Facebook engaged in fraud and unfair business practices. ER291-92, ¶¶ 364-68. Further, Plaintiffs alleged purposeful violations of HIPAA, a crime punishable by a fine up to $250,000 and a ten-year prison term if done "for commercial advantage." 42 U.S.C. § 1320d-6(b)(3); ER254-62, ¶¶ 207-34.[19] Finally, Plaintiffs also alleged violation of the Computer Fraud and Abuse Act, intrusion upon seclusion, CIPA, and negligence per se. ER275-76, ¶ 293.

Plaintiffs also satisfy *Sussman*. Here, the precise method by which Facebook acquired the sensitive data is not the entire harm or tort. Suppose instead that Facebook had obtained hard-copy summaries of the Plaintiffs' telephone communications with the health care entities and used them for advertising based on medical conditions and interests.[20] Such conduct would not violate the ECPA,

---

[19] *See United States v. Lam*, 271 F. Supp. 2d 1182, 1184 (N.D. Cal. 2003) (ruling that recordings of phone calls by a party to a communication for the unlawful purpose of "keeping business records for his unlawful gambling activities" were unlawful under § 2511 and inadmissible as evidence); *Haw. Reg'l Council of Carpenters v. Yoshimura*, No. 16-00198 ACK-KSC, 2016 U.S. Dist. LEXIS 123458 (D. Haw. Sept. 12, 2016) (holding criminal or tortious purpose exception applied where plaintiff alleged breach of fiduciary duty and extortion that were unlawful under federal law).

[20] This "hypothetical" is not at all far-fetched. *See* Kate Kaye, *Marketers Get On Board the Offline-to-Online Data Train*, Advertising Age (May 20, 2014), http://adage.com/article/datadriven-marketing/marketers-board-offline-online-data-train/293220/ (describing how Facebook and other companies are working to "turn[] offline consumer data into a tool for digital marketing").

but would still have a criminal or tortious purpose. Accordingly, Plaintiffs have satisfied section 2511.

6. Device – The ECPA defines an "electronic … or other device" as "any device . . . which can be used to intercept a[n] . . . electronic communication[.]" 18 U.S.C. § 2510(5). "Other" and "any" focus the ECPA's definition on function, i.e., whether something can be used to intercept (acquire) an electronic communication. Congress chose broad definitions in the ECPA to further the central purpose of the Wiretap Act – "to protect effectively the privacy of . . . communications." *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001). In addition to the broad statutory definition of "device," the dictionary definition includes, among other things, (1) "a thing made for a particular purpose; an invention or contrivance . . .," (2) "a plan or scheme for effecting a purpose," and (3) "a crafty scheme; trick."[21]

Here, Plaintiffs allege seven different devices: (1) cookies and other tools used by Facebook to track Plaintiffs' communications; (2) Plaintiffs' web browsers; (3) Plaintiffs' computing devices; (4) Facebook's web servers; (5) the health care entities' web servers; (6) the source code deployed by Facebook to effectuate its acquisition of users' communications; and (7) the plan Facebook

---

[21] *Device Definition*, Dictionary.com, http://www.dictionary.com/browse/device (last visited Aug. 16, 2017).

carried out to effectuate the acquisition of information in this case. ER268, ¶ 261; *see also* ER219-22, ¶ 50 (describing how these devices work together to accomplish Facebook's scheme).

Web servers and computers are devices under the ECPA. *Szymuszkiewicz*, 622 F.3d at 707. Software and computer source code are devices too. *In re Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015). Facebook's cookies are ECPA devices because they are an invention "designed to track and record an individual Internet user's communications … across the Internet." ER216, ¶ 41. Finally, Facebook's plan is a device because it is a "plan or scheme for effecting a purpose."

B. The California Invasion of Privacy Act

1. CIPA § 631

A claim under California Penal Code section 631 mirrors the ECPA with two significant differences.[22] First, CIPA is an all-party consent statute. Cal. Penal Code § 631(a) (establishing liability for conduct "without the consent of all parties to the communication."). Even if the Court determines that the health care entities consented to Facebook's acquisition, Plaintiffs themselves have not consented for the reasons set forth above. Second, CIPA does not require the use of a "device." Instead, it prohibits interceptions that occur "by means of any machine, instrument,

[22] Thus, Plaintiffs do not restate their arguments for the ECPA elements of intent, interception, content, and consent that are made above.

or contrivance, *or in any other manner*." *Id.* (emphasis added). Therefore, while Plaintiffs adequately alleged seven instruments or contrivances, even if those technically would not qualify as a "machine, instrument, or contrivance," the California statute does not require it.

2. CIPA § 632

Under California Penal Code section 632, even a party to the communication is forbidden from recording it where another party has "an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002). In some cases, California courts have held that Internet communications are not confidential for purposes of section 632 in certain circumstances. *See People v. Nakai*, 183 Cal. App. 4th 499, 514, 518 (2010) (finding 632 did not apply to communications between defendant who solicited a minor where defendant was communicating with someone he did not know, expressed concern about the privacy of the communications, and there was specific notice that "chat dialogues may be shared for the purpose of investigating illegal activities."). However, those circumstances are not present in this case. Here, one party to each of the communications at issue explicitly promised not to disclose it – and that party was a trusted health care entity which, in three instances, was a plaintiff's actual health care provider.

In *Nickelodeon*, the Third Circuit ruled that a website's privacy promises may "create[] an expectation of privacy" on those websites. *In re Nickelodeon*, 827 F.3d at 292. Here, the health care entities "created an expectation of privacy" of which Facebook had actual or constructive knowledge. This expectation was made all the more reasonable by the health care entities' status as HIPAA-covered entities or otherwise trusted health care organizations, and this court's reminder that "[o]ne can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]" *Norman-Bloodsaw*, 135 F.3d at 1269. Accordingly, to the extent this Court finds that Facebook (a third-party cookie company in this circumstance) was an actual "party to the communications" between Plaintiffs and the health care entities, Plaintiffs have nevertheless stated a claim under California Penal Code section 632.

C. California Constitutional Invasion of Privacy and Intrusion Upon Seclusion

The California Constitution provides, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art I, § 1. The phrase "and privacy" was not added until 1972. According to the California Supreme Court, the "primary purpose" of adding these two words was "to afford individuals some measure of protection against" the "most modern threat to personal privacy" –

"unnecessary information gathering . . . by public and private entities – [such as] . . . computer stored and generated 'dossiers' and 'cradle-to-grave profiles on every American.'" *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 21 (1994). "The evil addressed is … business conduct in 'collecting and stockpiling information. . .'" *Id*. Without knowing it, the California Supreme Court was essentially describing Facebook.

California courts have explained that a claim under Article 1, Section 1 of the California Constitution is "not so much one of total secrecy as it is of the right to define one's circle of intimacy – to choose who shall see beneath the quotidian mask." *Id.* at 25 (emphasis removed). Invasion of privacy has three elements "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Id*. at 66. Here, Plaintiffs have adequately alleged all three elements.

The elements of a claim for intrusion upon seclusion are similar. Under California law, a plaintiff must first allege an intrusion into a private matter, which may include "some zone of … privacy surrounding, or obtain[ing] unwanted access to data about, the plaintiff[]" and "an objectively reasonable expectation" of privacy in "the place, conversation or data source." *Shulman v. Grp. W Prods., Inc*., 18 Cal. 4th 200, 232 (1998). Second, the plaintiff must allege an intrusion that is "highly offensive" to a reasonable person. *Id.* at 231.

1. Legally Protected Privacy Interests – Plaintiffs alleged the existence of the following legally protected property interests: (a) the ECPA's Wiretap and Pen Register provisions; (b) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C) and its state corollaries; (c) CIPA; (d) HIPAA; (e) Cal. Civ. Code § 1798.91; and (f) the health care entities' privacy promises. ER282-84, ¶ 325.

2. Objectively Reasonable Expectations of Privacy – Plaintiffs alleged reasonable expectations of privacy through their legally protected privacy interests and the health care entities' explicit promises. ER284, ¶ 326. In 2014, the Supreme Court unanimously held that Americans have a reasonable expectation of privacy in the type of data at issue in this case. *See Riley*, 134 S. Ct. 2473; *see also Norman-Bloodsaw*, 135 F.3d at 1260; *In re Nickelodeon*, 827 F.3d 262; *In re Google Inc.*, 806 F.3d at 150; *Opperman*, 87 F. Supp. 3d at 1059.

3. Highly Offensive and Serious Invasion – For both intrusion and invasion of privacy, whether conduct is "highly offensive" or "serious" is ultimately a jury question, but first a court must determine "whether, as a matter of policy, such conduct should be considered, as a matter of law, not highly offensive." *Taus v. Loftus*, 40 Cal. 4th 683, 737 (2007). Here, Congress and every state has already made this policy decision through the passage of civil and criminal laws designed to protect communications and health privacy. Violation of the ECPA, CFAA, and HIPAA subjects a violator to substantial fines or prison.

Beyond criminal penalties, California explicitly declared that the activities in this case are "a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630. Even Facebook has publicly stated that less intrusive tracking of mere IP addresses (and not detailed GET requests to health care entities) raises concerns about "civil liberties and human rights" because it "could reveal details about a person's … medical conditions [or] substance abuse history[.]"[23]

Perhaps most important, the data at issue here is of a type that enjoys the highest protection under the law of this Circuit – and has been recognized as such in a unanimous opinion by the Supreme Court. *See Norman-Bloodsaw*, 135 F.3d at 1260; *Riley*, 134 S. Ct. 2473. Courts have permitted cases involving less sensitive data to move forward. *See In re Nickelodeon*, 827 F.3d 262 (children's use of the Nick.com website); *Opperman*, 87 F. Supp. 3d 1018 (phone contact lists). In *In re Google*, the Third Circuit permitted a case to move forward with an equally serious claim of intrusion. *See In re Google Inc.*, 806 F.3d 125 (broad tracking of Internet browsing history after explicit promises not to track at all on the plaintiff's chosen web-browsers). Thus, Plaintiffs' claims should not have been dismissed.

[23] *See* Letter from ECTR Coalition to Senators (June 6, 2016), *available at* https://www.ccianet.org/wp-content/uploads/2016/06/ECTR-Coalition-Letter-6-6-1.pdf. (last visited Sept. 10, 2017).

CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request this Court to remand the case back to the District Court for further proceedings with an order reinstating Plaintiffs' claims against Facebook for violation of the ECPA, violation of the CIPA, invasion of privacy, intrusion upon seclusion, breach of the duty of good faith and fair dealing, and fraud.

DATED: September 18, 2017 **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

STATEMENT OF RELATED CASES

Appellants are unaware of any related cases pending before this Court.

DATED: September 18, 2017 **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 September 18, 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 appellate CM/ECF system.

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

DATED: September 18, 2017 **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 [12,508] 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: Sep 18, 2017

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