KRONENBERGER ROSENFELD, LLP
Karl S. Kronenberger (CA Bar No. 226112)
Jeffrey M. Rosenfeld (CA Bar No. 222187)
Conor H. Kennedy (CA Bar No. 281793)
150 Post Street, Suite 520
San Francisco, CA 94108
Telephone: (415) 955-1155
Facsimile: (415) 955-1158
karl@KRInternetLaw.com
jeff@KRInternetLaw.com
conor@KRInternetLaw.com

Attorneys for Plaintiff
Charles Brautigam

SUPERIOR COURT OF CALIFORNIA
FOR LOS ANGELES COUNTY

CHARLES BRAUTIGAM, an individual,

Plaintiff,

v.

EAST WHITTIER CITY SCHOOL DISTRICT, a governmental entity created and existing under the laws of the State of California;
DAVID FELICIANO, an individual; and
MARY BRANCA, an individual,

Defendants.

Case No. BC541803

PLAINTIFF'S OPPOSITION TO DEFENDANTS' DEMURRER TO PLAINTIFF'S FIRST AMENDED COMPLAINT

Date: December 9, 2014
Time: 8:30 a.m.
Dept: 52
Before: The Hon. Susan Bryant-Deason

BY FAX

TABLE OF CONTENTS

KRONENBERGER | ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

TABLE OF AUTHORITIES

Cases

KRONENBERGER ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

Statutes

KRONENBERGER ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

INTRODUCTION

Defendants ask this Court to validate a destructive, invasive, and harmful online surveillance campaign against Plaintiff. Plaintiff is a school teacher who was placed on administrative leave on February 5, 2013. Plaintiff was instructed to return his work computers. His employer and his employer's chief business officer and co-superintendent, the Defendants here, discovered that one of the work computers had saved passwords to Plaintiff's personal Gmail and Facebook accounts. Instead of notifying Plaintiff about this security vulnerability, Defendants used Plaintiff's passwords to gain access to Plaintiff's private emails, in secret and without his consent. Over the span of six months, Defendants specifically targeted emails exchanged between Plaintiff and his friends and family, Plaintiff and his attorneys, and Plaintiff and his union representative. Defendants printed these emails and even relayed copies to third parties, including Defendants' attorneys. These communications included emails that Plaintiff had sent from his home using his own personal computing devices.

With this demurrer, Defendants attack most of Plaintiff's claims, disregarding the straightforward language of various statutes and the principle that Plaintiff's alleged facts must be taken as true. First, Defendants challenge the relevant standard under the Wiretap Act, imposing an unfounded "in transit" requirement. As courts across the country have held, no such requirement exists. Second, Defendants argue that a heightened pleading standard applies to any invasion of privacy claim based on access to a workplace computer. The Supreme Court of the United States recently adopted a contrary understanding of privacy, which accords with the realities of online communication and with common sense. Third, Defendants argue that Plaintiff's claims under section 502(c) of the California Penal Code do not allege that Defendants circumvented a "technical barrier." However, that is precisely what passwords do—they allow individualized access to accounts that are otherwise protected by technical, code-based barriers. If Plaintiff had left his house keys in his classroom, one wonders whether Defendants would have donned ski-masks and pried into his home. Finally, Defendants

KRONENBERGER | ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

argue that section 631 of the California Penal Code does not apply to email, cherry-picking isolated snippets of the law that refer to telegraphs and telephones. However, the Supreme Court of California first rejected Defendant's argument back in 1946, and almost seventy years later, courts continue to extend section 631's prohibitions to new technology.

A work computer should be a tool to assist employees with their workday responsibilities, not a trap to expose their personal lives to employers. This Court should overrule Defendants' demurrer.

BACKGROUND

Plaintiff has been a teacher with East Whittier City School District ("EWCSD") since 1999. (FAC ¶20.) At the beginning of the 2012-2013 academic year, EWCSD provided Plaintiff with a laptop, the second of two computers provided to Plaintiff by Defendants (the "Laptop"). (FAC ¶¶22-23.) Defendants allowed Plaintiff to use the Laptop for personal activities that did not interfere with Plaintiff's workday responsibilities, so long as he did not access inappropriate content. (FAC ¶24.) As a result, Plaintiff occasionally used the Laptop for personal reasons, namely to send and receive electronic messages through his personal Gmail and Facebook accounts. (FAC ¶27.) Plaintiff used his Gmail and Facebook accounts only for personal communications and not for work-related activities. (FAC ¶30.) Plaintiff never authorized Defendants to access his Gmail or Facebook accounts. (FAC ¶34.) Likewise, Plaintiff never actively saved his Gmail or Facebook passwords on the Laptop. (FAC ¶29.) Despite the foregoing, the Laptop's web browser automatically recorded Plaintiff's passwords for these accounts. (FAC ¶29.)

On February 5, 2013, Defendant EWCSD placed Plaintiff on administrative leave and demanded that Plaintiff return the Laptop. (FAC ¶¶36-37.) Defendant Mary Branca, ECWSD Secretary and Co-Superintendent ("Branca"), instructed EWCSD Chief Business Officer, Defendant David Feliciano ("Feliciano"), to search the Laptop for inappropriate content. (FAC ¶39.) Thereafter, Feliciano reviewed Plaintiff's web browser history and

KRONENBERGER | ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

noticed visits to the Gmail and Facebook websites. (FAC ¶¶40-48.) While still logged into the Laptop, Feliciano visited the Gmail and Facebook websites and used Plaintiff's passwords to access these accounts. (FAC ¶¶29, 42-44.)

Once Feliciano accessed Plaintiff's Gmail and Facebook accounts, he reviewed Plaintiff's personal communications. (FAC ¶45.) Feliciano printed several of Plaintiff's personal emails and provided them to Branca. (FAC ¶46.) Branca instructed Feliciano to continue accessing Plaintiff's Gmail and Facebook accounts over the course of several months. (FAC ¶55.) As Feliciano was accessing Plaintiff's accounts, Plaintiff continued to use his personal computer at home to exchange messages via these accounts. (FAC ¶50.) Thus, as Plaintiff continued to send and receive personal emails, Feliciano continued to monitor and intercept Plaintiff's personal communications, including email exchanges between Plaintiff and his attorneys and his union representative. (FAC ¶¶50-57.) As a result of Defendants' misconduct, Plaintiff has suffered, and continues to suffer, extreme embarrassment, anxiety, distress, and mental anguish.

On September 11, 2014, Defendants filed a demurrer as to the First Amended Complaint ("FAC").

ARGUMENT

Courts rarely entertain demurrers to privacy claims. *See Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal. 4th 992, 1003 (2009). When considering a demurrer, the court must construe the plaintiff's allegations liberally, "with a view to substantial justice between the parties." Code Civ. Proc. §452; s*ee CAMSI IV v. Hunter Tech. Corp.*, 230 Cal. App. 3d 1525, 1530 (1991). Privacy claims in particular require a "fact-dependent weighing" of evidence not available to the court at the demurrer stage. *See Sheehan*, 45 Cal. 4th at 1003. To the extent there are factual issues in dispute, this court must assume the truth not only of all facts properly pled, but also of those facts that may be implied or inferred. *See Marshall v. Gibson, Dunn & Crutcher*, 37 Cal. App. 4th 1397, 1403 (1995). Thus, where the plaintiff states a claim under any possible legal theory, the court must overrule the demurrer. *See Sheehan*, 45 Cal. 4th at 998; *Aubry v. Tri–City*

Hospital Dist., 2 Cal. 4th 962, 967 (1992).

A. Plaintiff has stated a claim under the Wiretap Act, where he has alleged that Defendants intentionally acquired his electronic communications.

Defendants demur to Plaintiff's claim under 18 U.S.C. §2511 (the "Wiretap Act"). To state a claim under the Wiretap Act, a plaintiff must allege that defendants (a) intentionally (b) intercepted (c) a wire, oral, or electronic communication and thereby (d) harmed the plaintiff. *See* 18 U.S.C. §2511. The Wiretap Act defines "intercept" as: "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). The Wiretap Act also defines "electronic communication" as: "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photooptical system that affects interstate or foreign commerce." *See* 18 U.S.C. §2510(12).

The FAC satisfies the four elements of a Wiretap Act claim. First, Plaintiff has alleged that Defendants intended to access Plaintiff's communications. (FAC ¶¶43-46, 50-53, 70-72.) As part of their investigation, Branca instructed Feliciano to acquire Plaintiff's electronic communications over a six-month span. (FAC ¶¶54-56.) Second, Plaintiff has alleged that Defendants acquired the contents of his emails through an electronic device, namely the Laptop. (FAC ¶¶41-53.) Third, Plaintiff has alleged that through this interception, Defendants accessed his "electronic communications," as that term is defined in the Wiretap Act. *See* 18 U.S.C. §2510(12). Specifically, Defendants accessed Plaintiff's Gmail and Facebook accounts and the electronic messages exchanged by Plaintiff using these accounts. (FAC ¶¶43-53.) Fourth, Plaintiff has alleged that Defendants' wrongful access harmed him. (FAC ¶59.)

Defendants have created an unsupported additional requirement. Defendants argue that Plaintiff must also allege that Defendants accessed Plaintiff's emails while they were in transit to state a claim under the Wiretap Act. This argument has no basis in the text of the Wiretap Act, and cases that interpret the Wiretap Act have rejected this

argument. *See* 18 U.S.C. §2511; *U.S. v. Szymuszkiewicz*, 622 F.3d 701, 704-06 (7th Cir. 2010); *see also Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 503 at n.1, 505 (2d Cir. 2005); *U.S. v. Councilman*, 418 F.3d 67, 72-80 (1st Cir. 2005); *Zaratzian v. Abadir,* No. 10 CV 9049, 2014 WL 4467919, at *7-8 (S.D.N.Y. Sept. 2, 2014); *Pure Power Boot Camp v. Warrior Fitness Boot Camp,* 587 F. Supp. 2d 548, 557 (S.D.N.Y. 2008); *Boane v. Boane*, No. 11-2565, 2012 WL 4340838, at *1 (W.D. Tenn. Sept. 21, 2012). In *U.S. v. Szymuszkiewicz*, for example, the Seventh Circuit rejected an argument identical to Defendants' argument here—*i.e.,* that the Wiretap Act has an "in transit" requirement. *Szymuszkiewicz*, 622 F.3d at 704-06. Judge Easterbrook held that the Wiretap Act applies wherever the defendant intercepts a plaintiff's electronic communication, including after the message has arrived. *Id.* at 705-06. Specifically, Judge Easterbrook explained that when defendants accessed the email "no more than an eyeblink" later than it arrived, such an acquisition was an interception. *Id.* at 706.

Courts in other circuits have reached the same conclusion, many citing Judge Easterbrook's decision. *See Hall*, 396 F.3d at 504; *Councilman*, 418 F.3d 67, 72-80; *Zaratzian,* 2014 WL 4467919 at *7-8; *Pure Power Boot Camp*, 587 F. Supp. 2d at 557; *Boane*, 2012 WL 4340838 at *1. In *Hall,* the Second Circuit refused to impose an in-transit requirement, finding that contemporaneous access to the contents of an email not in-transit satisfies the Wiretap Act. *See Hall*, 396 F.3d at 504 n.1, 505. Later decisions reaffirm the Second Circuit's analysis in *Hall*. *See e.g., Pure Power Boot Camp*, 587 F. Supp. 2d at 557 (citing *Hall*'s rejection of in-transit requirement under the Wiretap Act). Similarly, in *U.S. v. Councilman*, the First Circuit analyzed the legislative history of the Wiretap Act and rejected the defendants' interpretation that included an in-transit requirement. *See Councilman*, 418 F.3d at 72-80. In so holding, the First Circuit ruled that the legislative purpose of the Wiretap Act "was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections." *See id.* at 74.

Defendants rely on *Konop* and its progeny to argue for an in-transit requirement.

KRONENBERGER ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148 (C.D. Cal. 2007). However, *Konop* does not set forth an in-transit requirement. *See Konop*, 302 F.3d at 876-77. In *Konop*, the Ninth Circuit defined "interception" to require contemporaneous access, not in-transit access. *See id*. As Judge Easterbrook explained, contemporaneous acquisition is different from in-transit acquisition. *See id*. This distinction is of critical importance. Between the time an email is sent and the time of receipt, the email itself only exists as bits of data, and the bits do not travel together in lock step. *See Szymuszkiewicz*, 622 F.3d at 705-06. The contents of an email navigate networks in packets, which are "small digital envelopes of data," and separate envelopes can take separate paths. *See* P.W. Singer and A. Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 17 (2014). Prior to transmission, the computer divides the email into several packets. *See id.* at 17-24. The computer then directs each packet to move across a network of pathways to the recipient. *See id*. Only at the recipient's computer, after each of the packets has navigated from one computer to the other, are the packets reassembled into a single digital file, an email. *See id.* For this reason, Judge Easterbrook explained: "for email there is no single 'thing' that flies straight from sender to recipient." *See Szymuszkiewicz*, 622 F.3d at 705; *see also Zaratzian*, 2014 WL 4467919 at *7 ("The Court agrees with the Seventh Circuit's commonsense application of the contemporaneity requirement.").

Thus, Defendants' in-transit requirement makes little sense, because there is no such thing as an email in transit. The FAC alleges that Defendants engaged in contemporaneous access to Plaintiff's email by continuously monitoring his account. (FAC ¶¶47-48.) As a result, Plaintiff has stated a claim under the Wiretap Act.

B. Plaintiff has stated a claim for intrusion upon seclusion by alleging that Defendants invaded his objectively reasonable expectation of privacy.

To state a claim for intrusion upon seclusion, a plaintiff must allege (a) the defendant intentionally intruded upon a zone subject to an objectively reasonable

expectation of privacy; and (b) the intrusion would be highly offensive to a reasonable person. *See Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998). Whether a plaintiff had a reasonable expectation of privacy under the circumstances, and whether a defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact. *See Hill v. Nat'l College Athletic Assn.,* 7 Cal. 4th 1, 29 (1994). The factfinder must evaluate the evidence about the circumstances surrounding Plaintiff's expectation of privacy and the offensiveness of the Defendants' conduct. *See Miller v. Nat'l Broad. Co*., 187 Cal. App. 3d 1463, 1483-84 (1986) (ruling based on evidence regarding context, conduct, and circumstances surrounding intrusion, the intruder's motives and objectives, and the setting of defendant's intrusion).

Claims for intrusion upon seclusion extend to the workplace, and in the particular, personal emails sent from a workplace computer. *See Mintz v. Mark Bartelstein and Associates Inc*., 906 F. Supp. 2d 1017, 1033-34 (C.D. Cal. 2012) (plaintiff had reasonable expectation of privacy in personal emails, where personal account was password protected at all times, and plaintiff never authorized access by employer or fellow employees); *Doe v. City & Cnty. of San Francisco*, No. C10–4700 TEH, 2012 WL 2132398 at *4-5 (N.D. Cal. June 12, 2012) (plaintiff's intrusion upon seclusion claim proceeded to jury trial based on evidence that employer searched her personal email address).

Plaintiff has alleged sufficient facts to state a claim for intrusion upon seclusion. First, Plaintiff has alleged that Defendants violated an objectively reasonable expectation of privacy, by acquiring Plaintiff's personal emails without Plaintiff's knowledge, authorization, or consent. (FAC ¶¶28, 30-31, 33-34, 43, 45.) Second, Plaintiff has alleged that Defendants' intrusion would be highly offensive to a reasonable person, where Defendants read and copied Plaintiff's most sensitive emails to his attorneys, friends and family, and union representative. (FAC ¶¶46, 51-53.) The offensiveness of Defendants' conduct is further evidenced by Defendants' continuous access, occurring numerous times over the span of six months. (FAC ¶¶47-48.) Finally, Defendants

disclosed copies of Plaintiff's private emails to others, including Defendant EWCSD's attorneys. (FAC ¶55.)

Defendants argue that expectations of privacy are *per se* reduced on work computers. This argument fails. *See Doe v. City & Cnty. of San Francisco*, 2012 WL 2132398, at *5. In *Doe*, the defendants accessed an employee's email, directed to a union steward regarding workplace conditions. *See id*. at *4-5. The court rejected an argument identical to Defendants' argument here, because questions of fact existed about workplace privacy norms. *See id.* Defendants rely upon *TBG Ins. Servs. Corp. v. Superior Court*, 96 Cal. App. 4th 443 (2002). However, *TBG* did not address a claim for intrusion upon seclusion. *See id.* at 449-55. Rather, in *TBG*, the plaintiff put the contents of his work computer at issue by litigating a claim for wrongful termination. *See id.* at 449-55. The court held that the defendants were entitled to compel production of a work computer as part of discovery and pursuant to an e-discovery protective order excluding non-relevant content. *See id*. at 454; Code Civ. Proc. §2031(g).

Even if Plaintiff's work computer itself were subject to a diminished expectation of privacy, Defendants did not merely acquire work emails or files stored on the Laptop. Defendants accessed substantially all of Plaintiff's personal communications over a six month span, without limit, including those sent and received from Plaintiff's home, using his own mobile devices. (FAC ¶¶56-57.) Defendants' sole point of access was the Laptop, which recorded Plaintiff's passwords by default, not because Plaintiff authorized Defendants to access his personal email accounts. (FAC ¶¶29, 30-34, 43-45.) Moreover, Defendants did not notify Plaintiff of their ongoing access to his accounts. (FAC ¶49.) Significantly, Defendants' stock Acceptable Use Policy in no way contemplated access to employees' personal accounts, let alone by secretive use of their private passwords. (FAC ¶¶24-25.) For these reasons, Defendants' monitoring of Plaintiff's personal emails was uniquely invasive, extending beyond any reasonable monitoring of workplace conduct.

In essence, Defendants ask this Court to establish a reduced expectation of

privacy where none exists. Defendants challenge the very privacy interests validated by the Supreme Court of the United States just months ago. Specifically, without Plaintiff's consent, Defendants used Plaintiff's username and password to access a personal account that "hold[s] for many Americans 'the privacies of life.'" *See Riley v. California*, 134 S. Ct. 2473, 2490-91 (2014) (validating privacy interests in internet browsing history and mobile application data that could reveal disease symptoms, political affiliations, addictions, romantic endeavors, and commercial exchanges, among other categories of sensitive information). Based on this precedent, this Court should reject Defendants' argument wholesale.

C. Plaintiff has stated a claim under Penal Code section 502, because he has alleged that Defendants' access to his data was "without permission."

Defendants demur to Plaintiff's claim under California Penal Code section 502 ("Section 502"). Section 502 codifies seven different private causes of action, at least four of which are actionable under the facts Plaintiff has alleged in the FAC. *See* Cal. Penal Code §§502(c)(1), (2), (3), (7), *et seq*. Defendants only demur to Plaintiff's claim under section 502(c)(2), leaving the remaining claims unchallenged. A plaintiff states a claim under section 502(c)(2), where the plaintiff alleges that a defendant (1) knowingly (2) accessed and used data (3) taken from a "computer" (4) without permission. *See* Cal. Penal Code §502(c)(2).

Plaintiff has alleged sufficient facts to state a claim under section 502(c)(2). First, Defendants accessed Plaintiff's personal communications, and such access was willful. Branca instructed Feliciano to acquire Plaintiff's electronic communications, and Feliciano accessed Plaintiff's accounts on multiple occasions to do so. (FAC ¶¶50-59.) Second, Defendants accessed and used Plaintiff's data. Defendants acquired the contents of Plaintiff's emails, made copies, and relayed those copies to third parties. (FAC ¶¶43-46, 50-53.) Third, Defendants obtained this data from computers. Defendants used the Laptop to access Plaintiff's Gmail and Facebook accounts, which are operated via networks and systems owned by Google and Facebook. (FAC ¶28, 41-

42.) No other device in Defendants' possession recorded Plaintiff's login credentials, and Plaintiff's personal emails were not stored on the Laptop. (FAC ¶28.) Fourth, Plaintiff did not permit Defendants to access or use his data. (FAC ¶¶30, 33-34.)

Defendants ask this Court to read-in additional requirements that do not appear in Section 502. Defendants argue that Plaintiff must allege that Defendants circumvented a "technical barrier." However, the phrase "technical barrier" does not appear in the text of Section 502 or in the relevant jurisprudence. *See* Cal. Penal Code §§502(c)(1), (2), (3), (7), *et seq*. Thus, in *Facebook, Inc. v. Power Ventures,* the court held that the presence of a technical barrier was not dispositive of a section 502(c)(2) claim. No. 08-05780 JW, 2010 WL 3291750, at *10-12 (N.D. Cal. July 20, 2010). While the *Power Ventures* court noted that the plaintiff used a sophisticated method to block the defendant, the relevance of such "technical barriers" was one of the many factors relevant to the fourth element of section 502(c)(2): whether access was "without permission." *See id*. Here, the FAC clearly alleges Defendants' access was "without permission." (FAC ¶¶31-34.) Nothing more is required. *See* Cal. Penal Code §502(c)(2).

Even if section 502(c)(2) did require a technical barrier, Defendants' argument would fail. Defendants argue that Plaintiff's password does not satisfy the "technical barrier" element, because the Laptop stored Plaintiff's password. Defendants' argument conflates the lock with the key. A "technical barrier" is defined as a "code-based barrier[] that a computer network or website administrator erects to restrict the user's privileges within the system, or to bar the user from the system altogether." *See Power Ventures.* at *11. Gmail and Facebook accounts are indeed locked with code-based barriers that require a password and otherwise restrict all access. Here, Defendants misused Plaintiff's passwords without his permission to circumvent these barriers. *See Power Ventures* at *11.

Even assuming for the purposes of this demurrer that Defendant's argument forecloses a claim under section 502(c)(2), the FAC also asserts claims under section 502(c), subsections (1), (3), and (7). These subsections prohibit:

- Cal. Penal Code §502(c)(1): (1) knowingly (2) accessing and (3) without permission (4) using (5) any computer, computer system, or computer network in order to (6) wrongfully control or obtain data.
- Cal. Penal Code §502(c)(3): (1) knowingly and (2) without permission (3) using (4) "computer services."
- Cal. Penal Code §502(c)(7): (1) knowingly and without permission (2) accessing (3) any "computer," "computer system," or "computer network."

Plaintiff has alleged facts that establish claims under each of these subsections. *See id.* Satisfying subsection (c)(1), Plaintiff has alleged that Defendants knowingly accessed and without permission used computers to wrongfully control and obtain data containing Plaintiff's personal communications. (FAC ¶¶28-59, 88, 90, 92.) Satisfying subsection (c)(3), Plaintiff has alleged that Defendants knowingly and without permission used the "computer services" of Google and Facebook to access Plaintiff's accounts on both of those services. (FAC ¶28-59, 91, 94.) Satisfying subsection (c)(7), Plaintiff has alleged that Defendants accessed computers, computer networks, computer services, and computer systems that operated Plaintiff's Gmail and Facebook accounts. (FAC ¶¶28-59, 91, 95.)

D. Plaintiff has stated a claim under the California Invasion of Privacy Act, where he has alleged an unauthorized connection via email.

To state a claim under the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §631, a plaintiff can allege that defendants (a) by means of any machine, instrument, or contrivance, or in any other manner (b) intentionally (c) tapped or made an unauthorized connection whether physically or otherwise, (d) with any telegraph or telephone wire, line, cable, or instrument. *See* Cal. Penal Code 631. Alternatively, a plaintiff can allege that a defendant either read contents of a communication sent from, or received in, California; or a plaintiff can allege that a defendant used information from communications sent from or received in California. *See id.*

Plaintiff has stated a claim under CIPA. First, Plaintiff has alleged that Defendants

used the Laptop to make an unauthorized connection, by accessing Plaintiff's Gmail and Facebook accounts. (FAC ¶¶28, 43-46, 50-53, 70-72.) Second, Plaintiff has alleged that Defendants' conduct was intentional, as evidenced by Defendants' repeated instances of the same misconduct, including multiple unauthorized connections over a six month span. (FAC ¶¶43-46, 50-53, 70-72.) Third, Plaintiff has alleged that he never authorized Defendants to access data in his Gmail and Facebook accounts. (FAC ¶¶31-34.) Finally, Plaintiff has alleged that Defendants used the Laptop and an internet connection to access Plaintiff's accounts. (FAC ¶¶43-46.) Plaintiff has also stated a claim under CIPA because Plaintiff has alleged that Defendants read the contents of Plaintiff's private communications, which were sent from and/or received in California. (FAC ¶¶50-57.)

Defendants contend that email privacy is not recognized by CIPA, claiming that no CIPA precedent applies to email. This argument is easily disproved. *See In re Yahoo Mail Litig*., 7 F.Supp.3d 1016, 1036, (N.D. Cal. 2014) (defendant's motion to dismiss denied as to CIPA claims). Moreover, Defendants misread relevant case law. The Supreme Court of California has long established that CIPA's application extends beyond telegraphs and telephone. *See People v. Trieber*, 28 Cal. 2d. 657, 663-64 (1946). The statute expressly applies to "other" technologies. *See* Cal. Penal Code §631. CIPA applies where the contents of a communication received in California are accessed, without authorization, through "any instrument of any variety." *See People v. Trieber*, 28 Cal. 2d. at 663-64. There is thus no dispute that the emails at issue were sent over telephone wires, lines, cables, or other instruments and therefore subject to CIPA.

//

//

//

//

//

//

//

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court overrule Defendants' demurrer as to the FAC.

Respectfully Submitted,

DATED: November 24, 2014

KRONENBERGER ROSENFELD, LLP

By:_____
Conor H. Kennedy

Attorneys for Plaintiff Charles Brautigam

KRONENBERGER ROSENFELD
150 Post Street, Suite 520, San Francisco, CA 94108

CERTIFICATE OF SERVICE

I am a resident of the state of California, over the age of eighteen years and not a party to this action. My business address is 150 Post Street, Suite 520, San Francisco, California, 94108.

On November 24, 2014 I served the following document(s):

1. **PLAINTIFF'S OPPOSITION TO DEFENDANTS' DEMURRER TO PLAINTIFF'S FIRST AMENDED COMPLAINT**

on the parties listed below as follows:

Counsel for Defendants East Whittier City School District, Mary Branca, and David Feliciano:

Dana John McCune
Adam J. Beshara
McCune & Harber, LLP
515 South Figueroa Street
Suite 1150
Los Angeles, CA 90071

[X] BY OVERNIGHT MAIL via Federal Express..

[X] (State) I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATED: November 24, 2014

Leah Vulić