

# Exhibit B

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

DANIEL MATERA,  
Plaintiff,  
v.  
GOOGLE INC.,  
Defendant.

Case No. 15-CV-04062-LHK

**ORDER GRANTING IN PART AND  
DENYING IN PART DEFENDANT’S  
MOTION TO DISMISS BASED ON  
LACK OF STANDING**

Re: Dkt. No. 20

Plaintiff Daniel Matera (“Plaintiff”), individually and on behalf of those similarly situated, alleges that Defendant Google Inc. (“Google”) violated federal and state anti-wiretapping laws in its operation of Gmail, an email service. ECF No. 1 (“Compl.”).<sup>1</sup> Before the Court is Google’s motion to dismiss based on lack of standing. ECF No. 20. Having considered the parties’ submissions, the relevant law, and the record in this case, the Court **GRANTS IN PART AND DENIES IN PART** Google’s motion to dismiss based on lack of standing.

---

<sup>1</sup> Unless otherwise noted, all ECF references are to the docket of 15-CV-04062 in the Northern District of California.

1 **I. BACKGROUND**

2 **A. Factual Background**

3 **1. *In re Google Inc. Gmail Litigation***

4 Plaintiff's factual allegations overlap significantly with those in the related action *In re*  
5 *Google Inc. Gmail Litigation* ("*Gmail*"), 13-MD-02430, a consolidated multi-district litigation in  
6 which this Court considered whether Google's operation of Gmail violated federal and state anti-  
7 wiretapping laws. As both the factual and procedural history of *Gmail* are relevant to the instant  
8 motion, the Court briefly summarizes the background of that litigation.

9 Google provides several different but related systems of email delivery. First is a free  
10 service for individual users, which allows any user to register for an "@gmail.com" email address.  
11 *In re Google Inc. Gmail Litig.* ("*Gmail*"), 2013 WL 5423918, at \*2 (N.D. Cal. Sept. 26, 2013); *In*  
12 *re Google Inc. Gmail Litig.* ("*Gmail Class Cert.*"), 2014 WL 1102660, at \*1 (N.D. Cal. Mar. 18,  
13 2014). Second, Google offers "Google Apps" to businesses, educational organizations, and  
14 internet service providers ("ISPs"). *Gmail Class Cert.*, 2014 WL 1102660, at \*1. The end users  
15 of Google Apps do not receive "@gmail.com" email addresses. Rather, the email addresses  
16 contain the domain name of the business, educational institution, or ISP that contracts with Google  
17 to provide the email service (for example, "@cableone.com"). *Id.* However, Google Apps email  
18 services are powered by Google through Gmail.

19 The *Gmail* plaintiffs alleged that Google intercepted, read, and acquired the content of  
20 emails that were sent to or received by a Gmail user while the emails were in transit. *Gmail*, 2013  
21 WL 5423918, at \*1. Google allegedly intercepted the emails for the dual purposes of (1)  
22 providing advertisements targeted to the email's recipient or sender, and (2) creating user profiles  
23 to advance Google's profit interests. *Id.* According to the *Gmail* plaintiffs, Google's interception,  
24 scanning, and analyzing of email was done without the plaintiffs' knowledge or consent.

25 As relevant to the instant case, the putative class in *Gmail* included a class of all United  
26 States non-Gmail users "who have sent a message to a Gmail user and received a reply or received  
27 an email from a Gmail user." *Id.* at \*4. Because non-Gmail users exchange emails with Gmail

1 users, the *Gmail* plaintiffs alleged that non-Gmail users' communications were subject to the same  
 2 interception, scanning, and analyzing as Gmail users. The *Gmail* plaintiffs also sought to  
 3 represent (1) end users of Cable One, an ISP that contracted with Google to provide Google Apps-  
 4 related services to its customers; (2) users of Google Apps for Education; and (3) Gmail users  
 5 under the age of majority.

## 6 **2. Allegations in the Instant Case**

7 This case involves a subset of the *Gmail* putative class. In the instant case, Plaintiff seeks  
 8 to represent non-Gmail users "who have never established an email account with Google, and who  
 9 sent emails to or received emails from individuals with Google email accounts." Compl. ¶ 32. In  
 10 the complaint, Plaintiff uses "Gmail" to refer collectively to Gmail for individual users, Google  
 11 Apps for Work, and Google Apps for Education. *Id.* ¶ 1 n.1.

12 Plaintiff has never had a Gmail account. *Id.* ¶ 8. However, Plaintiff has sent emails to and  
 13 received emails from Gmail users, which Google allegedly has intercepted, scanned, and analyzed.  
 14 *Id.* In particular, Plaintiff alleges that Google employs a variety of devices that intercept, scan,  
 15 and analyze the content of emails during the transmission of emails to and from Gmail accounts.  
 16 For example, Google allegedly acquires and interprets the content of emails sent or received by  
 17 Gmail users through "Content Onebox" and "Changeling," which are "distinct piece[s] of  
 18 Google's infrastructure." *Id.* ¶ 19. Google then uses a process called "Nemo" to determine how  
 19 to best monetize the data extracted from the intercepted emails. *Id.* ¶ 20. Plaintiff contends that  
 20 these devices are "separate from the devices that are instrumental to sending and receiving email."  
 21 *Id.* ¶ 2.

22 Google allegedly uses the intercepted contents of Gmail messages for the "distinct  
 23 purpose" of creating targeted advertisements and user profiles to be stored indefinitely. *Id.* ¶¶ 21,  
 24 28. According to Plaintiff, Google utilizes the user profiles "for purposes of selling to paying  
 25 customers, and sending to the profiled communicants, targeted advertising based upon analysis of  
 26 these profiles." *Id.* ¶ 1; *see also id.* ¶ 17 (noting that Google "deliver[s] targeted advertisements  
 27

1 based on these [user] profiles”).

### 2 **3. Google’s Agreements with Users**

3 The operation of Gmail implicates two sets of legal agreements: those in place during the  
4 *Gmail* litigation and the amended agreements in place after the *Gmail* litigation. Plaintiff avers  
5 that during the *Gmail* litigation, “Google’s Gmail Terms of Service and Privacy Policy made no  
6 mention of the practices complained of herein, and thus Google failed to legally obtain the consent  
7 of Gmail users to the practices complained of herein.” Compl. ¶ 26.

8 In examining Google’s Terms of Service and Privacy Policies in place from April 16, 2007  
9 to September 26, 2013, this Court in *Gmail* determined that those documents did not sufficiently  
10 disclose Google’s alleged practice of intercepting and analyzing email content for commercial  
11 purposes. *Gmail*, 2013 WL 5423918, at \*12–14.

12 After the *Gmail* decision, Google amended both its Terms of Service and Privacy Policy.  
13 Specifically, Google amended its Terms of Service on April 14, 2014, *see* ECF No. 20-1 (“Google  
14 RJN”), Ex. A (“2014 TOS”). The 2014 TOS states that, “[b]y using our Services, you are  
15 agreeing to these terms. . . . If you do not agree to the modified terms for a Service, you should  
16 discontinue your use of that Service.” 2014 TOS at “About these Terms.” As relevant to  
17 Plaintiff’s allegations in the instant case, the 2014 TOS provides:

18 Our automated systems analyze your content (including emails) to provide you  
19 personally relevant product features, such as customized search results, tailored  
20 advertising, and spam and malware detection. This analysis occurs as the content is  
21 sent, received, and when it is stored.

22 *Id.* at “Your Content in our Services.” The 2014 TOS references Google’s Privacy Policies, and  
23 states that, “[b]y using our Services, you agree that Google can use such [personal] data in  
24 accordance with our privacy policies.” *Id.* at “Privacy and Copyright Protection.”

25 Google’s Privacy Policies have been amended at least eight times since January 1, 2013,  
26 including three times in 2015 alone. Compl. ¶ 30; *see also* Google RJN Ex. D (February 25, 2015  
27 Privacy Policy); Google RJN Ex. E (May 1, 2015 Privacy Policy); Google RJN Ex. F (June 5,  
28 2015 Privacy Policy); Google RJN Ex. G (June 30, 2015 Privacy Policy); Google RJN Ex. H

1 (August 19, 2015 Privacy Policy).

2 As relevant here, the December 19, 2014 Privacy Policy repeats the language in the 2014  
3 TOS that “Our automated systems analyze your content (including emails) to provide you  
4 personally relevant product features, such as customized search results, tailored advertising, and  
5 spam and malware detection.” Google RJN Ex. B. In addition, the December 19, 2014 Privacy  
6 Policy states that Google will “collect information about the services that you use and how you  
7 use them.” When the cursor is held over the phrase “collect information,” a text box appears.  
8 Google RJN ¶ 5. This text box states, “This includes information like your usage data and  
9 preferences, Gmail messages, G+ profile, photos . . . or other Google-hosted content. Learn  
10 more.” Clicking on the “Learn more” link in the “Example” box directs to a webpage entitled  
11 “collect information,” which states:

12 This includes information like your usage data and preferences, Gmail messages,  
13 G+ profile, photos, videos, browsing history, map searches, docs, or other Google-  
14 hosted content. Our automated systems analyze this information as it is sent and  
15 received and when it is stored.

16 This may include any content as it flows through our systems. For example, we  
17 may use the information in your Gmail inbox to provide you with flight  
18 notifications and check-in options, information in your Google+ profile to help you  
19 connect with your circles by email, and information in your web history cookies to  
20 provide you with more relevant search results.

21 Google RJN Ex. C.

22 Plaintiff contends that non-Gmail users like Plaintiff “were never subject to or on notice of  
23 Google’s Privacy Policy.” Compl. ¶ 8. Because non-Gmail users exchange emails with Gmail  
24 users, however, their communications are nevertheless subject to interception, scanning, and  
25 analysis by Google.

## 26 **B. Procedural History**

27 In light of the relationship between the instant case and *Gmail*, the Court briefly  
28 summarizes the relevant procedural history of *Gmail* in addition to the instant case.

### 1. Procedural History of *Gmail*

The first case that comprised the *Gmail* multi-district litigation, *Dunbar v. Google, Inc.*,

1 was filed on November 17, 2010 in the Eastern District of Texas. *See Dunbar v. Google, Inc.*, No.  
2 10-CV-00194, ECF No. 1 (E.D. Tex. Nov. 17, 2010). On June 27, 2012, upon Google's motion,  
3 the case was transferred to the Northern District of California and assigned to the undersigned  
4 judge. *See Dunbar v. Google, Inc.*, No. 12-CV-03305, ECF No. 180 (N.D. Cal. July 23, 2012).

5 While *Dunbar* was pending, five other actions involving substantially similar allegations  
6 against Google were filed in this District and throughout the country. *See Scott v. Google, Inc.*  
7 (*"Scott I"*), No. 12-CV-03413 (N.D. Cal.); *Scott v. Google, Inc.* (*"Scott II"*), No. 12-CV-00614  
8 (N.D. Fla.); *A.K. v. Google, Inc.*, No. 12-CV-01179 (S.D. Ill.); *Knowles v. Google, Inc.*, No. 12-  
9 CV-02022 (D. Md.); *Brinkman v. Google, Inc.*, No. 12-CV-00699 (E.D. Pa.). On April 1, 2013,  
10 the Judicial Panel on Multidistrict Litigation issued a Transfer Order, centralizing *Dunbar* along  
11 with the five other actions in the Northern District of California before the undersigned judge. *See*  
12 No. 13-MD-02430, ECF No. 1. The Court later related a seventh case to the multi-district  
13 litigation, *Fread v. Google, Inc.*, No. 13-CV-01961 (N.D. Cal.). *See* No. 13-MD-02430, ECF No.  
14 29.

15 The *Gmail* plaintiffs filed a Consolidated Complaint on May 16, 2013. No. 13-MD-02430,  
16 ECF No. 38. That complaint attempted to state causes of action under (1) the Electronic  
17 Communications Privacy Act of 1986 (the "ECPA" or the "Wiretap Act"), 18 U.S.C. § 2510 *et*  
18 *seq.*; (2) California's Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 *et seq.*; (3)  
19 Maryland's Wiretap Act, Md. Code Ann., Cts. & Jud. Proc. § 10-402; (4) Florida's Wiretap Act,  
20 Fla. Stat. Ann. § 934.01; and (5) Pennsylvania's Wiretapping and Electronic Surveillance Control  
21 Act, 18 Pa. Cons. Stat. § 5701. Google moved to dismiss the Consolidated Complaint on June 13,  
22 2013. *See* No. 13-MD-02430, ECF No. 44.

23 The Court granted in part and denied in part Google's motion on September 26, 2013. *See*  
24 No. 13-MD-02430, ECF No. 69. As relevant here, the Court denied the motion to dismiss  
25 plaintiffs' Wiretap Act claim. Specifically, the Court rejected Google's contention that any  
26 alleged interceptions fell within the "ordinary course" of Google's business and were therefore  
27

1 exempt from anti-wiretapping statutes. Using the tools of statutory interpretation, the Court  
2 concluded that the “ordinary course of business” exception was “designed only to protect  
3 electronic communication service providers against a finding of liability under the Wiretap Act  
4 where the interception facilitated or was incidental to provision of the electronic communication  
5 service at issue.” *Id.* at 13–20.

6 In addition, the Court rejected Google’s argument that Gmail users had consented to the  
7 alleged interceptions based on Google’s Terms of Service and Privacy Policies. The Court  
8 concluded that the Terms of Service and Privacy Policies did not provide sufficient disclosures to  
9 show that Gmail users had consented to the alleged interceptions. *Id.* at 22–26. The Court further  
10 rejected Google’s contention that all email users had impliedly consented to the alleged  
11 interceptions because all email users, including non-Gmail users, understand that such  
12 interceptions are part of how emails are transmitted. *Id.* at 27–28.

13 The Court also held that the *Gmail* plaintiffs could proceed on their claims under section  
14 631 of CIPA, California’s anti-wiretapping law. *Id.* at 28–40. The Court first found that section  
15 631 applies to email, not just to communications passing over telephone and telegraph wires, lines,  
16 or cables. The Court also concluded that Google was not exempt from section 631 liability as a  
17 “public utility.” Accordingly, the Court denied Google’s motion to dismiss the *Gmail* plaintiffs’  
18 section 631 claim.

19 On October 25, 2013, the *Gmail* plaintiffs moved for class certification of a damages class  
20 under Federal Rule of Civil Procedure 23(b)(3). No. 13-MD-02430, ECF No. 87-26. On March  
21 18, 2014, the Court denied class certification. No. 13-MD-02430, ECF No. 158. Specifically, the  
22 Court found that the *Gmail* plaintiffs had failed to meet the predominance requirement, which  
23 “tests whether proposed classes are sufficiently cohesive to warrant adjudication by  
24 representation.” *Id.* at 23. The Court concluded that the question of whether the *Gmail* class  
25 members had consented to the alleged interceptions needed to be litigated on an individual rather  
26 than classwide basis. The Court further concluded that individualized inquiries into consent  
27



1 would predominate over questions common to the class and thus denied class certification. On  
 2 May 12, 2014, the Ninth Circuit denied the *Gmail* plaintiffs' petition for interlocutory review of  
 3 the Court's class certification order. No. 13-MD-02430, ECF No. 174.

4 Following the Court's class certification ruling, only the individual plaintiffs' individual  
 5 claims remained. Google and the individual plaintiffs settled the individual claims and filed  
 6 stipulations of dismissal as to all cases. No. 13-MD-02430, ECF Nos. 175, 177. The case was  
 7 closed on July 14, 2014.

## 8 **2. Procedural History of the Instant Case**

9 Plaintiff filed the instant complaint on September 4, 2015. ECF No. 1. Similar to the  
 10 *Gmail* plaintiffs, Plaintiff asserts violations of the ECPA and CIPA. Plaintiff seeks to represent  
 11 the following classes:

12 CIPA Class (Count One): All persons in the State of California who have never  
 13 established an email account with Google, and who have sent emails to or  
 14 received emails from individuals with Google email accounts.

15 ECPA Class (Count Two): All persons in the United States who have never  
 16 established an email account with Google, and who sent emails to or received  
 17 emails from individuals with Google email accounts before December 19,  
 18 2014.

19 *Id.* ¶ 32. On September 23, 2015, the case was related to *Gmail* and reassigned to the undersigned  
 20 judge. ECF No. 13.

21 On October 29, 2015, Google filed a motion to dismiss, ECF No. 20 ("Mot."), and a  
 22 request for judicial notice, ECF No. 20-1. On December 4, 2015, Plaintiff opposed the motion to  
 23 dismiss, ECF No. 29 ("Opp."), and filed a request for judicial notice, ECF No. 31 ("Pl. RJN").  
 24 Google replied on December 22, 2015. ECF No. 33 ("Reply").

25 The same day that Google filed the motion to dismiss, Google also moved to temporarily  
 26 stay the case pending the Supreme Court's resolution of *Spokeo, Inc. v. Robins*, No. 13-01339.  
 27 ECF No. 21. Because the Court concluded that *Spokeo* may determine whether Plaintiff has  
 28 standing to proceed in this action, the Court granted Google's motion to stay on February 5, 2016.  
 ECF No. 36. On April 28, 2016, this Court set a case management conference for May 25, 2016.

1 ECF No. 37.

2 The Supreme Court issued an opinion in *Spokeo* on May 16, 2016. *See Spokeo, Inc. v.*  
3 *Robins*, 136 S. Ct. 1540 (2016). At the May 25, 2016 case management conference, the Court  
4 lifted the stay in the instant case and ordered supplemental briefing as to the impact of *Spokeo* on  
5 Plaintiff's standing. ECF No. 40. The parties filed simultaneous opening briefs on the impact of  
6 *Spokeo* on June 1, 2016. ECF No. 41 ("Pl. Supp. Br."); ECF No. 41 ("Google Supp. Br."). The  
7 parties filed simultaneous reply briefs on June 13, 2016. ECF No. 45 ("Pl. Supp. Reply"); ECF  
8 No. 46 ("Google Supp. Reply").

9 On August 12, 2016, the Court denied Google's motion to dismiss as to the merits of  
10 Plaintiff's claims. ECF No. 49. Specifically, the Court concluded that *Gmail* correctly analyzed  
11 the Wiretap Act's "ordinary course of business" exception, which is "designed only to protect  
12 electronic communication service providers against a finding of liability under the Wiretap Act  
13 where the interception facilitated or was incidental to provision of the electronic communication  
14 service at issue." Applying that interpretation to the instant case, the Court rejected Google's  
15 contention that the alleged interceptions of Plaintiff's email fell within the "ordinary course" of  
16 Google's business. *Id.* at 10–25. Accordingly, the Court denied Google's motion to dismiss  
17 Plaintiff's Wiretap Act claim. The Court declined to certify the interpretation of the "ordinary  
18 course of business" exception to the Ninth Circuit. *Id.* at 25–27.

19 In addition, the Court denied Google's motion to dismiss Plaintiff's CIPA claim. The  
20 Court retained supplemental jurisdiction over the CIPA claim on the grounds of economy,  
21 convenience, and fairness. *Id.* at 27–30. Moreover, the Court rejected Google's arguments—  
22 duplicative of those presented by Google during the *Gmail* litigation—that CIPA did not apply to  
23 email. *Id.* at 31–37.

## 24 **II. LEGAL STANDARD**

### 25 **A. Rule 12(b)(1)**

26 A defendant may move to dismiss an action for lack of subject matter jurisdiction pursuant  
27

1 to Rule 12(b)(1) of the Federal Rules of Civil Procedure. While lack of statutory standing requires  
 2 dismissal for failure to state a claim under Rule 12(b)(6), lack of Article III standing requires  
 3 dismissal for want of subject matter jurisdiction under Rule 12(b)(1). *See Maya v. Centex Corp.*,  
 4 658 F.3d 1060, 1067 (9th Cir. 2011). “A Rule 12(b)(1) jurisdictional attack may be facial or  
 5 factual.” *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). “In a facial  
 6 attack,” like the one made by Google here, “the challenger asserts that the allegations contained in  
 7 a complaint are insufficient on their face to invoke federal jurisdiction.” *Id.* The Court “resolves a  
 8 facial attack as it would a motion to dismiss under Rule 12(b)(6): Accepting the plaintiff’s  
 9 allegations as true and drawing all reasonable inferences in the plaintiff’s favor, the court  
 10 determines whether the allegations are sufficient as a legal matter to invoke the court’s  
 11 jurisdiction.” *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014).

12 Once a defendant has moved to dismiss for lack of subject matter jurisdiction under Rule  
 13 12(b)(1), the plaintiff bears the burden of establishing the Court’s jurisdiction. *See Chandler v.*  
 14 *State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir. 2010). The plaintiff carries that  
 15 burden by putting forth “the manner and degree of evidence required” by whatever stage of the  
 16 litigation the case has reached. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). At the  
 17 motion to dismiss stage, Article III standing is adequately demonstrated through allegations of  
 18 “specific facts plausibly explaining” why the standing requirements are met. *Barnum Timber Co.*  
 19 *v. EPA*, 633 F.3d 894, 899 (9th Cir. 2011).

#### 20 **B. Rule 12(b)(6) Motion to Dismiss**

21 Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include “a  
 22 short and plain statement of the claim showing that the pleader is entitled to relief.” A complaint  
 23 that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). Rule 8(a) requires a  
 24 plaintiff to plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl.*  
 25 *Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff  
 26 pleads factual content that allows the court to draw the reasonable inference that the defendant is  
 27

1 liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility  
2 standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a  
3 defendant has acted unlawfully.” *Id.* (internal quotation marks omitted).

4 For purposes of ruling on a Rule 12(b)(6) motion, the Court “accept[s] factual allegations  
5 in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving  
6 party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). The  
7 Court, however, need not accept as true allegations contradicted by judicially noticeable facts, *see*  
8 *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and it “may look beyond the plaintiff’s  
9 complaint to matters of public record” without converting the Rule 12(b)(6) motion into a motion  
10 for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor must the  
11 Court “assume the truth of legal conclusions merely because they are cast in the form of factual  
12 allegations.” *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam). Mere  
13 “conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to  
14 dismiss.” *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

### 15 **C. Leave to Amend**

16 If the Court concludes that the complaint should be dismissed, it must then decide whether  
17 to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to  
18 amend “shall be freely given when justice so requires,” bearing in mind “the underlying purpose  
19 of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or  
20 technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (ellipsis in  
21 original). Nonetheless, a district court may deny leave to amend a complaint due to “undue delay,  
22 bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by  
23 amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of  
24 the amendment, [and] futility of amendment.” *See Leadsinger, Inc. v. BMG Music Publ’g*, 512  
25 F.3d 522, 532 (9th Cir. 2008).

### 26 **III. JUDICIAL NOTICE**

1 Plaintiff and Google have each filed requests for judicial notice. Under Federal Rule of  
2 Evidence 201(b), the Court can take judicial notice of any fact that is “not subject to reasonable  
3 dispute because it . . . can be accurately and readily determined from sources whose accuracy  
4 cannot reasonably be questioned.” Fed. R. Evid. 201(b). Under the doctrine of incorporation by  
5 reference, the Court also may consider documents whose contents are alleged in the complaint,  
6 provided that the complaint “necessarily relies” on the documents, the documents’ authenticity is  
7 uncontested, and the documents’ relevance is uncontested. *Coto Settlement v. Eisenberg*, 593 F.3d  
8 1031, 1038 (9th Cir. 2010).

9 Plaintiff asks for judicial notice of the transcript of the November 2, 2015 oral argument  
10 before the U.S. Supreme Court in *Spokeo*, as well as a U.S. Senate Report regarding the passage of  
11 the ECPA. See Pl. RJN. Google requests judicial notice of the 2014 TOS; various versions of  
12 Google’s Privacy Policy; Google’s website entitled “Updates: Privacy Policy”; two reports from  
13 California Senate Committees; and three bills introduced in the California Legislature. See  
14 Google RJN. Both Plaintiff’s and Google’s requests for judicial notice are unopposed, and the  
15 documents therein are the proper subject of judicial notice. See *Anderson v. Holder*, 673 F.3d  
16 1089, 1094 n.1 (9th Cir. 2012) (“Legislative history is properly a subject of judicial notice.”); *Lee*  
17 *v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001) (matters of public record), *overruled in*  
18 *part on other grounds by Galbraith v. Cty. of Santa Clara*, 307 F.3d 1119, 1125–26 (9th Cir.  
19 2002); *Caldwell v. Caldwell*, 2006 WL 618511, at \*4 (N.D. Cal. Mar. 13, 2006) (publicly  
20 accessible websites). Accordingly, the Court GRANTS Plaintiff’s and Google’s requests for  
21 judicial notice.

#### 22 **IV. DISCUSSION**

23 Google raises two challenges to Plaintiff’s standing. First, Google contends that Plaintiff  
24 has failed to plead injury in fact under the standard set forth in *Spokeo, Inc. v. Robins*, 136 S. Ct.  
25 1540 (2016). Thus, Google argues that Plaintiff lacks standing to pursue Plaintiff’s claims under  
26 either the Wiretap Act or CIPA. Second, Google argues that Plaintiff lacks standing to seek  
27

United States District Court  
Northern District of California

1 injunctive relief. Under the Wiretap Act, the consent of one party to the interception of the  
2 communication is a complete defense to liability. 18 U.S.C. § 2511(2)(d). Under CIPA, a consent  
3 defense is established when both parties—the sender and the recipient of the communication—  
4 consent to the alleged interception. Cal. Penal Code § 631(a). In the instant case, according to  
5 Google, there is no risk of Plaintiff suffering future injury because Google’s post-*Gmail* Terms of  
6 Service and Privacy Policies establish Gmail users’ consent to the interception, scanning, and  
7 analysis of their email. The Court addresses Google’s standing challenges in turn.

8 **A. Injury in Fact**

9 **1. Legal Standard**

10 Plaintiff “bear[s] the burden of establishing . . . standing to sue.” *San Diego Cty. Gun*  
11 *Rights Comm. v. Reno*, 98 F.3d 1121, 1126 (9th Cir. 1996). “To do so, [Plaintiff] must  
12 demonstrate three elements which constitute the irreducible constitutional minimum of Article III  
13 standing.” *Id.* (internal quotation marks omitted). First, Plaintiff “must have suffered an injury-  
14 in-fact to a legally protected interest that is both concrete and particularized and actual or  
15 imminent, as opposed to conjectural or hypothetical.” *Id.* (internal quotation marks omitted).  
16 Second, “there must be a causal connection between the[] injury and the conduct complained of.”  
17 *Id.* Third, “it must be likely—not merely speculative—that the[] injury will be redressed by a  
18 favorable decision.” *Id.* (internal quotation marks omitted). In the class action context, “standing  
19 is satisfied if at least one named plaintiff meets the[se] [three] requirements.” *Bates v. United*  
20 *Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007).

21 **2. Application**

22 Google limits its attack on Plaintiff’s standing to the first of the three standing  
23 requirements: injury in fact. Plaintiff alleges that Google intercepts, scans, and analyzes the  
24 content of Plaintiff’s private emails for commercial purposes and without consent, in violation of  
25 the Wiretap Act and CIPA. Compl. ¶¶ 1–4, 7–8, 18–24. According to Plaintiff, these violations  
26 are “egregious and illegal invasions of privacy,” and constitute injury in fact. *Id.* ¶ 7.

United States District Court  
Northern District of California

1 In response, Google argues that Plaintiff can not rely “solely on the purported statutory  
2 violations *alone* as the basis for Article III standing.” Google Supp. Br. at 1. According to  
3 Google, in light of the U.S. Supreme Court’s *Spokeo* decision, Plaintiff must allege a concrete  
4 harm that is “*independent[]* of the alleged statutory violations.” *Id.* at 1, 4. Because Plaintiff  
5 relies only on the alleged statutory violations, without claiming any additional harm, Google  
6 argues that Plaintiff has not pled a “concrete” injury in fact.

7 In addressing Google’s argument, the Court first examines the legal standard set forth in  
8 *Spokeo* in more detail. The Court then analyzes whether, under *Spokeo*, Plaintiff sufficiently  
9 alleges a concrete injury.

10 **a. *Spokeo***

11 In *Spokeo*, the U.S. Supreme Court reiterated two longstanding principles governing the  
12 injury in fact analysis. First, the U.S. Supreme Court confirmed that for an injury to be  
13 “concrete,” it must be “*de facto*,” meaning that it is “real,” and not “abstract.” *Spokeo*, 136 S. Ct.  
14 at 1548. However, an injury need not be “tangible” in order to be “concrete,” and intangible  
15 injuries may constitute injury in fact. *Id.* at 1549.

16 Second, the *Spokeo* Court reaffirmed that Congress may “elevat[e]” injuries “previously  
17 inadequate in law” to legally cognizable “concrete” injuries. *Id.* at 1549 (quoting *Lujan*, 504 U.S.  
18 at 578); *see also Lujan*, 504 U.S. at 580 (Kennedy, J., concurring) (“Congress has the power to  
19 define injuries and articulate chains of causation that will give rise to a case or controversy where  
20 none existed before.”). In other words, the violation of a right granted by statute may be sufficient  
21 to constitute injury in fact, without alleging “any *additional* harm beyond the one Congress has  
22 identified.” *Spokeo*, 136 S. Ct. at 1549; *see also Warth v. Seldin*, 422 U.S. 490, 500 (1975)  
23 (stating that the “actual or threatened injury required by Art. III may exist solely by virtue of  
24 statutes creating legal rights, the invasion of which creates standing” (internal quotation marks  
25 omitted)). Justice Thomas, concurring in *Spokeo*, put the principle plainly: “Congress can create  
26 new private rights and authorize private plaintiffs to sue based simply on the violation of those  
27

1 private rights,” such that “[a] plaintiff seeking to vindicate a statutorily created private right need  
2 not allege actual harm beyond the invasion of that private right.” *Spokeo*, 136 S. Ct. at 1553  
3 (Thomas, J., concurring).

4 Accordingly, *Spokeo* clearly rejects Google’s position that a plaintiff may *never* rely  
5 “solely on the purported statutory violations *alone* as the basis for Article III standing.” Google  
6 Supp. Br. at 1. Rather, a plaintiff may plead injury in fact by alleging the violation of a statute  
7 without alleging “any *additional* harm beyond the one Congress has identified.” *Spokeo*, 136 S.  
8 Ct. at 1549.

9 However, Google is correct that not *every* harm recognized by statute will be sufficiently  
10 “concrete” for standing purposes. *Id.* (“Congress’ role in identifying and elevating intangible  
11 harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement  
12 whenever a statute grants a person a statutory right and purports to authorize that person to sue to  
13 vindicate that right.”). When evaluating whether the violation of a statute establishes concrete  
14 injury, *Spokeo* instructs courts to consider two factors.

15 First, because the standing requirement is grounded in “historical practice,” “it is  
16 instructive to consider whether an alleged intangible harm has a close relationship to a harm that  
17 has traditionally been regarded as providing a basis for a lawsuit in English or American courts.”  
18 *Id.*; *see also* *Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 774 (2000) (“Article  
19 III’s restriction of the judicial power to ‘Cases’ and ‘Controversies’ is properly understood to  
20 mean ‘cases and controversies of the sort traditionally amenable to, and resolved by, the judicial  
21 process.’”).

22 Second, “because Congress is well positioned to identify intangible harms that meet  
23 minimum Article III requirements, its judgment is also instructive and important.” *Spokeo*, 136 S.  
24 Ct. at 1549. Relevant to this inquiry is whether Congress created a procedural or substantive right  
25 in the statute at issue. By way of example, in *Spokeo*, the defendant allegedly violated the Fair  
26 Credit Reporting Act (“FCRA”), which requires consumer reporting agencies to “follow



1 reasonable procedures to assure maximum possible accuracy of” consumer reports. *Id.* at 1545  
 2 (quoting 15 U.S.C. § 1681e(b)). The U.S. Supreme Court expressed no opinion as to whether this  
 3 procedural FCRA violation constituted a “concrete injury,” instead “leav[ing] that issue for the  
 4 Ninth Circuit to consider on remand.” *Id.* at 1550 & n.8. However, the U.S. Supreme Court did  
 5 note that “[i]t is difficult to imagine how the dissemination of an incorrect zip code [in violation of  
 6 the FCRA], without more, could work any concrete harm.” *Id.* Thus, while “the violation of a  
 7 procedural right granted by statute can be sufficient in some circumstances to constitute injury in  
 8 fact,” a “bare procedural violation, divorced from any concrete harm” is not. *Id.* at 1549 (citing  
 9 *Summers v. Earth Island Inst.*, 555 U.S. 488, 496 (2009) (“[D]eprivation of a procedural right  
 10 without some concrete interest that is affected by the deprivation . . . is insufficient to create  
 11 Article III standing.”)).

12 In sum, *Spokeo* held that two factors may be relevant to whether the violation of statutory  
 13 rights constitutes injury in fact: (1) whether the statutory violation bears a “close relationship to a  
 14 harm that has traditionally been regarded as providing a basis for a lawsuit in English or American  
 15 courts,” and (2) congressional judgment in establishing the statutory right, including whether the  
 16 statutory right is substantive or procedural. With these principles in mind, the Court proceeds to  
 17 analyze whether Plaintiff has alleged injury in fact.

18 **b. Relationship to a Harm that Has Traditionally Been Regarded as Providing a**  
 19 **Basis for a Lawsuit**

20 A Wiretap Act violation exists when any person “intentionally intercepts, endeavors to  
 21 intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or  
 22 electronic communication.” 18 U.S.C. § 2511(1)(a). Similarly, CIPA is violated when a person  
 23 “reads, or attempts to read, or to learn the contents or meaning of any message, report, or  
 24 communication while the same is in transit or passing over any wire, line, or cable.” Cal. Penal  
 25 Code § 631. Plaintiff asserts that the Wiretap Act and CIPA are intended to protect privacy, and  
 26 that claims under the two statutes bear a “close relationship” to the common law tort of invasion of  
 27 privacy. Because the common law recognized similar harms to those arising under the Wiretap

1 Act and CIPA, Plaintiff argues, this factor supports finding concrete injury in fact.

2 The Court agrees. Invasion of privacy has been recognized as a common law tort for over  
3 a century. *See* Restatement (Second) of Torts §§ 652A–I (noting that the right to privacy was first  
4 accepted by an American court in 1905, and “a right to privacy is now recognized in the great  
5 majority of the American jurisdictions that have considered the question”). One variation of  
6 invasion of privacy is intrusion upon seclusion, which makes a defendant liable for intruding,  
7 physically or otherwise, upon the solitude or seclusion of another’s private affairs. *Id.* § 652B.  
8 Numerous courts have recognized both invasion of privacy and intrusion upon seclusion. *See e.g.*,  
9 *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 493–94 (1975) (discussing the “developing law  
10 surrounding the tort of invasion of privacy”); *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos.*,  
11 306 F.3d 806, 812 (9th Cir. 2002) (analyzing Arizona’s tort of intrusion upon seclusion, a  
12 variation on invasion of privacy); *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286–87 (2009)  
13 (discussing a privacy violation based on California’s common law tort of intrusion).

14 Of particular relevance to the instant case, the Second Restatement of Torts recognizes that  
15 intrusion upon seclusion may occur through a defendant “opening [a plaintiff’s] private and  
16 personal mail” or “tapping [a plaintiff’s] telephone wires.” Restatement (Second) of Torts § 652B  
17 cmt. b. In line with the Restatement, courts across the country have found that the unauthorized  
18 interception of an individual’s private communications may state a claim for common law  
19 invasion of privacy. *See, e.g.*, *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976) (finding that a  
20 plaintiff stated a claim for common law invasion of privacy when “the defendant is accused of  
21 opening plaintiff’s private mail and reading it without authority”); *Quigley v. Rosenthal*, 327 F.3d  
22 1044, 1073 (10th Cir. 2003) (noting that, under Colorado law, “it is clear that the interception of  
23 the Quigleys’ telephone conversations would constitute an intentional intrusion on the Quigleys’  
24 seclusion or solitude”); *Billings v. Atkinson*, 489 S.W.2d 858, 860 (Tex. 1973) (noting that  
25 eavesdropping was an indictable offense at common law, and recognizing an invasion of privacy  
26 cause of action based on a wiretap of plaintiff’s telephone); *Arrington v. Colortyme, Inc.*, 972 F.

1 Supp. 2d 733, 746–47 (W.D. Pa. 2013) (denying motion to dismiss state law invasion of privacy  
2 claim based on electronic surveillance of plaintiff’s computer activity); *Cruikshank v. United*  
3 *States*, 431 F. Supp. 1355, 1360 (D. Haw. 1977) (finding that plaintiff stated a claim for  
4 intentional invasion of privacy based on government agents’ opening and photographing of  
5 plaintiff’s mail). Similar to the above authority, the Wiretap Act and CIPA each prohibit the  
6 unauthorized interception of an individual’s communications. 18 U.S.C. § 2511(1)(a); Cal. Penal  
7 Code § 631.

8 Moreover, both the Wiretap Act and CIPA were passed to protect against the invasion of  
9 privacy. In particular, the Wiretap Act “was intended to afford privacy protection to electronic  
10 communications.” *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002); *see also*  
11 *DirectTV, Inc. v. Webb*, 545 F.3d 837, 850 (9th Cir. 2008) (stating that the Wiretap Act’s  
12 “emphasis on privacy is evident in both the legislative history of the Wiretap Act and in the  
13 breadth of its prohibitions”). Likewise, CIPA was intended to “accord every citizen’s privacy the  
14 utmost sanctity” and “provide those who suffer an infringement of this aspect of their personal  
15 liberty a means of vindicating their right.” *Ribas v. Clark*, 38 Cal. 3d 355, 365 (Cal. 1985).  
16 Accordingly, violations of the Wiretap Act and CIPA are similar to common law invasion of  
17 privacy in both their substantive prohibitions and their purpose.

18 Google recognizes that invasion of privacy claims are similar to claims under the Wiretap  
19 Act and CIPA. However, Google counters that there is not a “close relationship” between the  
20 claims because common law invasion of privacy usually requires a plaintiff to prove elements that  
21 are not required by the Wiretap Act and CIPA, such as a reasonable expectation of privacy. *See*  
22 *Google Supp. Br.* at 4–7. For example, Google points to *In re Yahoo Mail Litigation*, 7 F. Supp.  
23 3d 1016, 1038–41 (N.D. Cal. 2014), in which this Court held that the plaintiffs failed to establish  
24 an invasion of privacy claim under the California Constitution because the plaintiffs failed to  
25 allege that the communications intercepted contained confidential and sensitive content. Google  
26 contends that the California Constitution’s requirements are parallel to common law invasion of  
27

1 privacy claims, and thus Plaintiff, like the plaintiffs in *Yahoo Mail*, must allege the specifics of the  
2 intercepted emails to show injury in fact under the Wiretap Act and CIPA.

3 The Court is not persuaded. Essentially, Google argues that the Wiretap Act and CIPA  
4 must have the same elements as common law invasion of privacy in order for violations of the  
5 Wiretap Act and CIPA to constitute injury in fact. However, such a requirement is inconsistent  
6 with *Spokeo*'s holding that Congress may "elevat[e] to the status of legally cognizable injuries  
7 concrete, de facto injuries that *were previously inadequate in law.*" *Spokeo*, 136 S. Ct. at 1549  
8 (emphasis added). Thus, that the Wiretap Act and CIPA are not identical in every respect to  
9 invasion of privacy does not preclude violations of the Wiretap Act and CIPA from constituting  
10 injury in fact. *See id.* (noting that a "close relationship to a harm that has traditionally been  
11 regarded as providing a basis for a lawsuit" supports finding injury in fact).

12 Case law since *Spokeo* confirms this result. The U.S. Court of Appeals for the Third  
13 Circuit found that the disclosure of information in violation of the Wiretap Act constitutes injury  
14 in fact. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 273–74 (3d Cir. 2016). The  
15 Third Circuit did not engage in a detailed comparison of the elements of the Wiretap Act and any  
16 common law claims. Rather, the Third Circuit found that "Congress has long provided plaintiffs  
17 with the right to seek redress for unauthorized disclosures of information that, in Congress's  
18 judgment, ought to remain private." *Id.* at 274; *cf. Thomas v. FTS USA, LLC*, — F. Supp. 3d —,  
19 2016 WL 3653878, at \*10 (E.D. Va. June 30, 2016) (finding injury in fact based on allegations of  
20 certain violations of the Fair Credit Reporting Act, and noting that "[t]he common law has long  
21 recognized a right to personal privacy, and 'both the common law and the literal understandings of  
22 privacy encompass the individual's control of information concerning his or her person.'" (quoting  
23 *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989))).

24 Here, Plaintiff asserts that Google intercepted, scanned, and analyzed Plaintiff's  
25 communications in violation of the Wiretap Act and CIPA. As recognized by the Third Circuit  
26 and other courts, and as seen in the common law invasion of privacy tort, such unauthorized  
27

1 interception of communications may give rise to a legally cognizable injury.

2 **c. Congressional Judgment in Establishing a Statutory Right, Including Whether**  
 3 **the Right is Substantive or Procedural**

4 The Court next considers Congress’s judgment in “elevat[ing] to the status of legally  
 5 cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.” *Spokeo*,  
 6 136 S. Ct. at 1549. Congress is “well positioned to identify intangible harms that meet minimum  
 7 Article III requirements.” *Id.* “Essentially, the standing question in such cases is whether the  
 8 constitutional or statutory provision on which the claim rests properly can be understood as  
 9 granting persons in the plaintiff’s position a right to judicial relief.” *Edwards v. First Am. Corp.*,  
 10 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Warth*, 422 U.S. at 500).

11 Since *Spokeo*, three factors have emerged that favor finding that a statute “grant[s] persons  
 12 in the plaintiff’s position a right to judicial relief”: (1) the provision of a private right of action; (2)  
 13 the availability of statutory damages; and (3) the substantive nature of the statutory right. For  
 14 example, in *Church v. Accretive Health, Inc.*, — F. App’x —, 2016 WL 3611543 (11th Cir. July  
 15 6, 2016), the Eleventh Circuit found that the plaintiff sufficiently alleged injury in fact based on  
 16 violations of the Fair Debt Collections Practices Act (“FDCPA”). The Eleventh Circuit noted that  
 17 the FDCPA “creates a private right of action, which [the plaintiff] seeks to enforce.” *Id.* at \*3.  
 18 The Eleventh Circuit further noted that “Congress provided [the plaintiff] with a substantive right  
 19 to receive certain disclosures and [the plaintiff] has alleged that [the defendant] violated that  
 20 substantive right.” *Id.* at \*3 n.2. Thus, although the plaintiff’s injury—not receiving disclosures  
 21 to which the plaintiff was entitled under the FDCPA—“may not have resulted in tangible  
 22 economic or physical harm that courts often expect,” the injury was sufficiently “concrete” for  
 23 Article III standing. *Id.* at \*3.

24 Similarly, in *Thomas v. FTS USA, LLC*, — F. Supp. 3d —, 2016 WL 3653878, (E.D. Va.  
 25 June 30, 2016), the Eastern District of Virginia District Court held that the plaintiff’s allegations  
 26 of Fair Credit Reporting Act (“FCRA”) violations established Article III standing. First, the court  
 27 found that “it was Congress’ judgment . . . to afford consumers rights to information and privacy,”

1 and the FCRA provisions violated “are clearly substantive, and neither technical nor procedural.”  
2 *Id.* at \*7–8. Next, the court noted that “Congress permitted consumers to sue to redress a breach  
3 of the substantive rights set forth in the foregoing subsections and, if successful, to be awarded  
4 actual, statutory, and punitive damages, as applicable.” *Id.* Because the plaintiff received a  
5 disclosure from the defendant that did not meet the substantive requirements of FCRA, and had  
6 the right to sue based on that FCRA violation, the plaintiff alleged a concrete injury. *Id.* at \*10;  
7 *Prindle v. Carrington Mortg. Servs., LLC*, 2016 WL 4369424, \*8 (M.D. Fla. Aug. 16, 2016)  
8 (holding that plaintiff sufficiently alleged standing when Congress provided a statutory,  
9 substantive right and a private right of action, “without regard to whether a consumer experienced  
10 a more tangible ‘harm’—such as economic loss—resulting from the conduct”).

11 Likewise, in *Cour v. Life360, Inc.*, 2016 WL 4039279, at \*2 (N.D. Cal. July 28, 2016),  
12 Judge Thelton E. Henderson of this district held that the plaintiff sufficiently alleged standing  
13 based on violations of the Telephone Consumer Protection Act (“TCPA”). The plaintiff alleged  
14 that the plaintiff received one or more text messages from the defendant in violation of the TCPA.  
15 *Id.* at \*1. Judge Henderson noted that the plaintiff “has not simply alleged a procedural violation;  
16 instead, he relies on an allegation that he was harmed because [the defendant] invaded his  
17 privacy.” *Id.* at \*2. Accordingly, Judge Henderson found that the plaintiff alleged concrete injury  
18 based on the TCPA violations. *Id.*

19 Similar to Judge Henderson, many courts since *Spokeo* have placed dispositive weight on  
20 whether a plaintiff alleges the violation of a substantive, rather than procedural, statutory right. If  
21 the right created by statute is substantive, courts have generally found that Congress permissibly  
22 “elevated [the harm recognized by the statute] to the status of legally cognizable injuries,” and  
23 thus that a plaintiff alleging violation of a substantive statutory right has Article III standing. *See*  
24 *e.g., Guarisma v. Microsoft Corp.*, — F. Supp. 3d —, 2016 WL 4017196, at \*3 (S.D. Fla. July 26,  
25 2016) (“The Supreme Court recognized where Congress has endowed plaintiffs with a *substantive*  
26 legal right, as opposed to creating a procedural requirement, the plaintiffs may sue to enforce such

1 a right without establishing additional harm.”); *Larson v. Trans Union, LLC*, — F. Supp. 3d —,  
 2 2016 WL 4367253, at \*3 (N.D. Cal. Aug. 11, 2016) (finding plaintiff adequately alleged standing  
 3 when plaintiff alleged an “informational” injury rather than a “bare procedural violation”); *Booth*  
 4 *v. Appstack, Inc.*, 2016 WL 3030256, at \*5 (W.D. Wash. May 25, 2016) (injury in fact satisfied  
 5 when the alleged injury was substantive, not procedural); *see also Jamison v. Bank of Am., N.A.*,  
 6 — F. Supp. 3d —, 2016 WL 3653456, at \*4 (E.D. Cal. July 7, 2016) (plaintiff did not have  
 7 standing when plaintiff made only conclusory allegations of harm, and alleged a procedural  
 8 statutory violation).

9 In the instant case, each of the three factors weighs in favor of finding concrete injury  
 10 based on Google’s alleged violations of the Wiretap Act and CIPA. First, there is no dispute that  
 11 both the Wiretap Act and CIPA create a private right of action for individuals in Plaintiff’s  
 12 position. The Wiretap Act provides that “any person” whose electronic communication is  
 13 “intercepted, disclosed, or intentionally used” in violation of the Act may bring suit against the  
 14 entity which engaged in that violation. 18 U.S.C. § 2520(a). CIPA likewise provides a private  
 15 cause of action. Specifically, CIPA provides that “[a]ny person who has been injured by a  
 16 violation of this chapter may bring an action against the person who committed the violation.”  
 17 Cal. Penal Code § 637.2(a).

18 Second, neither the Wiretap Act nor CIPA require a showing of actual harm. Under the  
 19 Wiretap Act, plaintiff may recover *either* actual damages, statutory damages, or injunctive relief.  
 20 18 U.S.C. § 2520(b), (c)(2). Likewise, CIPA provides that a plaintiff may recover statutory  
 21 damages or “[t]hree times the amount of actual damages, *if any*, sustained by the plaintiff.” Cal.  
 22 Penal Code § 637.2 (emphasis added). As the California Court of Appeal has stated, “Section  
 23 637.2 is fairly read as establishing that no violation of [CIPA] is to go unpunished. Any invasion  
 24 of privacy involves an affront to human dignity . . . . The right to recover this statutory minimum  
 25 accrue[s] at the moment the Privacy Act [CIPA] was violated.” *Friddle v. Epstein*, 16 Cal. App.  
 26 4th 1649, 1660–61 (1993).

1 Third, both the Wiretap Act and CIPA create substantive rights to privacy in one's  
2 communications. *See* 18 U.S.C. § 2511(1)(a); Cal. Penal Code § 631. By contrast, in *Spokeo* the  
3 defendant allegedly violated the FCRA, which requires credit reporting agencies to “follow  
4 reasonable procedures to assure maximum possible accuracy of” consumer reports. 136 S. Ct. at  
5 1545 (quoting 15 U.S.C. § 1681e(b)). The U.S. Supreme Court expressed no opinion as to  
6 whether this procedural FCRA violation constituted a “concrete injury,” but did note that “[i]t is  
7 difficult to imagine how the dissemination of an incorrect zip code [under the FCRA], without  
8 more, could work any concrete harm.” *Id.* at 1550. Thus, the U.S. Supreme Court held that a  
9 “bare procedural violation, divorced from any concrete harm” does not establish concrete injury.  
10 *Id.* at 1549. Here, Plaintiff alleges not a “bare procedural violation.” Instead, Plaintiff alleges that  
11 Google unlawfully intercepted, scanned, and analyzed Plaintiff’s communications in violation of  
12 the Wiretap Act and CIPA.

13 In sum, three aspects of the Wiretap Act and CIPA—the existence of a private right of  
14 action, the availability of statutory damages, and the creation of a substantive private right—  
15 support finding that both Congress and the California Legislature intended to “grant[] persons in  
16 [Plaintiff’s] position a right to judicial relief” without additional allegations of injury. *Edwards*,  
17 610 F.3d at 517; *see also Bona Fide Conglomerate, Inc. v. SourceAmerica*, 2016 WL 3543699, at  
18 \*7–8 (S.D. Cal. June 29, 2016) (violations of CIPA are sufficiently concrete to constitute injury in  
19 fact). Thus, the judgment of Congress and the California Legislature in creating enforceable,  
20 substantive legal rights through the Wiretap Act and CIPA supports finding that Plaintiff has  
21 alleged concrete injury based on the violation of those rights.

22 The Court notes that, before *Spokeo*, courts in this district consistently reached the same  
23 conclusion. *See Gmail*, 2013 WL 5423918, at \*17 (“[T]he allegation of a violation of CIPA, like  
24 an allegation of the violation of the Wiretap Act, is sufficient to confer standing without any  
25 independent allegation of injury.”); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1055  
26 (N.D. Cal. 2012) (“[A] violation of the Wiretap Act . . . may serve as a concrete injury for the  
27



1 purposes of Article III injury analysis.”); *In re Google Inc. Privacy Litig.*, 2013 WL 6248499, at  
 2 \*9 (N.D. Cal. Dec. 3, 2013) (“Courts have recognized that . . . alleged violations of the Wiretap  
 3 Act or the Stored Communications Act are sufficient to establish Article III injury. These statutes  
 4 grant persons in Plaintiffs’ position a right to relief and thus Plaintiffs have standing for these  
 5 claims.” (footnote omitted)); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal.  
 6 2011) (finding that where the plaintiffs alleged that their communications had been intercepted in  
 7 violation of the Wiretap Act, plaintiffs “alleged facts sufficient to establish that they have suffered  
 8 the injury required for standing under Article III”).

9 Google raises one additional counterargument as to CIPA. Google argues that state  
 10 statutes like CIPA can not confer Article III standing. Google Supp. Br. at 4 n.4; Google Supp.  
 11 Reply at 3 n.2. However, *Spokeo* said nothing about the ability of state legislatures to create rights  
 12 sufficient to confer Article III standing. In the absence of governing U.S. Supreme Court  
 13 precedent, the Ninth Circuit has held that “state law can create interests that support standing in  
 14 federal courts” and “[s]tate statutes constitute state law that can create such interests.” *Cantrell v.*  
 15 *City of Long Beach*, 241 F.3d 674, 684 (9th Cir. 2001). As the Ninth Circuit has explained, state  
 16 law must be able to support Article III standing, or else “there would not be Article III standing in  
 17 most diversity cases, including run-of-the-mill contract and property disputes.” *Id.* Thus, under  
 18 Ninth Circuit law, violations of CIPA may confer standing even though CIPA is a state statute.

19 The two Ninth Circuit cases cited by Google do not compel a contrary finding. The  
 20 plaintiffs in those two cases lacked standing because they sued as private attorneys general and  
 21 were not claiming that they themselves had suffered a concrete injury. *See Lee v. Am. Nat’l Ins.*  
 22 *Co.*, 260 F.3d 997, 1001–02 (9th Cir. 2001) (finding no Article III standing when the plaintiff  
 23 “suffered no individualized injury as a result of the defendant’s challenged conduct”); *Fiedler v.*  
 24 *Clark*, 714 F.2d 77, 79–80 (9th Cir. 1983) (rejecting Article III standing when the plaintiff claimed  
 25 to be “suing as a private Attorney General on behalf of citizens of Hawaii rather than as a private  
 26 citizen”). By contrast, Plaintiff seeks to recover for the alleged interception of Plaintiff’s own  
 27

1 email in violation of Plaintiff's substantive rights under CIPA.<sup>2</sup> Accordingly, the Court finds that  
 2 Plaintiff may allege standing based on violations of CIPA. *See Bona Fide Conglomerate*, 2016  
 3 WL 3543699, at \*7–8 (finding, after *Spokeo*, that plaintiff sufficiently alleged injury in fact based  
 4 on alleged violations of CIPA).

5 In sum, the Court concludes that the judgment of Congress and the California Legislature  
 6 indicate that the alleged violations of Plaintiff's statutory rights under the Wiretap Act and CIPA  
 7 constitute concrete injury in fact. This conclusion is supported by the historical practice of courts  
 8 recognizing that the unauthorized interception of communication constitutes cognizable injury.  
 9 The Court DENIES Google's motion to dismiss based on lack of standing under *Spokeo*.

### 10 **B. Injunctive Relief**

11 Having determined that Plaintiff sufficiently alleges concrete injury in fact, the Court turns  
 12 to Google's challenge to Plaintiff's standing to seek injunctive relief. Plaintiff seeks two types of  
 13 injunctive relief under both the Wiretap Act and CIPA. First, Plaintiff seeks an order enjoining  
 14 Google from intercepting the content of Plaintiff's and the Class members' emails in the future in  
 15 violation of the Wiretap Act or CIPA. Compl. ¶¶ 54(b), 68(b). Second, Plaintiff asks the Court to  
 16 require Google to destroy all data created or otherwise obtained from illegally intercepted email.  
 17 *Id.* ¶¶ 54(c), 68(c). The Court addresses these two types of injunctive relief in turn.

18 As a preliminary matter, in the motion to dismiss Google challenges only Plaintiff's  
 19 standing to seek injunctive relief under the Wiretap Act, not under CIPA. However, this Court  
 20 must "sua sponte . . . examine jurisdictional issues such as standing." *Ervine v. Desert View Reg'l*  
 21 *Med. Ctr. Holdings, LLC*, 753 F.3d 862, 866 (9th Cir. 2014). Thus, the Court analyzes Plaintiff's  
 22 standing to seek injunctive relief under both the Wiretap Act and CIPA.

---

23  
 24 <sup>2</sup> Google also cites a district court from outside this circuit that held that violations of state statutes  
 25 do not confer Article III standing in the absence of a separate concrete injury. *Khan v. Children's*  
 26 *Nat'l Health Sys.*, — F. Supp. 3d —, 2016 WL 2946165, at \*7 (D. Md. May 19, 2016). However,  
 27 unlike *Khan*, Plaintiff here has alleged concrete injury. Moreover, *Khan* is not binding on this  
 Court, which must follow the Ninth Circuit's rule that state statutes "can create interests that  
 support standing in federal courts." *Cantrell*, 241 F.3d at 684.

1           **1. Legal Standard**

2           A plaintiff “must show standing with respect to each form of relief sought.” *Ellis v.*  
3 *Costco Wholesale Corp.*, 657 F.3d 970, 978 (9th Cir. 2011). To establish standing for prospective  
4 injunctive relief, a plaintiff may not rely solely on “[p]ast exposure to illegal conduct.” *O’Shea v.*  
5 *Littleton*, 414 U.S. 488, 495–96 (1974). Instead, a plaintiff must demonstrate “continuing, present  
6 adverse effects” from the defendant’s illegal conduct, *id.*, or that the plaintiff has suffered or is  
7 threatened with a concrete and particularized legal harm “coupled with ‘a sufficient likelihood that  
8 he will again be wronged in a similar way,’” *Bates*, 511 F.3d at 985 (quoting *City of L.A. v. Lyons*,  
9 461 U.S. 95, 111 (1983)); *see also Chapman v. Pier 1 Imports (U.S.) Inc.*, 631 F.3d 939, 946 (9th  
10 Cir. 2011) (en banc) (“[T]o establish standing to pursue injunctive relief . . . [a plaintiff] must  
11 demonstrate a real and immediate threat of repeated injury in the future.” (internal quotation marks  
12 omitted)). Finally, in a class action, a named plaintiff must show that he himself is subject to a  
13 likelihood of future injury. Allegations that a defendant’s conduct will subject unnamed class  
14 members to the alleged harm is insufficient to establish standing to seek injunctive relief on behalf  
15 of the class. *Hodgers-Durgin v. de la Vina*, 199 F.3d 1037, 1044–45 (9th Cir. 1999).

16           **2. Injunction Seeking to End Future Processing of Gmail**

17           First, Plaintiff requests an injunction “enjoining Google from continuing its practice of  
18 intercepting the content of Plaintiff’s and Class members’ emails in violation” of the Wiretap Act  
19 and CIPA. Compl. VII.D; *see also* ¶¶ 54(b), 68(b). To analyze whether Plaintiff has standing to  
20 seek this injunction, the Court must distinguish among the three types of Gmail services discussed  
21 in the complaint. As discussed in the factual background, “Gmail” encompasses a number of  
22 email delivery systems. Google offers “Google Apps for Education” for educational organizations  
23 and “Google Apps for Work” for businesses. *Id.* ¶ 1 n.1; *Gmail Class Cert.*, 2014 WL 1102660, at  
24 \*1. In addition, Google provides a free Gmail service for individual users, which allows any user  
25 to register for an “@gmail.com” email address. Compl. ¶ 1 n.1; *Gmail Class Cert.*, 2014 WL  
26 1102660, at \*1. As discussed below, Google treats Google Apps for Education differently from  
27

1 Gmail for individual users and Google Apps for Work for purposes of intercepting, scanning, and  
 2 analyzing email content. Because of this difference in Google’s practices, the Court first  
 3 addresses Plaintiff’s requested injunction as it relates to Google Apps for Education, then to Gmail  
 4 for individual users, and finally Google Apps for Work.

5 **a. Email Plaintiff May Exchange with Users of Google Apps for Education**

6 Plaintiff seeks to enjoin Google from intercepting, scanning, and analyzing, for purposes of  
 7 creating targeted advertising and user profiles, emails that Plaintiff sends to or receives from  
 8 Google Apps for Education users. However, Plaintiff admits that “in April 2014, Google ceased  
 9 intercepting, scanning, and cataloging the contents of emails it provides to its educational clients  
 10 via its Google Apps for Education product.” Opp. at 11. Moreover, Google has confirmed that  
 11 Google ceased intercepting and scanning, for advertising purposes, the contents of emails  
 12 processed via Google Apps for Education. *See Corley v. Google, Inc.*, 16-CV-00473-LHK, ECF  
 13 No. 73 at 17 (N.D. Cal.) (statement of Google) (noting that April 30, 2014 is “the last date of any  
 14 scanning for these edu plaintiffs. So in other words, the practice at issue stopped.”).<sup>3</sup>

15 In light of the above circumstances, it appears that there is no “real and immediate threat of  
 16 repeated injury in the future” and thus that Plaintiff lacks standing to enjoin Google from  
 17 intercepting, scanning, and analyzing emails that Plaintiff may exchange with Google Apps for  
 18 Education users. Accordingly, the Court GRANTS with prejudice Google’s motion to dismiss  
 19 Plaintiff’s claim for an injunction as it relates to Google Apps for Education.

20 **b. Email Plaintiff May Exchange with Users of Gmail for Individual Users**

21 Next, Plaintiff seeks to enjoin Google from intercepting, scanning, and analyzing, for  
 22 purposes of creating targeted advertising and user profiles, emails that Plaintiff may exchange with  
 23

---

24 <sup>3</sup> The Court takes judicial notice of the transcript of the April 20, 2016 case management  
 25 conference in *Corley*. In that case, also related to *Gmail*, the plaintiffs are users of Google Apps  
 26 for Education who allege that Google unlawfully intercepted and scanned their email for  
 27 advertising purposes and without consent. No. 16-CV-00473, ECF No. 19. Lawyers representing  
 Plaintiff and Google in the instant case also represent the respective parties in *Corley*. Moreover,  
 the Court may take judicial notice of public court records. *See Lee*, 250 F.3d at 688.

1 users of Gmail for individual users. Google argues that Plaintiff can not seek this injunctive relief  
2 because users of Gmail for individual users consent to the alleged interception, scanning, and  
3 analysis of email.

4 To establish a consent defense under CIPA, both parties—the sender and the recipient of  
5 the communication—must consent to the alleged interception. Cal. Penal Code § 631(a)  
6 (prohibiting interceptions done “without the consent of all parties to the communication, or in any  
7 unauthorized manner”); *see also Gmail*, 2013 WL 5423918, at \*19. By contrast, under the  
8 Wiretap Act, the consent of one party to the interception of the communication is a complete  
9 defense to liability. 18 U.S.C. § 2511(2)(d) (“It shall not be unlawful . . . to intercept a wire, oral,  
10 or electronic communication . . . where one of the parties to the communication has given prior  
11 consent to such interception.”); *see also Murray v. Fin. Visions, Inc.*, 2008 WL 4850328, at \*4 (D.  
12 Ariz. Nov. 7, 2008). If Google establishes a consent defense as to one party under the Wiretap Act  
13 or both parties under CIPA, Plaintiff lacks standing to enjoin Google’s future interception,  
14 scanning, and analysis of email because Plaintiff would not be under “real and immediate threat of  
15 repeated injury in the future.” *See Chapman*, 631 F.3d at 946 (internal quotation marks omitted).

16 As to consent under CIPA, Google does not contend that non-Gmail users like Plaintiff  
17 consent to the alleged interception, scanning, and analysis of email for purposes of creating  
18 targeted advertising and user profiles. In the complaint, Plaintiff alleges that “Google has not  
19 obtained any consent from non-Gmail users” and that Plaintiff “has never consented to having his  
20 emails intercepted and scanned by Google for the purpose of acquiring and cataloging their  
21 message content.” Compl. ¶¶ 3, 8. Accordingly, Google does not establish a consent defense  
22 under CIPA, which requires consent from both parties to a communication. *See* Cal. Penal Code  
23 § 631(a).

24 As to consent under the Wiretap Act, Google contends that users of Gmail consent to the  
25 alleged interception, scanning, and analysis of their email for purposes of creating targeted  
26 advertising and user profiles. Such one-party consent would be a complete defense to liability  
27

United States District Court  
Northern District of California

1 under the Wiretap Act. *See* 18 U.S.C. § 2511(2)(d). To demonstrate consent, Google relies on the  
2 2014 TOS and Privacy Policies. As discussed above, Google altered its Terms of Service on April  
3 14, 2014 and Privacy Policy on December 19, 2014, after this Court held that the earlier versions  
4 of these agreements did not establish consent to the interceptions alleged in *Gmail*. According to  
5 Google, the updated 2014 TOS and Privacy Policies sufficiently disclose Google’s interception,  
6 scanning, and analysis practices to establish consent. Plaintiff counters that (i) there is no  
7 evidence that users of Gmail for individual users are notified of or otherwise agree to Google’s  
8 modified Terms of Service or Privacy Policies; (ii) Google’s disclosures are inadequate to  
9 demonstrate consent as a matter of law; and (iii) even if Google’s 2014 TOS and Privacy Policies  
10 establish consent, Plaintiff is still at risk of future injury because Google may alter its policies at  
11 any time. The Court addresses Plaintiff’s arguments respectively.

12 (i) **Enforceability of the 2014 TOS**

13 In *Gmail*, this Court described the earlier versions of the Terms of Service and Privacy  
14 Policies as “legal agreements.” *Gmail*, 2013 WL 5423918, at \*2. The Court found that users of  
15 the individual Gmail service “were required to agree” to the Terms of Service in order to use  
16 Gmail. *Id.* at \*2, \*13–14; *see also Corley v. Google, Inc.*, — F.R.D. —, 2016 WL 4411820, at \*1  
17 (N.D. Cal. Aug. 19, 2016). Additionally, the Terms of Service analyzed in *Gmail* provided that  
18 amendments to the Terms of Service are implemented by posting to the website. Specifically, the  
19 Terms of Service analyzed in *Gmail* stated, “You should look at the terms regularly. We’ll post  
20 notice of modifications to these terms on this page. . . . If you do not agree to the modified terms  
21 for a Service, you should discontinue your use of that Service.” *See* No. 13-MD-02439, ECF No.  
22 46-6 (Terms of Service Effective March 1, 2012).

23 Applying these principles to the instant case, users of the individual Gmail service agreed  
24 to the 2014 TOS upon its posting. *See MySpace, Inc. v. The Globe.com, Inc.*, 2007 WL 1686966,  
25 at \*10 (C.D. Cal. Feb. 27, 2007) (holding that the plaintiff and the defendant were bound by future  
26 versions of the defendant’s terms of service when the terms of service provided that modifications  
27

1 were effective upon posting); *see also Rudgayzer v. Google, Inc.*, 986 F. Supp. 2d 151, 154 n.1  
 2 (E.D.N.Y. 2013) (noting that plaintiffs consented to Google’s terms of service because the earlier  
 3 terms of service provide that a user would be bound by future changes in its terms).

4 **(ii) Consent Established by the 2014 TOS**

5 Because users of the individual Gmail service agree to the 2014 TOS, the Court next  
 6 addresses whether the 2014 TOS sufficiently establishes user consent by notifying Gmail users of  
 7 Google’s alleged conduct. In the instant case, Plaintiff alleges that Google intercepts, scans, and  
 8 analyzes emails that Plaintiff sends to or receives from Gmail users, so that Google may create  
 9 targeted advertising and user profiles for Gmail and non-Gmail users. Compl. ¶¶ 1, 8, 21. Thus,  
 10 the Court evaluates whether the 2014 TOS adequately notifies the reasonable user of Gmail that:  
 11 (1) Google intercepts, scans, and analyzes, (2) a Gmail user’s incoming and outgoing email  
 12 communications with non-Gmail users, (3) to create targeted advertising and user profiles, (4) for  
 13 Gmail and non-Gmail users.

14 Under the Wiretap Act, “the question of express consent is usually a question of fact,  
 15 where a fact-finder needs to interpret the express terms of any agreements to determine whether  
 16 these agreements adequately notify individuals regarding the interceptions.” *Gmail Class Cert.*,  
 17 2014 WL 1102660, at \*15 (citing *Murray*, 2008 WL 4850328, at \*4). In addition, consent is “not  
 18 an all-or-nothing proposition.” *Gmail*, 2013 WL 5423918, at \*12; *see also Watkins v. L.M. Berry*  
 19 *& Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (“[C]onsent within the meaning of section 2511(2)(d)  
 20 . . . can be limited. It is the task of the trier of fact to determine the scope of the consent and to  
 21 decide whether and to what extent the interception exceeded that consent.”). In other words, “[a]  
 22 party may consent to the interception of only part of a communication or to the interception of  
 23 only a subset of its communications.” *Yahoo Mail*, 7 F. Supp. 3d at 1028 (quoting *In re*  
 24 *Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003)). Furthermore, as “the party seeking the benefit  
 25 of the exception,” it is Google’s burden to prove consent. *Id.* This Court applies a reasonable user  
 26 standard to determine consent under the Wiretap Act. *See Perkins v. LinkedIn Corp.*, 2014 WL

1 2751053, at \*14 (N.D. Cal. June 12, 2014); *Gmail*, 2013 WL 5423918, at \*14.

2 With these principles in mind, the Court first addresses whether Google sufficiently  
3 discloses the interception, scanning, and analysis of email for purposes of creating targeted  
4 advertising for non-Gmail users. The 2014 TOS provides:

5 Our automated systems analyze your content (including emails) to provide you  
6 personally relevant product features, such as customized search results, tailored  
7 advertising, and spam and malware detection. This analysis occurs as the content is  
8 sent, received, and when it is stored.

9 2014 TOS at “Your Content in our Services.” Notably, the 2014 TOS makes no mention of non-  
10 Gmail users. By indicating that Google provides “you” (the Gmail user reading the 2014 TOS)  
11 with targeted advertising, the 2014 TOS could mislead Gmail users into believing that emails are  
12 intercepted to create targeted advertising only for the Gmail user, not for non-Gmail users.<sup>4</sup>

13 Specifically, the 2014 TOS states that Google analyzes “*your* content (including emails) to  
14 provide *you* personally relevant product features, such as . . . tailored advertising.” *Id.* (emphases  
15 added); *see also Watkins*, 704 F.2d at 582 (“[C]onsent within the meaning of section 2511(2)(d) is  
16 not necessarily an all or nothing proposition; it can be limited.”); *Backhaut v. Apple, Inc.*, 74 F.  
17 Supp. 3d 1033, 1045–46 (N.D. Cal. 2014) (holding that consent to the interception of  
18 communications for one purpose does not provide consent for other, undisclosed purposes).

19 Moreover, Google claims that the disclosure of Google’s targeted advertising practices  
20 necessarily discloses Google’s creation of user profiles because Plaintiff alleges that user profiles  
21 are used to create targeted advertising. Mot. at 7. The Court need not determine the merits of  
22 Google’s argument.<sup>5</sup> As discussed above, Google has not shown that Gmail users consent to the

23 <sup>4</sup> Google argues that there are “no meaningful distinctions” between Google’s 2014 TOS and the  
24 disclosures in *Yahoo Mail*, which this Court held established consent for Defendant Yahoo’s email  
25 scanning practices. Reply at 5. However, Yahoo’s terms of service expressly mentioned non-  
26 Yahoo users: “If you [Yahoo user] consent to this ATOS and communicate with *non-Yahoo users*  
27 *using the Services [Yahoo Mail], you are responsible for notifying those users about this feature.*”  
*Yahoo Mail*, 7 F. Supp. 3d at 1029.

<sup>5</sup> The Court notes that whether “tailored advertising” in the 2014 TOS and December 19, 2014  
Privacy Policy refers to advertising based solely on the content of a single email or advertising  
based on data aggregated about a Gmail user or non-Gmail user over time may be relevant to this  
inquiry.



1 interception, scanning, and analysis of email for purposes of creating targeted advertising for non-  
2 Gmail users. *See In re Pharmatrak, Inc.*, 329 F.3d at 19 (noting that the burden is on the party  
3 claiming consent). Consequently, the 2014 TOS can not, and does not, establish Gmail users'  
4 consent to the interception, scanning, and analysis of email for purposes of creating targeted  
5 advertising and user profiles for both Gmail and non-Gmail users.

6 Similarly, Google's December 19, 2014 Privacy Policy, incorporated by reference into the  
7 2014 TOS, suffers from the same defect. The December 19, 2014 Privacy Policy makes no  
8 mention of non-Gmail users, and fails to disclose the fact that Google intercepts, scans, and  
9 analyzes email to create targeted advertising and user profiles for non-Gmail users. Therefore, the  
10 December 19, 2014 Privacy Policy can not, and does not establish consent to Google's alleged  
11 interception, scanning, and analysis practices.

12 Because Google has not established a consent defense, Plaintiff has alleged "real and  
13 immediate threat of repeated injury" from Google's alleged interception, scanning, and analysis  
14 practices.<sup>6</sup> *See Chapman*, 631 F.3d at 946. Accordingly, the Court DENIES Google's motion to  
15 dismiss Plaintiff's request for an injunction as to Gmail for individual users.

16 **c. Email Plaintiff May Exchange with Users of Google Apps for Work**

17 Lastly, the Court addresses Plaintiff's requested injunctive relief as it applies to Google  
18 Apps for Work. No party specifically addresses Google Apps for Work in the briefing on the  
19 instant motion. *See generally* Mot., Opp., Reply. Accordingly, Google fails to show that Google  
20 Apps for Work users consent to the alleged interception, scanning, and analysis of email, and thus  
21 Google's motion to dismiss is DENIED.

22 The denial, however, is without prejudice because the Court has learned that Google  
23 publicly represents that Google no longer intercepts, scans, and analyzes for advertising purposes  
24 emails transmitted via Google Apps for Work. *See FAQs for Google Apps users*, Google Apps for  
25

---

26 <sup>6</sup> Because Google fails to establish a consent defense, the Court need not reach Plaintiff's final  
27 argument that Plaintiff is still at risk of future injury because Google may alter its policies at any  
28 time.

1 Work, <https://apps.google.com/faq/security/> (last visited September 22, 2016) (“Unlike Google’s  
2 consumer offerings, which may show ads, we do not collect, scan or use your Google Apps data  
3 for advertising purposes . . . .”); *Privacy*, Google for Work Help,  
4 <https://support.google.com/work/answer/6056650?hl=en> (last visited September 22, 2016)  
5 (“Google does not collect or use data in Google Apps services for advertising purposes.”).  
6 Because this is a factual issue not developed on the record before the Court, the Court will discuss  
7 this issue with the parties at the September 28, 2016 case management conference.

### 8 **3. Injunction Seeking Destruction of Data**

9 As to Plaintiff’s second requested injunction, Plaintiff asks the Court to require Google to  
10 “destroy all data created or otherwise obtained” from Google’s unlawful interception of email.  
11 Compl. ¶¶ 54(c), 68(c).<sup>7</sup> Under the Wiretap Act, Plaintiff limits the requested injunctive relief to  
12 data created or obtained before December 19, 2014. *Id.* ¶ 68(c). Under CIPA, there is no time  
13 limitation on the requested injunctive relief. *Id.* ¶ 54(c). Plaintiff alleges that Google’s retention  
14 and use of unlawfully acquired data is an ongoing injury. *Opp.* at 5–6.

15 Google again challenges the requested injunction solely on the basis of standing. The  
16 merits and scope of the injunction are not before the Court. Specifically, Google contends that the  
17 consent given by Gmail users under Google’s 2014 TOS applies retroactively to all emails that  
18 remain in a Gmail user’s account, even to emails sent before the 2014 TOS was posted in April  
19 2014. *Mot.* at 7–8.

20 The Court is unpersuaded. First, the 2014 TOS itself provides that “[c]hanges [to the  
21 Terms of Service] will not apply retroactively.” Thus, any consent given under the 2014 TOS  
22 would not apply retroactively to the interception, scanning, and analysis of email before the 2014  
23

---

24 <sup>7</sup> Specifically, under CIPA, Plaintiff requests “Injunctive relief in the form of, *inter alia*, an order  
25 requiring Google to destroy all data created or otherwise obtained from its illegal interception of  
26 emails sent or received by Plaintiff or any Class member.” Compl. ¶ 54(c). Under the Wiretap  
27 Act, Plaintiff requests “Injunctive relief in the form of, *inter alia*, an order requiring Google to  
destroy all data created or otherwise obtained from the interceptions of emails sent or received by  
Plaintiff and Class members, or any of them, before December 19, 2014.” *Id.* ¶ 68(c).

United States District Court  
Northern District of California

1 TOS was in place. Moreover, as discussed above, neither Google’s 2014 TOS or December 19,  
2 2014 Privacy Policy establish consent to Google’s alleged interception, scanning, and analysis  
3 practices as to non-Gmail users. Accordingly, the Court DENIES Google’s motion to dismiss  
4 Plaintiff’s second requested injunction.

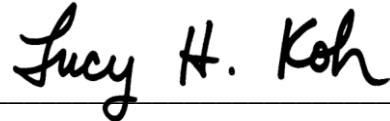
5 **V. CONCLUSION**

6 For the foregoing reasons, the Court GRANTS IN PART and DENIES IN PART Google’s  
7 motion to dismiss based on lack of standing.

8 **IT IS SO ORDERED.**

9

10 Dated: September 23, 2016



11 \_\_\_\_\_  
12 LUCY H. KOH  
13 United States District Judge

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28