EXHIBIT A

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE YAHOO MAIL LITIGATION	Case No.: 5:13-CV-04980 ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

This case involves putative class action claims regarding Defendant Yahoo!, Inc.'s ("Yahoo") practice of scanning and analyzing emails of non-Yahoo Mail users in purported violation of federal and California anti-wiretapping laws. Plaintiffs Cody Baker, Brian Pincus, Halima Nobles, and Rebecca Abrams, individually and on behalf of those similarly situated ("Plaintiffs"), allege that Yahoo's operation of its Yahoo Mail service violates their expectation of privacy under the Electronic Communications Privacy Act (ECPA), California's Invasion of Privacy Act (CIPA), and the California Constitution. Plaintiffs filed a Consolidated Class Action Complaint on February 12, 2014. ECF No. 35 ("Compl."). Before the Court is Yahoo's Motion to Dismiss. ECF No. 37 ("Mot."). Pursuant to Civil Local Rule 7-1(b), the Court finds this matter appropriate for resolution without a hearing and hereby VACATES the hearing set for August 29, 2014. The Case Management Conference set for August 29, 2014 at 10 a.m. remains as set. For the reasons stated below, the Court DENIES in part and GRANTS in part Yahoo's Motion to Dismiss.

I. BACKGROUND

A. Factual Allegations

Plaintiffs are four individuals representing a class of individuals who do not use Yahoo's email service ("Yahoo Mail") but have sent emails to Yahoo Mail users from non-Yahoo email addresses. Compl. ¶¶ 15-18. Plaintiffs allege Yahoo's practices while operating Yahoo Mail violate state and federal anti-wiretapping laws and invade their protected privacy interests under the California Constitution. *Id.* ¶¶ 5-7**.** Plaintiffs seek injunctive and declaratory relief and statutory damages on behalf of a class of non-Yahoo Mail users. *Id.* ¶ 7. Plaintiffs' proposed class consists of all persons in the United States who are not Yahoo Mail users and who sent emails to or received emails from a Yahoo Mail user between October 2, 2011 and the present. *Id.* ¶ 97.

1. Yahoo Mail and Yahoo's Use of Scanned Emails

Yahoo operates Yahoo Mail as a free web-based email service. *Id.* ¶¶ 20-23. More than 275 million users have registered for Yahoo Mail to create @yahoo.com, @ymail.com, or @rocketmail.com email addresses. *Id.* ¶¶ 20-21. Before signing up for a Yahoo Mail account, potential users must provide Yahoo with personal information such as their name, birthday, telephone number, and account information. *Id.* ¶ 31.

In order to provide Yahoo Mail as a free email service to users, Yahoo charges advertisers to display advertisements on Yahoo Mail webpages. *Id.* ¶ 23. Roughly 75% of Yahoo's revenue in 2013 came from advertising. *Id.* ¶ 28. Plaintiffs allege Yahoo can increase its revenues by charging advertisers higher rates to display targeted advertisements to Yahoo Mail users. *Id.* Thus, Yahoo has a financial incentive to scan and store email content to allow advertisers to target individuals based on certain personal characteristics. *Id.*

The instant dispute concerns Yahoo's interception, scanning, and storage of Yahoo Mail users' incoming and outgoing emails for content, specifically the content of emails to and from non-Yahoo Mail users with whom Yahoo Mail users communicate. Plaintiffs allege Yahoo intercepts and scans Yahoo Mail users' emails "during transit and before placing the emails into storage." *Id.* ¶ 24. Plaintiffs allege Yahoo scans, analyzes, collects, and stores user information without their consent. *Id.* ¶¶ 1, 3, 5, 26.

2. Yahoo Terms and Privacy Policy

Three relevant agreements exist between Yahoo and Yahoo Mail users: Yahoo Terms of Service (ECF No. 35-1, "TOS"), Yahoo Global Communications Additional Terms of Service for Yahoo Mail and Yahoo Messenger (ECF No. 35-4, "ATOS"), and Yahoo Privacy Policy (ECF No. 35-2). When creating a Yahoo Mail account, Yahoo directs users to view the ATOS and Privacy Policy via hyperlinks. Compl. ¶ 31. The sentence "I agree to the Yahoo Terms and Privacy" appears above the "Create Account" Button. " *Id.*; *see also* Mot. at 7. The phrase "Yahoo Terms" links to the ATOS. Compl. ¶ 31. The word "Privacy" is an individual hyperlink to Yahoo's Privacy Policy. *Id.* The Complaint does not allege whether "Yahoo Terms" links to the TOS. However, Plaintiff's Opposition concedes that the TOS, ATOS, and Privacy Policy comprise the agreements between Yahoo and its users. ECF No. 39 ("Opp'n") at 11.

Section 1(c) of the ATOS references Yahoo's practice of scanning and analyzing users' email content. Additionally, the ATOS places responsibility on Yahoo Mail users to notify about these scanning policies non-users with whom they communicate. The ATOS in relevant part provides:

> Please note that your Yahoo Messenger account is tied to your Yahoo Mail account. Therefore, your use of Yahoo Messenger and all Yahoo Messenger services will be subject to the TOS and laws applicable to the Applicable Yahoo Company in Section 10. Yahoo's automated systems scan and analyze all incoming and outgoing communications content sent and received from your account (such as Mail and Messenger content including instant messages and SMS messages) including those stored in your account to, without limitation, provide personally relevant product features and content, to match and serve targeted advertising and for spam and malware detection and abuse protection. By scanning and analyzing such communications content, Yahoo collects and stores the data. Unless expressly stated otherwise, you will not be allowed to opt out of this feature. If you consent to this ATOS and communicate with non-Yahoo users using the Services, you are responsible for notifying those users about this feature.

ATOS § 1 (c) (emphasis in original). Plaintiffs allege that Yahoo added the line "By scanning and analyzing such communications content, Yahoo collects and stores the data" "at some time during" the proposed class period. Compl. ¶ 42. The phrase "collects and stores" is a hyperlink that leads the user to a page titled "Yahoo Mail FAQ." ECF No. 35-7. The FAQ page explains that Yahoo's scanning technology "looks for patterns, keywords, and files" in users' emails. Compl. ¶ 47. Yahoo

further discloses that it "may anonymously share specific objects from a message with a 3rd party to provide a more relevant experience." ECF No. 35-7; Compl. ¶ 47.

Yahoo's TOS and Privacy Policy do not explicitly reference the content of email sent between users and non-users. Instead, the TOS provides:

> Registration Data and certain other information about you are subject to our applicable privacy policy. For more information, see the full Yahoo Privacy Policy at http://info.yahoo.com/privacy/us/yahoo/ … You understand that through your use of the Yahoo Services you consent to the collection and use (as set forth in the applicable privacy policy) of this information, including the transfer of this information to the United States and/or other countries for storage, processing and use by Yahoo and its affiliates.

TOS § 4. Yahoo's Privacy Policy also does not explicitly mention email content. The policy states: "Yahoo collects personal information when you register with Yahoo, when you use Yahoo products or services, when you visit Yahoo pages or the pages of certain Yahoo partners, and when you enter promotions or sweepstakes." ECF No. 35-2 at 1. Furthermore, the Privacy Policy suggests it covers only "how Yahoo treats personal information that Yahoo collects and receives, including information related to your past use of Yahoo products and services." *Id.* Yahoo goes on to define personal information as "personally identifiable" information such as "your name address, email address, or phone number, and that is not otherwise publicly available." *Id.* The Privacy Policy also discloses that Yahoo provides users' personal information to "trusted partners who work on behalf of or with Yahoo under confidentiality agreements." *Id.* at 2; Compl. ¶ 37.

Yahoo also has a number of other terms and privacy documents in its Terms Center and Privacy Center online. Compl. ¶¶ 43-46. Plaintiffs' Complaint references one privacy document that applies to Yahoo Mail. ECF No. 35-6. The document has a section titled "Personally Relevant Experiences" that speaks to the scanning and analysis of email content:

> Yahoo provides personally relevant product features, content, and advertising, and spam and malware detection by scanning and analyzing Mail, Messenger, and other communications content. Some of these features and advertising will be based on our understanding of the content and meaning of your communications. For instance, we scan and analyze email messages to identify key elements of meaning and then categorize this information for immediate and future use.

ECF No. 35-6.

3. Class Allegations and Relief Sought

Plaintiffs allege that Yahoo's operation of Yahoo Mail violates the Electronic Communications Privacy Act (ECPA), California's Invasion of Privacy Act (CIPA), and Article I Section I of the California Constitution. Compl. ¶¶ 5-6. Plaintiffs seek relief on behalf of a class of persons who are not Yahoo Mail users who have either sent emails to or received emails from a Yahoo Mail user. *Id.* ¶ 97. The proposed class period begins October 2, 2011 and extends to the present. *Id.* Plaintiffs seek certification of a class of non-Yahoo Mail users, injunctive relief, declaratory relief, statutory damages, and disgorgement of Yahoo's revenues from unjust enrichment related to Yahoo's interception, scanning, and storage of emails from and to non-Yahoo Mail users. *Id.* at p.18.

B. Procedural History

Beginning on October 2, 2013, Plaintiffs filed six separate class action complaints against Yahoo in the Northern District of California, alleging that Yahoo scans and analyzes emails in violation of privacy laws. On December 18, 2013, this Court related all six pending actions because they involve the same defendant, Yahoo, and "substantially the same basic allegations" that Yahoo's "interception, storage, reading and scanning of email violates Plaintiffs' and other consumers' rights of privacy." ECF No. 14 at 2. On January 8, 2014, two of the Plaintiffs filed stipulations to dismiss their actions, which the Court granted. *See Kevranian v. Yahoo!*, 13-cv-04547-LHK, ECF No. 36. On January 22, 2014, this Court consolidated the remaining four cases for pretrial purposes, ECF No. 27, and appointed interim class counsel, ECF No. 29. Plaintiffs filed a consolidated class action complaint on February 12, 2014. ECF No. 35.

On March 5, 2014, Yahoo filed a Motion to Dismiss Plaintiffs' claims. ECF No. 37. On March 26, 2014, Plaintiffs filed an Opposition to Yahoo's Motion to Dismiss. ECF No. 39. On April 7, 2014, Yahoo filed a Reply. ECF No. 41 ("Reply").

II. LEGAL STANDARDS

A. Request for Judicial Notice

The Court generally may not look beyond the four corners of a complaint in ruling on a Rule 12(b)(6) motion, with the exception of documents incorporated into the complaint by reference, and any relevant matters subject to judicial notice. *See Swartz v. KPMG LLP*, 476 F.3d

756, 763 (9th Cir. 2007); *Lee v. City of L.A.*, 250 F.3d 668, 688-89 (9th Cir. 2001). Under the doctrine of incorporation by reference, the Court may consider on a Rule 12(b)(6) motion not only documents attached to the complaint, but also documents whose contents are alleged in the complaint, provided the complaint "necessarily relies" on the documents or contents thereof, the document's authenticity is uncontested, and the document's relevance is uncontested. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010); *see Lee*, 250 F.3d at 688-89. The purpose of this rule is to "prevent plaintiffs from surviving a Rule 12(b)(6) motion by deliberately omitting documents upon which their claims are based." *Swartz*, 476 F.3d at 763.

The Court also may take judicial notice of matters that are either (1) generally known within the trial court's territorial jurisdiction or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b). Proper subjects of judicial notice when ruling on a motion to dismiss include legislative history reports, *see Anderson v. Holder*, 673 F.3d 1089, 1094, n.1 (9th Cir. 2012); court documents already in the public record and documents filed in other courts, *see Holder v. Holder*, 305 F.3d 854 866 (9th Cir. 2002); and publicly accessible websites, *see Caldwell v. Caldwell*, No. C 05-4166 PJH, 2006 WL 618511, at *4 (N.D. Cal. Mar. 13, 2006); *Wible v. Aetna Life Ins. Co.*, 375 F. Supp. 2d 956, 965 (C.D. Cal. 2005).

B. Motion to Dismiss

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss an action for failure to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the non-moving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

However, a court need not accept as true allegations contradicted by judicially noticeable facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and a "court may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). A court is also not required to "'assume the truth of legal conclusions merely because they are cast in the form of factual allegations.'" *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Min. Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004); *accord Iqbal*, 556 U.S. at 678. Furthermore, "a plaintiff may plead herself out of court" if she "plead[s] facts which establish that [s]he cannot prevail on h[er] . . . claim." *Weisbuch v. Cnty. of L.A.*, 119 F.3d 778, 783 n.1 (9th Cir. 1997) (internal quotation marks and citation omitted).

C. Leave to Amend

If the Court determines that the complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation marks and citation omitted). Nonetheless, a court "may exercise its discretion to deny leave to amend due to 'undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . ., [and] futility of amendment.'" *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892-93 (9th Cir. 2010) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)) (alterations in original).

III. REQUESTS FOR JUDICIAL NOTICE

In support of its Motion to Dismiss, Yahoo requests the Court take judicial notice of (A) a transcript of proceedings held on September 5, 2013 in *In Re: Google Inc. Gmail Litigation*, 13-md-02430 LHK (N.D. Cal); and (B) U.S. Senate Report No. 99-541 (1986) discussing Congress' intent in passing ECPA. ECF No. 38. Plaintiffs did not file any opposition to these requests, and

even cite to Exhibit B in their Opposition. Opp'n at 14. The Court takes judicial notice of both Exhibit A and Exhibit B. Yahoo's Exhibit A is a public document that is part of this Court's own records. *See Jared v. Keahey (In re Keahey)*, 414 Fed. Appx. 919, 923 (9th Cir. 2011) (unpublished) ("A trial court may take judicial notice of its own records, even in unrelated cases[.]"). Exhibit B is a legislative history report, which is also a proper subject of judicial notice. *See Anderson*, 673 F.3d at 1094 n.1.

In support of their Opposition to Yahoo's Motion to Dismiss, Plaintiffs request judicial notice of (A) an amicus brief filed by Senator Patrick J. Leahy in *United States v. Councilman*, First Circuit Case No. 03-1383; (B) Senate Report 90-1097 discussing Congress' intent in passing the Omnibus Crime Control and Safe Streets Act of 1968; and (C) a California state superior court decision addressing violations of the California constitution, *Ung v. Facebook*, 1-12-cv-217244, Dkt. No. 54 (July 2, 2012). ECF No. 40. Yahoo did not file any opposition to Plaintiffs' request for judicial notice. The Court also takes judicial notice of Plaintiffs' Exhibits A, B, and C. All three are matters of public record and thus judicially noticeable. Exhibit A is an amicus brief that discusses the legislative history of the ECPA. Courts have taken judicial notice of amicus briefs that relate to the matters at issue. *See Gustavson v. Wrigley Sales Co.*, 961 F. Supp. 2d 1100, 1113 n.1 (N.D. Cal. 2013). Exhibit B is a Senate Report discussing legislative history, which is judicial noticeable. *See Anderson*, 673 F.3d at 1094 n.1. Exhibit C is a relevant state court decision. *Bias v. Moynihan*, 508 F.3d 1212, 1225 (9th Cir. 2007) ("[W]e 'may take notice of proceedings in other courts, both within and without the federal judicial system, if those proceedings have a direct relation to the matters at issue.'" (internal citations omitted)).

While neither party requests judicial notice of the following items, the Court sua sponte takes judicial notice of Exhibits A-G attached to Plaintiffs' Complaint because they are aspects of a publicly accessible website, Plaintiffs' Complaint necessarily relies on the contents of these webpages, and Yahoo does not contest the authenticity of the documents. *See Coto Settlement*, 593 F.3d at 1038; *Caldwell*, 2006 WL 618511, at *4. These include: (1) Yahoo Terms of Service (ECF No. 35-1, "TOS"); (2) Yahoo Privacy Policy (ECF No. 35-2); (3) Yahoo Global Communications

Additional Terms of Service for Yahoo Mail and Yahoo Messenger (ECF No. 35-4, "ATOS"); and (4) Yahoo Mail FAQ (ECF No. 35-7).

IV. MOTION TO DISMISS

A. Electronic Communications Privacy Act

Plaintiffs allege that Yahoo's email scanning practices violate federal anti-wiretapping laws. Plaintiffs bring causes of action under two separate titles of ECPA: the Wiretap Act, Compl. ¶¶ 75-83, and the Stored Communications Act ("SCA"), *id.* ¶¶ 84-92. The Court provides background on both statutes before addressing Yahoo's arguments in its Motion to Dismiss.

Congress passed ECPA in 1986 to protect the privacy of electronic communications. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). Title I of the ECPA amended the federal Wiretap Act to impose liability for the interception of certain electronic communications while they are in transit. Specifically, a Wiretap Act violation exists when any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see also id.* § 2520 (creating a private right of action for violations of *id.* § 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). Prior to the ECPA, the Wiretap Act only imposed liability for the interception of wire and oral communications such as telephone calls. However, the Wiretap Act now sweeps more broadly and applies with equal force to private email communications and websites. *See Konop,* 302 F.3d at 876 ("We therefore conclude that Konop's website fits the definition of 'electronic communication.'").

The Wiretap Act includes various exemptions for such interceptions, two of which are relevant to the instant case. First, the Wiretap Act provides that "[i]t shall not be unlawful . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). Since the Wiretap Act concerns the *unauthorized* interception of electronic communication, the consent of one party is a complete defense to a Wiretap Act claim. *Murray v. Fin. Visions, Inc.*, CV-07-2578-

PHX-FJM, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008). Second, in the Wiretap Act's definition of "device," there is an explicit exclusion for "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business." 18 U.S.C. § 2510(5)(a)(ii). Without use of a "device" as defined by the Act, there is no illegal interception.

In contrast to the interception of electronic communications, the SCA prohibits certain unauthorized access to stored communications and records. Enacted as Title II of the ECPA, the SCA imposes civil and criminal liability for anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in *electronic storage* in such system." 18 U.S.C. § 2701(a) (emphasis added). 18 U.S.C. § 2510(17)(A) states that " 'electronic storage' means . . . any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." The SCA grants immunity to 18 U.S.C. § 2701(a) claims to electronic communication service providers ("ECS providers") for accessing content on their own servers. 18 U.S.C. § 2701(c)(1). "A provider of email services is an ECS [provider]." *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1022 (N.D. Cal. 2012). Because Yahoo is an ECS provider, the SCA permits Yahoo to access Yahoo Mail communications. 18 U.S.C. § 2701(c)(1). However, ECS providers still may not "knowingly divulge . . . the contents of a communication while in electronic storage by that service." *Id.* § 2702(a)(1). Similar to the Wiretap Act, the SCA also includes an exception to liability under 18 U.S.C. § 2701(a) for user consent, *id.* § 2701(c)(2), and to liability under 18 U.S.C. § 2702(a) due to user consent, *id.* § 2702(b)(3).

1. The Wiretap Act

a. Whether the Wiretap Act Applies to Yahoo's Conduct

Yahoo first argues Plaintiffs' Wiretap Act claim must be dismissed because the SCA, not the Wiretap Act, applies to Yahoo's conduct. Mot. at 1. Yahoo first notes that the Ninth Circuit has held that for a communication to be "intercepted" in violation of the Wiretap Act, it must be accessed during transmission – i.e., while it is in transit – and not while it is in "electronic storage."

Mot. at 4 (citing *Konop*, 302 F.3d at 878). Yahoo then argues that the emails Yahoo accessed and scanned in this case *had already reached Yahoo's servers*, and that because such emails "are necessarily in temporary storage en route to the recipient," they fall within the SCA's definition of "electronic storage." Mot. at 1, 4 (citing 18 U.S.C. § 2510(17)(A) which states " 'electronic storage' means . . . any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."). Accordingly, Yahoo argues that its access to these emails is governed by the SCA because Yahoo has not made any "interception" under the Wiretap Act. In support of its argument that the term "intercept" under the Wiretap Act does not apply to the "en route storage of electronic communications," Yahoo sets forth its interpretation of a footnote in *Konop*, 302 F.3d at 880 n.6. Mot. at 5. Plaintiffs respond by claiming that *Konop*'s footnote is dicta, and that out of circuit authority makes clear that an interception can occur at any point "during the transmission of an email from the sender to the recipient." Opp'n at 8.

The Court does not address Yahoo's argument by analyzing whether Ninth Circuit law holds that the term "intercept" under the Wiretap Act applies to the "en route storage of electronic communications" because Yahoo's argument is premature. On a Rule 12(b)(6) motion to dismiss, the Court must "accept factual allegations in the complaint as true." *Manzarek*, 519 F.3d at 1031. Here, Plaintiffs allege Yahoo "intercepts emails sent to and from its Yahoo Mail users while the emails are *in transit*," Compl. ¶ 1 (emphasis added); *see also id.* ¶ 24 ("Yahoo intercepts and scans its users' incoming emails for content *during transit and before placing the emails into storage*.") (emphasis added); *id.* ¶ 80 ("Yahoo knowingly and purposefully intercepts emails *in transit* to and from Yahoo Mail accounts." (emphasis added)); *id.* ¶ 87 ("Plaintiffs allege that Yahoo intercepts communications while 'in transit' and thus in violation of the Wiretap Act."). At this stage, the Court must accept as true Plaintiffs' allegations that the emails were in transit when Yahoo accessed them. Because Yahoo's argument rests on Yahoo's assumption that the emails were in electronic storage and no longer in transit when Yahoo accessed them, the Court cannot consider Yahoo's argument because that assumption contradicts Plaintiffs' allegations.

In other words, until the Court can determine when and how Yahoo intercepted users' emails, the Court must accept as true Plaintiffs' allegation that they were accessed while "in

transit." Yahoo does not provide the Court with any judicially noticeable information as supporting evidence for its claim that the emails had already reached Yahoo's servers when Yahoo accessed them. The Court will consider Yahoo's argument that the term "intercept" under the Wiretap Act does not apply to the en route storage of electronic communications if and when Yahoo shows, at the summary judgment stage after discovery, that Yahoo intercepted users' emails after those emails had already reached Yahoo's servers. Accordingly, the Court DENIES Yahoo's Motion to Dismiss Plaintiffs' Wiretap Act claim on the basis that the Wiretap Act does not apply to the emails at issue.

b. Consent

Plaintiffs allege Yahoo's operation of Yahoo Mail involves the knowing and purposeful interception of emails "in transit to and from Yahoo Mail accounts" without consent and "for [Yahoo's] own profit." Compl. ¶¶ 79-81. Yahoo moves to dismiss the Wiretap Act claim on the ground that Yahoo obtained express consent for its interception and email scanning from all Yahoo Mail users when they signed up for Yahoo Mail. Mot. at 7. Plaintiffs respond there is no consent by Yahoo Mail users because none of Yahoo's terms adequately discloses that Yahoo engages in this conduct. Opp'n at 11. The Court GRANTS Yahoo's Motion to Dismiss for the reasons stated below.

Consent to an interception under the Wiretap Act may be either explicit or implied, but it must be actual. *See United States v. Poyck*, 77 F.3d 285, 292 (9th Cir. 1996); *United States v. Amen*, 831 F.3d 373, 378 (2d Cir. 1987); *United States v. Corona-Chavez*, 328 F.3d 974, 978 (8th Cir. 2003). The Wiretap Act only requires one party to the communication to consent to an interception to relieve the provider of liability. 18 U.S.C. § 2511(2)(d). Thus, Yahoo has not violated the Wiretap Act if Yahoo's agreements with Yahoo Mail users suffice to show consent. However, consent under § 2511(2)(d) is "not an all-or-nothing proposition." *See In Re: Google Inc. Gmail Litigation*, 13-md-02430-LHK, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013) (hereinafter "*Gmail*"); *see also Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) ("[C]onsent within the meaning of section 2511(2)(d) . . . can be limited. It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception

exceeded that consent."). In other words, "[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications." *In re Pharmatrack, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003). Furthermore, as "the party seeking the benefit of the exception," the burden is on Yahoo to prove it obtained consent. *Id.* This Court applies a reasonable user standard to determine consent under the Wiretap Act. *See Perkins v. LinkedIn Corp.*, 13-CV-04303-LHK, 2014 WL 2751053, at *14 (N.D. Cal. June 12, 2014); *Gmail*, 2013 WL 5423918, at *14.

Yahoo argues that Yahoo Mail users explicitly consented[1] to Yahoo's conduct by agreeing to the ATOS. Mot. at 1, 7-8. As a preliminary matter, Yahoo is correct that Yahoo Mail users agreed to the ATOS. When registering for Yahoo Mail, users must click a "Create Account" button that appears below the sentence: "I agree to the Yahoo Terms and Privacy." Compl. ¶ 31; Mot. at 7. The "Yahoo Terms" hyperlink directs users to view the ATOS. Compl. ¶ 31. The word "Privacy" is an individual hyperlink to Yahoo's Privacy Policy. *Id.* Thus, it is clear based on the allegations in the Complaint that Yahoo Mail users agreed to at least the ATOS and Privacy Policy when they created an account. Notably, Plaintiffs do not argue that Yahoo Mail users did not read and agree to these documents when creating accounts, and do not dispute that users can view these agreements when they sign-up for Yahoo Mail and click "Create Account." Compl. ¶ 31. To the contrary, Plaintiffs concede that the ATOS, TOS, and Privacy Policy all "comprise the agreement between Yahoo and its users." Opp'n at 11.

The question thus becomes whether the ATOS sufficiently establishes user consent by putting users on notice of Yahoo's alleged conduct, and if so, to what extent. Plaintiffs allege that Yahoo scanned and analyzed emails to "provide personally relevant product features and content," "to match and serve targeted advertising," for "spam and malware detection and abuse protection," to use the information from the emails to create user profiles, to share the information from the emails with third parties, and to "collect" and "store" the information for "future use." Compl. ¶¶ 1, 3-4, 26-27, 29, 41, 46-49, 50, 70-71. The Court thus evaluates whether the ATOS adequately

[1] Yahoo does not argue there was implied consent by either party to the communication, nor does Yahoo contend that non-users consented to the alleged interceptions.

notifies the reasonable Yahoo Mail user that their emails with non-Yahoo Mail users will be intercepted for these various purposes.

The Court concludes that the ATOS establishes explicit consent by Yahoo Mail users to Yahoo's conduct. Notably, Section 1(c) of the ATOS explicitly acknowledges that Yahoo scans and analyzes users' email for various purposes: "Yahoo's automated systems *scan and analyze* all incoming and outgoing communications content sent and received from your account (such as Mail and Messenger content including instant messages and SMS messages) including those stored in your account to, without limitation, *provide personally relevant product features and content, to match and serve targeted advertising and for spam and malware detection and abuse protection. . .* . Unless expressly stated otherwise, you will not be allowed to opt out of this feature. If you consent to this ATOS and communicate with non-Yahoo users using the Services, you are responsible for notifying those users about this feature." Compl. ¶ 41; ECF No. 35-4 (ATOS) (emphases added). In light of the clarity of the language in this disclosure, to which Yahoo Mail users agreed when creating an account, the Court finds that the ATOS provides explicit and sufficient notification to Yahoo Mail users that any communication sent via Yahoo Mail will be scanned and analyzed for the stated purposes of providing personal product features, providing targeted advertising, and detecting spam and abuse. By agreeing to the ATOS, Yahoo Mail users consented to such conduct. Plaintiffs provide no convincing argument to the contrary other than to say that "the ATOS does not explicitly inform Yahoo Mail users what Yahoo does with the contents of its users' email." Opp'n at 11. This argument fails in light of the specific statements in the ATOS that Yahoo scans the emails *in order to* "provide personally relevant product features and content, to match and serve targeted advertising and for spam and malware detection and abuse protection." ECF No. 35-4 at 1. Plaintiffs' other argument that the TOS and Privacy Policy "say nothing about the scanning and analysis of email," Opp'n at 11, is unavailing in light of how the language in the ATOS itself suffices to establish explicit consent. Accordingly, the Court concludes that Yahoo obtained consent from one party to the electronic communications to scan and analyze emails for the purposes of providing personal product features, providing targeted advertising, and detecting spam and abuse. *See Mortensen v. Bresnan Commun., L.L.C.*, CV 10-13-

BLG-RFC, 2010 WL 5140454, at *5 (D. Mont. Dec. 13, 2010) (dismissing ECPA claim because "through the *OnLine Subscriber Agreement,* the *Privacy Notice* and the NebuAd link on Bresnan's website, Plaintiffs did know of the interception and through their continued use of Bresnan's Internet Service, they gave or acquiesced their consent [under § 2511(2)(d)] to such interception").

The Court further finds that the ATOS also established Yahoo Mail users' consent to Yahoo's practice of scanning and analyzing emails for the purposes of creating user profiles for both parties to the email communication and sharing content from the emails with third parties. Compl. ¶ 27. Notably, Plaintiffs allege that Yahoo's creation of user profiles serves to "enhance Yahoo's ability to target advertising" and that Yahoo's sharing of information with third parties is for "advertising purposes." *Id.*[2] Plaintiffs do not allege that creation of user profiles or sharing of information with third parties serves any other purpose other than targeted advertising. Thus, the Court concludes that the explicit notice in the ATOS that Yahoo scans and analyzes emails in order to "match and serve targeted advertising" suffices to prove that by agreeing to the ATOS, users also consented to Yahoo's conduct of scanning and analyzing emails for the purpose of creating user profiles and sharing content with third parties. In light of the ATOS, the Court concludes that additional allegations cannot save Plaintiff's claim that there was no consent to scan and analyze emails for the purposes of providing personal product features, providing targeted advertising, detecting spam and abuse, creating user profiles, and sharing information with third parties. Thus, the Court GRANTS Yahoo's Motion to Dismiss Plaintiffs' Wiretap Act claim with respect to scanning and analyzing for these purposes with prejudice.

The only remaining question is whether there was consent to Yahoo's conduct of "collecting" and "storing" the content from emails for "future use." Plaintiffs claim Yahoo provided Yahoo Mail users no notice of this conduct. Opp'n at 12. Plaintiffs note that for part of the class period, the ATOS did not inform users that Yahoo collects and stores email content on its

[2] The Complaint also alleges that "Yahoo can increase revenues by obtaining more detailed background information about users of the service," and that "Yahoo benefits from gathering as much personal information about its Yahoo Mail users, and non-users who email with its users, as it can." *Id.* ¶ 28. Plaintiffs' allegations do not explain how Yahoo increases its revenues other than to provide targeted advertisements. *Id.* ("Yahoo can charge advertisers substantially more to place ads that are 'targeted' to certain demographic groups and even to specific individuals.").

servers. *Id.*; Compl. ¶ 42. Plaintiffs concede that "at some time during the proposed class period," Yahoo revised ATOS § 1(c) by adding the line: "By scanning and analyzing such communications content, Yahoo collects and stores the data." Compl. ¶¶ 41-42; Opp'n at 12. Nonetheless, Plaintiffs argue that even after Yahoo added this statement, Yahoo did not provide sufficient notice of collection and storage because Yahoo failed to explain to users "what it does with the data" it stores or what Yahoo "plans to do with it in the future." Opp'n at 12. The Court disagrees and finds users were on notice and thus consented to how Yahoo "collects" and "stores" the content from emails for "future use," as explained below.

Plaintiffs concede that for at least the latter part of the class period, the ATOS explicitly notified users that Yahoo "collects and stores" their email communications. Compl. ¶¶ 41-42; Opp'n at 12. The Court concludes that this explicit language contained in the agreement between Yahoo and its users sufficed to put a reasonable user on notice of such collection and storage for the latter part of the class period. The Court further concludes that even for the portion of the class period during which the ATOS did not explicitly reference collection and storage, the reasonable user was nonetheless similarly on notice that Yahoo engages in collection and storage of email content. This is because the reasonable user would know that the ATOS's language that Yahoo "scan[s] and analyze[s]" email content necessarily means Yahoo simultaneously collects and stores the email content, i.e., the reasonable user would know that "scanning and analyzing" *requires* Yahoo to collect and store the email content. In other words, the Court finds it implausible that users did not – after agreeing, based on the ATOS, to Yahoo's scanning and analysis of emails – realize that in order to engage in analysis of emails, Yahoo would have to store the emails somewhere on its servers. Indeed, Plaintiffs do not provide any plausible reason why scanning and analyzing email content does not require the collection and storage of that content. If anything, Plaintiffs' allegation that Yahoo "scans [email] content, storing the data it collects" suggests that the very process of scanning simultaneously stores the content. Compl. ¶ 1. Furthermore, the ATOS stated, at *all* times during the class period, that Yahoo "store[s]" emails in users' accounts, which would have put the reasonable user on notice that Yahoo already stores at least some emails on its servers. ECF No. 35-4 (ATOS) ("Yahoo's automated systems scan and analyze all incoming

and outgoing communications content sent and received from your account . . . including those *stored* in your account[.]") (emphasis added). Thus, the Court concludes that the reasonable user was on notice and thus consented to Yahoo's collection and storage of email content when the user agreed to the ATOS.

The only remaining issue is whether Yahoo informed users that Yahoo was going to use the information it was collecting and storing in the "future." Plaintiffs claim there was no notice of such future conduct because users had no notice of what specific *use* Yahoo would make of the email content in the future. Opp'n at 12. Plaintiffs' argument is unconvincing. Given the explicit statements in the ATOS that Yahoo scans and analyzes email content to provide personal product features, provide targeted advertising, and detect spam and abuse. It is logical that Yahoo's future uses would be the same. Further, Plaintiffs do not allege what they believe Yahoo was planning to do with the email content in the future separate and apart from the various uses of which this Court has already found users were on notice: to provide personal product features, provide targeted advertising, and detect spam and abuse. Accordingly, the Court finds that Yahoo Mail users consented to Yahoo's collection and storage of their emails for future use, and GRANTS Yahoo's Motion to Dismiss the Wiretap claim with respect to this conduct. However, the Court GRANTS leave to amend in order to allow Plaintiffs to allege any other "future use" they believe Yahoo would make of their email content, separate and apart from the uses of which this Court has found users had notice.[3]

2. The Stored Communications Act

In the alternative to a Wiretap Act violation, Plaintiffs argue that Yahoo's scanning practices violate the Stored Communications Act. Compl. ¶ 6. Plaintiffs assert this claim in the alternative "in the event the Court concludes that Yahoo accesses plaintiffs' emails after they have been delivered to the recipients" and are thus in storage. Opp'n at 3; Compl. at ¶ 87 ("Plaintiffs

[3] Because the Court GRANTS Yahoo's Motion to Dismiss the Wiretap Act claim on consent grounds, the Court need not reach Yahoo's argument that the "ordinary course of business" exception to Wiretap Act liability applies. The Court also need not reach Yahoo's argument, raised for the first time in Reply, that Plaintiffs' "bare allegation" that Yahoo intercepts emails while they are "in transit" fails to state a Wiretap Act claim under *Twombly*. Reply at 2.

assert this SCA claim in the alternative, in the event the Court finds that Yahoo intercepts the emails while they are in 'storage' rather than 'in transit'[.]"). Yahoo moves to dismiss Plaintiffs' SCA claim.

Yahoo contends that if the SCA applies to Plaintiffs' claims, Yahoo has statutory immunity to any alleged 18 U.S.C. § 2701(a) violation[4] pursuant to 18 U.S.C. § 2701(c)(1) and 18 U.S.C. § 2701(c)(2). Mot. at 11-12. Plaintiffs concede that Yahoo has immunity to any alleged § 2701(a) violation pursuant to § 2701(c)(1), which grants immunity for alleged violations of § 2701(a) to ECS providers like Yahoo for accessing electronic communications stored on their own servers.[5] Opp'n at 14 (acknowledging that "the SCA immunizes electronic service providers like Yahoo from liability for accessing emails that are in its users' mailboxes or in the service providers' 'backup protection.'"); *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012).[6] Accordingly, the Court GRANTS Yahoo's Motion to Dismiss with prejudice any claim that Yahoo violated § 2701(a).[7]

However, Plaintiffs also assert Yahoo is liable under 18 U.S.C. § 2702(a)(1), which prohibits Yahoo from *disclosing* the content of users' emails to third parties. Compl. ¶ 90 (alleging Yahoo's "sharing of the content with third parties"); Opp'n at 14-15 (stating Yahoo is "prohibited from disclosing the contents of their customers' emails to any person or entity"). Plaintiffs claim Yahoo improperly disclosed to third parties the content from the scanned emails between Yahoo Mail users and non-users. *Id.* Section 2702(a)(1) holds ECS providers liable under the SCA if they "knowingly divulge to any person or entity the contents of a communication while in electronic

---

[4] An SCA violation under 18 U.S.C. § 2701(a) occurs when someone "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a).

[5] Section 2701(c)(1) provides an exception to liability for an 18 U.S.C. § 2701(a) violation when the conduct is authorized: "(1) by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1).

[6] Plaintiffs' Complaint does not explicitly state which provision of the SCA Yahoo has violated.

[7] Because the parties agree that Yahoo has immunity under 18 U.S.C. § 2701(c)(1), the Court does not reach whether Yahoo had its users' consent to access the communications under 18 U.S.C. § 2701(c)(2), as Yahoo claims, Mot. at 12 n.9.

storage by that service." 18 U.S.C. § 2702(a)(1). Yahoo argues Plaintiffs' claim for a violation of § 2702(a)(1) lacks the factual specificity required by *Twombly* because "plaintiffs have failed to allege specific information about what information they contend was shared, with whom, and for what purpose." Mot. at 13 n.10. The Court finds that the Complaint adequately alleges that Yahoo improperly disclosed portions of the "contents of a communication" to third parties in violation of § 2702(a)(1), as explained below. Accordingly, the Court DENIES Yahoo's Motion to Dismiss Plaintiffs' SCA claim for improper disclosure under § 2702(a)(1).

In order to state a claim for improper disclosure under the SCA, Plaintiffs must plausibly allege that Yahoo knowingly divulged "the contents of a communication." *See In re Zynga Privacy Litigation*, 750 F.3d 1098, 1109 (9th Cir. 2014). The Complaint makes several references to Yahoo's alleged disclosure of email content to third parties. Compl. ¶¶ 27, 37, 47, 49, 71, 90. Plaintiffs allege that after Yahoo scans and analyzes electronic communications between users and non-users of Yahoo Mail, Yahoo "provides some of the information it collects from its users' incoming and outgoing email to unidentified 'trusted partners' and other third parties for advertising purposes." Compl. ¶¶ 26-27. Plaintiffs claim their allegations lack detail in terms of alleging what content was shared because discovery is at an early stage and Yahoo has not revealed with whom it shares email content. Opp'n at 15. Plaintiffs claim, however, that their allegations are sufficient because they are "based on Yahoo's own statements about its practices" contained in two documents: the Privacy Policy, ECF No. 35-2, and the Yahoo Mail FAQ, ECF No. 35-7. Opp'n at 15.

The Court notes, as a preliminary matter, that Plaintiffs are incorrect to argue that the Privacy Policy supports Plaintiffs' argument that their allegations sufficiently plead that Yahoo divulged "the contents of a communication." The Plaintiffs cite to one part of the Privacy Policy which states that Yahoo provides "its users' personal information 'to trusted partners who work on behalf of or with Yahoo under confidentiality agreements.'" Compl. ¶ 37. The SCA distinguishes between "contents of a communication" and "record information." The SCA incorporates the definition of "contents" from the Wiretap Act. 18 U.S.C. § 2711(1). Under the Wiretap Act, "contents" includes "any information concerning the substance, purport, or meaning of that

communication." *Id.* § 2510(8). The Ninth Circuit has interpreted the language and statutory framework of ECPA to find that "contents" means "a person's intended message to another." *Zynga*, 750 F. 3d at 1106. In contrast to "contents," customer "record information" includes personally identifiable information such as the customer's name, address, and identity. *Id.* at 1104. The Ninth Circuit has clearly held that "contents" under the ECPA "does not include record information regarding the characteristics of the message that is generated in the course of the communication." *Id*. at 1106. As noted above, in order to state a claim for improper disclosure, Plaintiffs must plausibly allege that Yahoo knowingly divulged "the contents of a communication." *Id.* at 1109. Thus, Plaintiffs' allegations must show that Yahoo disclosed "contents," not "record information," to third parties. However, the Privacy Policy appears to refer only to "record information" rather than the "contents" of an electronic communication like emails, as Yahoo argues. Reply at 9. The Privacy Policy states that "[Yahoo] provide[s] the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your *personal information* to help Yahoo communicate with you about offers from Yahoo and our marketing partners." ECF No. 35-2 (emphasis added). The Privacy Policy, which states that it "covers how Yahoo treats personal information," defines "personal information" as "information about you that is personally identifiable like your name, address, email address or phone number, and that is not otherwise publicly available." *Id.* Nothing in this language suggests that "personal information" includes content from email exchanges. Plaintiffs themselves even admit that the Privacy Policy says "nothing about the scanning and analysis of email." Opp'n at 11. Accordingly, because the Privacy Policy refers to "record information" rather than the "contents" of an electronic communication, the Privacy Policy language that Yahoo shares personal information with "trusted partners" does not support Plaintiffs' allegation that Yahoo shares "contents of a communication" with third parties.

Nonetheless, the Court still finds that Plaintiffs' allegations suffice to plausibly allege a claim under *Twombly*. This is because the Complaint contains sufficient factual detail to plausibly allege that Yahoo shared with third parties "the contents of a communication." *Zynga*, 750 F. 3d at 1109. As stated above, Plaintiffs allege at various points that Yahoo shared email content with third

parties. *See* Compl. at ¶ 71 (alleging Yahoo "distributes the content of the emails to third parties"); *id.* at ¶ 90 (alleging Yahoo shares "the content [of emails] with third parties"). Plaintiffs further allege that one question in the FAQ reads: "Does Yahoo Mail automatically share my messages with anyone else?" to which Yahoo's response states, "Yahoo may anonymously share *specific objects from a message* with a 3rd party to provide a more relevant experience within your mail. For example, Yahoo may share a package tracking number with the shipping company so that you can easily see when your package will arrive, or may share your flight number with your airline to enable flight notifications within your inbox." *Id.* at ¶¶ 47, 49 (citing ECF No. 35-7 at 2 (emphasis added)). The language "specific objects from a message" falls within the SCA's definition of "contents of a communication" because the phrase "specific objects" clearly refers to the "contents" of a "message," the latter of which is an email communication. *See Konop*, 302 F.3d at 875 ("The legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards."); *see also O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1443 (2006) ("[The SCA] clearly prohibits any disclosure of stored *email* other than as authorized by enumerated exceptions." (emphasis added)). Thus, pursuant to Plaintiffs' allegations, Yahoo's own FAQ page admits that Yahoo shares email content with third parties. Under these circumstances, the Court concludes that Plaintiffs have plausibly alleged that Yahoo improperly disclosed "contents" of email communications to third parties.

While Yahoo argues Plaintiffs have failed to allege what specific information was shared and with what specific third parties, the FAQ, as alleged in the Complaint, does give at least one example of the kind of information in emails that was shared with third parties – i.e., a package tracking number. In any event, Yahoo cites no case holding that a plaintiff must allege the specific information in the content that was shared or the identity of the third party in order to state a claim for a violation of § 2702(a)(1). Ultimately, the Court finds that Plaintiffs' allegations as a whole sufficiently plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (internal citations omitted).

The Court notes that in its Reply, Yahoo argues in one sentence in a footnote that the language in the ATOS "suffices as consent for SCA purposes." Reply at 6 n.7. Because the Court has concluded, as Plaintiffs concede, that Yahoo has not violated § 2701(a), the only consent exception relevant under the SCA is the consent exception to a § 2702(a) violation, *see* § 2702(b)(3). However, Yahoo did not argue in its opening brief that there was consent for a § 2702(a) violation and only focused on how Yahoo had consent to a § 2701(a) violation pursuant to § 2701(c)(2). Mot. at 12 n.9. Thus, the Court does not consider Yahoo's consent argument in its Reply because arguments raised for the first time in Reply briefs are waived. *Sealant Sys. Intl., Inc. v. TEK Global S.R.L.*, 5:11-CV-00774-PSG, 2014 WL 1008183, at *14 (N.D. Cal. March 7, 2014). Accordingly, the Court DENIES Yahoo's Motion to Dismiss Plaintiffs' SCA claim for improper disclosure under § 2702(a)(1).

3. Good Faith Defense

Yahoo raises a good faith defense against Plaintiffs' Wiretap Act and SCA claims. Mot. at 13. The Wiretap Act provides:

> A good faith reliance on—
> (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703 (f) of this title);
> (2) a request of an investigative or law enforcement officer under section 2518 (7) of this title; or
> (3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;
> is a complete defense against any civil or criminal action brought under this chapter or any other law.

18 U.S.C. § 2520(d); *see also* 18 U.S.C. § 2707(e) (providing a nearly identical good faith defense for SCA violations). Specifically, as a defense to Plaintiffs' § 2701(a) SCA claim, Yahoo claims it relied in good faith on §§ 2701(a), (c). As a defense to Plaintiffs' Wiretap claim, Yahoo claims it relied on (1) the decisions of the Ninth Circuit in *Konop* and *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003), that hold, in Yahoo's view, that the SCA rather than the Wiretap Act applies to email scanning that occurs once emails have reached an ECS provider's servers; (2) 18 U.S.C. § 2511(c), the consent exception; and (3) 18 U.S.C. § 2511(2)(a)(i), the ordinary course of business exception. Mot. at 13.

The Court does not reach Yahoo's good faith reliance on §§ 2701(a) and (c) because the Court GRANTS, on other grounds as stated above, Yahoo's Motion to Dismiss any claim that Yahoo violated § 2701(a). *See supra*, Part IV.A.2. The Court also does not reach Yahoo's alleged good faith reliance on the Ninth Circuit decisions *Konop* and *Theofel* or on §§ 2511(c) and 2511(2)(a)(i) of the Wiretap Act because the Court GRANTS, on other grounds as set forth above, Yahoo's Motion to Dismiss the Wiretap claim, *see supra*, Part IV.A.1.b. Thus, the Court need not reach Yahoo's Motion to Dismiss either the SCA claim or Wiretap claim based on the good faith defense.

B. California's Invasion of Privacy Act ("CIPA")

Plaintiffs bring a cause of action under CIPA, Cal. Penal Code § 630, *et seq*. CIPA is California's anti-wiretapping and anti-eavesdropping statute that prohibits unauthorized interceptions of communications in order "to protect the right of privacy." Cal. Penal Code § 630. The California Legislature enacted CIPA in 1967 in response to "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications[.]" *Id.* Yahoo moves to dismiss the CIPA claim. The Court DENIES Yahoo's motion.

Section 631 of CIPA makes it unlawful to use "any machine, instrument or contrivance" to intentionally intercept the content of a communication over any "telegraph or telephone wire, line, cable or instrument," or to read, attempt to read, or learn the "contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable" without the consent of all parties to the communication. *See* Cal. Penal Code § 631(a). The California Supreme Court has held that § 631 protects against three distinct types of harms: "intentional wiretapping, willfully attempting to learn the contents or meaning of a communication in transit over a wire, and attempting to use or communicate information obtained as a result of engaging in either of the two previous activities." *Tavernetti v. Superior Court*, 22 Cal. 3d 187, 192 (1978).

Plaintiffs allege Yahoo has violated § 631 of CIPA. Compl. ¶¶ 53-65. Yahoo moves to dismiss first on the grounds that § 631 only applies to communications intercepted "in transit," and

that here the communications at issue were not "in transit" but in "electronic storage" because the emails were already on Yahoo's servers when Yahoo accessed the emails. Mot. at 14-15. Second, Yahoo similarly argues that the all-party consent provision in § 631 should not apply to "recorded communications" already in the hands of and received by a provider because that would lead to illogical results, *id.* at 16, and thus that this Court must interpret CIPA to find that "when an email reaches the recipient's provider," the email "is no longer in transit" and CIPA does not apply. Reply at 13. Finally, Yahoo argues that the SCA and Wiretap Act would preempt § 631 *if* CIPA applied to emails "on an ECS providers' servers" – like the emails Yahoo contends are at issue here. *Id*. at 18-19.

Yahoo relies on *Konop* to support its contention that emails an ECS provider has received en route to a recipient are in electronic storage rather than "in transit," and thus that CIPA does not apply. Mot. at 14. Yet as discussed above, *see supra* Part IV.A.1.a, the Court must accept as true Plaintiffs' allegation that "Yahoo intercepts and scans its users' incoming emails for content during transit and before placing the emails into storage." Compl. ¶ 24. The Court must defer resolution of whether Yahoo accessed the emails only after the emails were on Yahoo's servers until after discovery makes clear where and how Yahoo's scanning technology intercepted the emails. Thus, the Court rejects Yahoo's first argument that CIPA does not apply.

Yahoo's second argument that CIPA should not apply when an email has reached Yahoo's servers – based on allegedly illogical implications that would result from applying CIPA's all-party consent provision to such emails – similarly assumes the emails were on Yahoo's server when intercepted, which this Court cannot assume at this stage. Even if the Court could make such an assumption, the Court would still have to reject Yahoo's argument that the Court should find the emails at issue were not "in transit" when intercepted because that would contradict the allegations in the Complaint, which the Court must accept as true. Thus, the Court rejects Yahoo's second argument why CIPA does not apply.

Finally, the Court rejects Yahoo's preemption argument for similar reasons. Yahoo contends that the SCA and Wiretap Act preempt Plaintiffs' CIPA claims, relying on all three theories of federal preemption. Mot. at 18; *Chae v. SLM Corp.*, 593 F.3d 936, 941 (9th Cir. 2010)

(internal quotation marks and citations omitted) ("Federal preemption occurs when: (1) Congress enacts a statute that explicitly pre-empts state law; (2) state law actually conflicts with federal law; or (3) federal law occupies a legislative field to such an extent that it is reasonable to conclude that Congress left no room for state regulation in that field."). Specifically, Yahoo does not contend that ECPA wholly preempts CIPA, but argues that CIPA would conflict with ECPA *only if* CIPA applied to emails that have already reached a provider's servers, as Yahoo argues the emails in the instant case had. Mot. at 18; Reply at 13; Mot. at 19 (arguing that the ECPA "preempts parallel state legislation regulating the conduct of email providers when accessing emails on their servers."). However, again here, Yahoo's argument assumes the emails were on Yahoo's server when intercepted, which this Court cannot simply assume at this stage when allegations in the Complaint are to the contrary.

Accordingly, the Court DENIES Yahoo's Motion to Dismiss Plaintiffs' CIPA claim.

C. California Constitution

Plaintiffs allege that Yahoo's scanning, storage, and disclosure of Plaintiffs' email content violates their right to privacy under Article I, Section 1 of the California Constitution. Compl. ¶¶ 66-74. Yahoo contends Plaintiffs fail to allege sufficient facts to state a claim. Mot. at 21. The Court GRANTS Yahoo's motion with leave to amend.

The California Constitution creates a privacy right that protects individuals from the invasion of their privacy by private parties. *Am. Acad. of Pediatrics*, 16 Cal. 4th 307, 326 (1997); *Leonel v. Am. Airlines, Inc.*, 400 F.3d 702, 711-12 (9th Cir. 2005), *opinion amended on denial of reh'g*, 03–15890, 2005 WL 976985 (9th Cir. 2005). To establish an invasion of privacy claim, a plaintiff must demonstrate 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." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 39-40 (1994). These elements are not a categorical test, but rather serve as threshold components of a valid claim to be used to "weed out claims that involve so insignificant or de minimis an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." *Loder v. City of Glendale*, 14 Cal. 4th 846, 893 (1997).

"A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill*, 7 Cal. 4th at 37. The decision "must take into account any 'accepted community norms,' advance notice to [Plaintiff] . . ., and whether [Plaintiff] had the opportunity to consent to or reject the very thing that constitutes the invasion." *TBG Ins. Servs. Corp. v. Superior Court*, 96 Cal. App. 4th 443 (2002). The plaintiff in an invasion of privacy action must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant. *Hill*, 7 Cal. 4th at 26. The "community norms" aspect of the "reasonable expectation of privacy" element means that "'[t]he protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.'" *TBG Ins. Servs. Corp.*, 96 Cal. App. 4th at 450. Finally, "[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. Thus, the extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy." *Hill*, 7 Cal. 4th at 37.

In the event a plaintiff establishes the three elements, the "diverse and somewhat amorphous character of the privacy right" may still be balanced with competing or countervailing interests of the defendant. *Id.* at 37-38 ("Conduct alleged to be an invasion of privacy is to be evaluated based on the extent to which it furthers legitimate and important competing interests."). "Invasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest." *Id.* at 38. Furthermore, if Plaintiffs' allegations "show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law." *Pioneer Electronics, Inc. v. Sup. Ct. of L.A.*, 40 Cal. 4th 360, 370 (2007) (citing *Hill*, 7 Cal. 4th at 40).

The California Constitution sets a "high bar" for establishing an invasion of privacy claim. *See Belluomini v. Citigroup, Inc.*, No. CV 13–01743 CRB, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013). Even disclosure of very personal information has not been deemed an "egregious breach of social norms" sufficient to establish a constitutional right to privacy. *Id.*; *see also In re*

iPhone Application Litig., 844 F. Supp. 2d at 1063 (holding that the disclosure to third parties of unique device identifier number, personal data, and geolocation information did not constitute an egregious breach of privacy sufficient to prove a serious invasion of a privacy interest); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008), *aff'd*, 380 Fed. Appx. 689 (9th Cir. 2010) (unpublished) (holding that the theft of a retail store's laptop containing personal information, including the social security numbers, of job applicants did not constitute an egregious breach of privacy and therefore was not sufficient to state a claim); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) ("Here, the supposed invasion of privacy essentially consisted of [defendant] obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine commercial behavior.").

Finally, "[w]hether a legally recognized privacy interest is present in a given case is a question of law to be decided by the court." *Hill*, 7 Cal. 4th at 40. "Whether plaintiff has a reasonable expectation of privacy in the circumstances and whether defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact. If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law." *Id.*

Here, the question is whether Plaintiffs have alleged sufficient facts to demonstrate (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by Yahoo that amounts to a serious invasion of that protected privacy interest. Plaintiffs allege that Yahoo scans and stores the content of emails between Yahoo Mail users and non-users, and distributes that content to third parties. Compl. ¶ 71. Plaintiffs allege they have a legally protected privacy interest "in the private email communications" they send to Yahoo Mail users. *See id.* ¶ 69; Opp'n at 24.[8] Plaintiffs assert that they "reasonably expect that their email

[8] Plaintiffs allege in the Complaint that they have a "legally protected interest in their private email communications with Yahoo Mail users." Compl. ¶ 69. From the Complaint alone, it is unclear if Plaintiffs allege that non-Yahoo Mail users have privacy interest in both the emails sent to and received from Yahoo Mail users. However, in their Opposition, Plaintiffs assert they have a privacy interest in the "emails they send to Yahoo Mail users." Opp'n at 23-24. This suggests

communications with Yahoo Mail users are private," and do not expect Yahoo to intercept, scan, and store the content of their emails without their consent. Compl. ¶ 70. Finally, Plaintiffs allege Yahoo committed an egregious breach of social norms when it intercepted these emails, scanned and stored their content, and distributed the content to third parties without Plaintiffs' consent. *Id.* ¶ 71. In response, Yahoo argues that Plaintiffs fail to set forth facts supporting all three elements but merely recite elements of the claim. Mot. at 21. Yahoo argues Plaintiffs "allege no facts regarding the content of their emails, their intent in sending those emails, the circumstances under which those emails were sent, or who the recipients of those emails were[.]" *Id.* at 21-22. The Court agrees with Yahoo that Plaintiffs have failed to allege sufficient facts to establish that Yahoo's conduct invaded their constitutionally protected right to privacy.

As a preliminary matter, under California law there are only two classes of legally protected privacy interests under the California Constitution: "interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ('autonomy privacy')." *Hill*, 7 Cal. 4th at 35. It is unclear from Plaintiffs' briefing and allegations whether Plaintiffs assert a claim for informational privacy or autonomy privacy. However, the Court construes Plaintiffs' claim as asserting only an informational privacy interest, as California courts have discussed autonomy privacy in the context of cases alleging *bodily* autonomy. *See, e.g., Comm. To Defend Reprod. Rights v. Myers*, 29 Cal. 3d 252, 275 (1981) (noting there is a constitutional right to privacy in a woman's "personal bodily autonomy"); *Smith v. Fresno Irrigation Dist.*, 72 Cal. App. 4th 147, 161 (1999) (discussing autonomy privacy in the context of drug testing through use of a urine sample).

Next, the Court notes it is unclear from Plaintiffs' allegations and briefing whether Plaintiffs claim a privacy interest in their emails generally, or in the specific *content* in the emails they sent to Yahoo Mail users. To the extent Plaintiffs claim a legally protected privacy interest and reasonable expectation of privacy in email *generally* based on the mere fact that Yahoo

---

Plaintiffs only intend to allege that they have a constitutionally protected privacy interest in their own outgoing email content rather than the content they receive from Yahoo Mail users.

intercepted and distributed their emails, regardless of the specific content in the emails, Plaintiffs' claim fails as a matter of law. Plaintiffs do not cite, nor has this Court found, any case in the California or federal courts holding that individuals have a legally protected privacy interest or reasonable expectation of privacy in emails generally. Rather, the cases in which courts have found a protected privacy interest in the context of email communications have done so in circumstances where the plaintiff alleged *with specificity* the material in the content of the email. *See, e.g.*, *Mintz v. Mark Bartelstein & Associates Inc.*, 906 F. Supp. 2d 1017, 1033-34 (C.D. Cal. 2012) (finding legally protected privacy interest in the personal financial and employment information contained in an email account). The conclusion that there is no legally protected privacy interest and reasonable expectation of privacy in emails as a general matter is consistent with well-established California law that in the context of informational privacy, the California Constitution protects only the "dissemination or misuse of *sensitive* and *confidential* information." *Hill*, 7 Cal. 4th at 35 (emphasis added). *Hill* suggests that in order to receive protection under the Constitution for an email communication, Plaintiffs must allege that the email intercepted actually included content that qualifies under California law as "confidential" or "sensitive." Indeed, courts make their decisions regarding whether a plaintiff has stated a legally protectable privacy interest based on the nature of the information at issue. *See, e.g.*, *Tourgeman v. Collins Financial Servs. Inc.*, No. 08–01392, 2009 WL 6527758, at *2 (S.D. Cal. Nov. 23, 2009) (holding plaintiff had legally protected privacy interest by citing California case law holding that financial information is protectable); *see also Zbitoff v. Nationstar Mortgage, LLC*, No. C 13–05221 WHA, 2014 WL 1101161, at *4 (N.D. Cal. March 18, 2014) (holding plaintiff failed to state privacy claim "with the required specificity" where she "merely state[d] that she had a 'reasonable expectation that defendants would preserve the privacy of [p]laintiff's private information'" and did "not identify exactly *what* private information defendants are alleged to have disclosed in relation to the credit checks[.]" (emphasis added)); *Norman–Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1271 n.17 (9th Cir. 1998) ("Under California law, a legally recognizable privacy interest arises from the sort of information revealed[.]").[9] Thus, to the extent Plaintiffs claim they have a legally protected privacy interest and

[9] The nature of the content at issue is also examined when courts assess whether the third prong of

reasonable expectation of privacy in email *generally*, regardless of the specific content in the emails at issue, Plaintiffs' claim fails as a matter of law.

However, this Court concludes, as others have, that there can be a legally protected privacy interest or reasonable expectation of privacy in any confidential and sensitive content within emails. *See, e.g.*, *Mintz*, 906 F. Supp. 2d at 1033-34 (finding legally protected privacy interest in personal financial and employment information contained in emails).[10] The problem for Plaintiffs in the instant case, however, is that to the extent Plaintiffs intend to allege that they have a privacy interest in the specific content of their emails, their allegations are fatally conclusory. The Complaint merely alleges that Plaintiffs' emails were "private" without alleging any facts related to what particular emails Yahoo intercepted, or the content within particular emails. *See* Compl. ¶¶ 69-70; *Zbitoff*, 2014 WL 1101161, at *4 (holding allegations for constitutional privacy claim were conclusory because plaintiff "merely state[d]" defendants disclosed her "private information"); *Scott-Codiga v. Cnty. of Monterey*, 10-CV-05450-LHK, 2011 WL 4434812, at *7 (N.D. Cal. Sept. 23, 2011) (dismissing constitutional privacy claim on ground that plaintiff had not "specified the material defendants released to the public in enough detail for the Court to determine whether it might conceivably fall within a recognized privacy interest protected by the [California] constitution" (internal citation omitted)). Without more, Plaintiffs' allegations are simply a bare recitation of the elements of a privacy claim, and this Court cannot assess whether Plaintiffs had a legally protected privacy interest in the specific emails that Yahoo intercepted, or a reasonable expectation of privacy in the content within those emails.

Plaintiffs' arguments to the contrary are unavailing. First, they argue that they have stated a privacy claim by emphasizing that they do not consent to Yahoo's conduct. Opp'n at 23-24;

---

a privacy claim is met – i.e., whether there was a serious or egregious violation of social norms. *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (declining to find that defendant violated constitutional right to privacy in releasing digital identification information to third parties in part because "it is not clear . . . *what* information, precisely, these third parties have obtained." (emphasis added)).

[10] While Yahoo cites this Court's holding in *Gmail* that the plaintiffs in that case had not shown that the email communications were "confidential communications" under CIPA § 632, Reply at 15, *Gmail* did not suggest or hold that there can never be a reasonable expectation of privacy in email content. Rather, *Gmail* confronted a circumstance similar to the instant motion, where plaintiffs suggested that emails in general were confidential.

Compl. ¶¶ 70-71. However, Plaintiffs cite no authority in support of their argument that an allegation of lack of consent suffices to state a privacy claim. Rather, the case law suggests that in determining whether a plaintiff has satisfied the elements of the claim, a plaintiff's lack of consent does not matter so much as the nature of the information in which he or she alleges a privacy interest. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 ("Even assuming this information was transmitted *without Plaintiffs' knowledge and consent*, a fact disputed by Defendants, such disclosure [of information including device identifier number, personal data, and geolocation information] does not constitute an egregious breach of social norms." (emphasis added)).

Plaintiffs also argue that they need not allege that each of their emails contained confidential information in order to state a claim because the right to privacy was adopted to protect the public from the "stockpiling of personal information." Opp'n at 24. Plaintiffs cite to the ballot argument for the initiative creating the constitutional right to privacy as evidence that the people intended to prevent "government and business interests from collecting and stockpiling unnecessary information about us and or misusing information gathered for one purpose in order to serve other purposes or to embarrass us." *Id.* at 23 (citing *Hill*, 7 Cal. 4th at 27). According to Plaintiffs, this history demonstrates that the right to privacy protects individuals from Yahoo's unauthorized scanning and storage of private email content for their own financial gain. *Id.* at 23-24. The Court is not convinced. Plaintiffs cite no authority holding that an allegation of "stockpiling" by itself is sufficient to state a privacy claim, and somehow nullifies the need to allege facts regarding the three required prongs of the *Hill* test.[11] To the contrary, this Court has

[11] Plaintiffs' cited cases do not so hold. Opp'n at 25. Rather, they are inapposite, as they arise in the Fourth Amendment context. *See United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013). In these cases, courts considered the implications of the government's intelligence gathering and surveillance practices, and the compelled disclosure of communications held by an internet service provider. A person's reasonable expectation of privacy is considerably distinct in the context of the instant case, where an ECS provider scanned emails that were either written by Yahoo Mail users through a service Yahoo itself provided (Yahoo Mail) or were voluntarily sent to Yahoo's servers. Furthermore, a claim under Article 1, Section 1 requires a plaintiff to show the privacy invasion is serious and "egregious," thus setting a higher threshold than for a federal claim under the Fourth Amendment. *Chevron Corp. v. Donziger*, 12-MC-80237 CRB (NC), 2013 WL

noted that merely alleging stockpiling is not enough; plaintiffs must still allege facts with respect to the three elements. *See Low*, 900 F. Supp. 2d at 1024 n.3 (holding, where plaintiffs argued that the intent of the voters was to prevent "stockpiling" of information, that "[e]ven in light of this ballot history, the subsequent case law regarding the Constitutional right to privacy establishes that only serious invasions of privacy give rise to a private right of action.").[12]

In sum, because Plaintiffs do not plead sufficient facts to allege an invasion of privacy, Yahoo's Motion to Dismiss Plaintiffs' claims for a violation of Article I, Section 1 of the California Constitution is GRANTED. However, the Court grants leave to amend because Plaintiffs may be able to plead specific email content in specific emails that may suffice to state the elements of the claim.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS Yahoo's Motion to Dismiss with prejudice Plaintiffs' Wiretap Act claim that Yahoo scans and analyzes emails for the purposes of providing personal product features, providing targeted advertising, detecting spam and abuse, creating user profiles, and sharing information with third parties. The Court GRANTS Yahoo's Motion to Dismiss without prejudice Plaintiffs' Wiretap Act claim with respect to collecting and storing emails for future use.

4536808, at *10 (N.D. Cal. Aug. 22, 2013) (citing *Norman–Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1271 (9th Cir. 1998)).

[12] While Plaintiffs rely on *Ung v. Facebook, Inc.*, Santa Clara County Superior Court Case No. 1-12-cv-217244, Dkt. No. 54 (July 2, 2012), *see* ECF No. 40-1 at 230, that case did not hold that an allegation of stockpiling information automatically suffices to state a privacy claim. Further, that case is distinguishable. There, where it was alleged that Facebook created user profiles linked to Facebook users' identities by tracking the internet browsing history of users across numerous other websites even when the user is not logged into Facebook, the court found a legally protected privacy interest in users' "identifiable browsing history" because Facebook could link the history to their identities, or names. *Id.* The court also held that *non*-Facebook users did *not* have a protected interest in their browsing history which Facebook tracked because the history "had not been linked to their identities." *Id.* Plaintiffs in *Yahoo* are more analogous to the non-Facebook users in *Ung* who did not have a privacy interest because the emails Yahoo allegedly intercepts are not linked to Plaintiffs' identities, as Yahoo does not necessarily know who Plaintiffs are. While Plaintiffs allege Yahoo creates "profiles" of them, Compl. ¶ 27, Plaintiffs do not allege that Yahoo attempts to link the information it acquires to Plaintiffs' *identities* (i.e., to their *names*) as opposed to just creating generic profiles that describe Plaintiffs' interests and general characteristics (female, likes shampoo products, etc).

The Court GRANTS Yahoo's Motion to Dismiss with prejudice with respect to Plaintiffs' SCA claim for unauthorized access under § 2701(a). The Court DENIES Yahoo's Motion to Dismiss Plaintiffs' SCA claim for improper disclosure under § 2702(a)(1). The Court GRANTS Yahoo's Motion to Dismiss without prejudice Plaintiffs' claim under Article I, Section 1 of the California Constitution. The Court DENIES Yahoo's Motion to Dismiss Plaintiffs' CIPA § 631 claim.

Plaintiffs shall file any amended complaint within 21 days of this order. Plaintiffs may not add new causes of action or parties without a stipulation or order of the Court under Rule 15 of the Federal Rules of Civil Procedure. Failure to cure the deficiencies addressed in this Order will result in dismissal with prejudice.

IT IS SO ORDERED.

Dated: August 12, 2014

LUCY H. KOH
United States District Judge