

1 COOLEY LLP  
2 MICHAEL G. RHODES (116127) (rhodesmg@cooley.com)  
3 WHITTY SOMVICHIAN (194463) (wsomvichian@cooley.com)  
4 KYLE C. WONG (224021) (kwong@cooley.com)  
5 101 California Street, 5th Floor  
6 San Francisco, CA 94111-5800  
7 Telephone: (415) 693-2000  
8 Facsimile: (415) 693-2222

9 Attorneys for Defendant  
10 GOOGLE INC.

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**

IN RE GOOGLE INC. GMAIL LITIGATION

THIS DOCUMENT RELATES TO:  
ALL ACTIONS

Case No. 5:13-md-02430-LHK

**DEFENDANT GOOGLE INC.'S MOTION TO  
DISMISS PLAINTIFFS' CONSOLIDATED  
INDIVIDUAL AND CLASS ACTION  
COMPLAINT; MEMORANDUM OF POINTS  
AND AUTHORITIES IN SUPPORT THEREOF**

**F.R.C.P. 12(b)(1), 12(b)(6)**

Date: September 5, 2013  
Time: 1:30 p.m.  
Judge: Hon. Lucy H. Koh  
Courtroom: 8

Trial Date: Not yet set

## TABLE OF CONTENTS

	Page
NOTICE OF MOTION AND MOTION TO DISMISS .....	1
STATEMENT OF ISSUES TO BE DECIDED .....	1
I. INTRODUCTION .....	2
II. STATEMENT OF FACTS .....	3
A. Gmail.....	3
B. Google Apps .....	4
C. Google’s Terms and Disclosures .....	4
D. Plaintiffs, Their Consent to Automated Processing, And Their Claims .....	5
III. APPLICABLE STANDARDS .....	6
IV. ARGUMENT .....	6
A. The Wiretapping Claims Fail Because the Alleged Scanning Practices Are Part of Google’s Ordinary Course of Business as an ECS Provider.....	6
1. The Wiretap Statutes Exempt ECS Providers from Liability .....	6
2. Courts Have Consistently Dismissed Claims Against ECS Providers Involving Circumstances Similar to Those Alleged Here .....	8
3. Plaintiffs’ Efforts to Plead around the “Ordinary Course of Business” Exemption Fail.....	10
4. Plaintiffs’ Theory of Liability Would Lead to Absurd Results.....	12
5. The Pennsylvania Wiretap Statute Applies Only to the Senders, Not the Recipients of a Communication .....	13
B. Plaintiffs’ Claims Also Fail Under the Consent Defenses of the Wiretap Statutes at Issue .....	13
1. Gmail Plaintiffs Expressly Consent to Automated Scanning, Precluding Any Claim under ECPA .....	14
2. Minors like Plaintiff J.K Cannot Avoid the Terms They Agreed to.....	16
3. Plaintiffs Fread and Carrillo Cannot Avoid Their Express Consent by Claiming They Were Pressured into Using Gmail.....	17
4. The Non-Gmail Plaintiffs Also Impliedly Consent to the Automated Processing of Their Messages.....	19
C. The CIPA Claim Also Fails as a Matter of Law for Multiple Reasons .....	21
1. CIPA Does Not Apply to Email Communications .....	21
2. Plaintiffs Also Have no Article III Standing to Pursue a CIPA claim .....	23
3. Plaintiffs Also Fail to Allege Any Connection with California.....	24
D. The Section 632 Claim Fails for Additional Reasons.....	25
1. Plaintiffs Allege no Facts to Show that Their Emails Were “Confidential Communications” within the Meaning of the Statute .....	25

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

**TABLE OF CONTENTS**  
**(continued)**

	<b>Page</b>
2. Federal Law Preempts Any Claim that an ECS Provider’s Operations Constitute an Illegal “Recording” under Section 632 .....	26
E. The CIPA Claim Should Also Be Dismissed Under Choice Of Law Principles.....	27
V. CONCLUSION .....	30

# TABLE OF AUTHORITIES

## Page

### CASES

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	6
<i>Banks v. Nissan N. Am., Inc.</i> , No. 11-cv-2022, 2012 U.S. Dist. LEXIS 37754 (N.D. Cal. Mar. 20, 2012).....	28
<i>Bayview Hunters Point Cmty. Advocates v. Metro. Transp. Comm’n</i> , 366 F.3d 692 (9th Cir. 2004).....	12
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	6
<i>Berg v. Traylor</i> , 148 Cal. App. 4th 809 (2007) .....	16
<i>Bohach v. City of Reno</i> , 932 F. Supp. 1232 (D. Nev. 1996) .....	7
<i>Borninski v. Williamson</i> , No. 02-cv-1014, 2005 WL 1206872 (N.D. Tex. May 17, 2005) .....	16
<i>Bunnell v. MPAA</i> , 567 F. Supp. 2d 1148 (C.D. Cal. 2007) .....	27
<i>Cavines v. Horizon Cmt. Learning Ctr., Inc.</i> , 590 F.3d 806 (9th Cir. 2010).....	6
<i>City of Richmond v. S. Bell Tel. &amp; Tel. Co.</i> , 174 U.S. 761 (1899).....	23
<i>Commonwealth v. Blystone</i> , 549 A.2d 81 (Pa. 1988) .....	5
<i>Commonwealth v. Maccini</i> , No. 06-cv-0873, 2007 WL 1203560 (Mass. Super. Ct. Apr. 23, 2007).....	20
<i>Commonwealth v. Proetto</i> , 771 A.2d 823 (Pa. Super. Ct. 2001), <i>aff’d</i> , 837 A.2d 1163 (Pa. 2003).....	20
<i>Deacon v. Pandora Media, Inc.</i> , 901 F. Supp. 2d 1166 (N.D. Cal. 2012) .....	23
<i>Deering v. CenturyTel, Inc.</i> , No. 10-cv-0063, 2011 WL 1842859 (D. Mont. May 16, 2011).....	16

**TABLE OF AUTHORITIES**  
(continued)

		<b>Page</b>
3	<i>Deibler v. State</i> ,	
4	776 A.2d 657 (Md. Ct. App. 2001) .....	5
5	<i>Diamond v Google Inc.</i> ,	
6	No. CIV-1202715 (Cal. Sup. Ct. 2012) .....	22
7	<i>In re DoubleClick Privacy Litig.</i> ,	
8	154 F. Supp. 2d 497 (S.D.N.Y. 2001) .....	7, 19
9	<i>Faulkner v. ADT Servs., Inc.</i> ,	
10	706 F.3d 1017 (9th Cir. 2013) .....	26
11	<i>Fraser v. Nationwide Mut. Ins. Co.</i> ,	
12	352 F.3d 107 (3d Cir. 2003) .....	7
13	<i>Frezza v. Google, Inc.</i> ,	
14	No. 12-cv-0237, 2013 WL 1736788 (N.D. Cal. Apr. 22, 2013) .....	27
15	<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.</i> ,	
16	528 U.S. 167 (2000) .....	24
17	<i>In re Google, Inc. Privacy Policy Litig.</i> ,	
18	No. 12-cv-1382 PSG, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012) .....	8, 9, 10, 11
19	<i>In re Google, Inc. Street View Elec. Commc'ns Litig.</i> ,	
20	794 F. Supp. 2d 1067 (N.D. Cal. 2011) .....	27
21	<i>Hall v. EarthLink Network, Inc.</i> ,	
22	396 F.3d 500 (2d Cir. 2005) .....	6, 8, 11
23	<i>Healy v. Beer Inst., Inc.</i> ,	
24	491 U.S. 324 (1989) .....	29
25	<i>Hibbs v. Winn</i> ,	
26	542 U.S. 88 (2004) .....	12
27	<i>Ideal Aerosmith, Inc. v. Acutronic USA, Inc.</i> ,	
28	No. 07-cv-1029, 2007 WL 4394447 (E.D. Pa Dec. 13, 2007) .....	10
	<i>In re iPhone Application Litig.</i> ,	
	No. 11-md-2250, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) .....	24, 25
	<i>Kearney v. Salomon Smith Barney, Inc.</i> ,	
	39 Cal. 4th 95 (2006) .....	25, 29

**TABLE OF AUTHORITIES**  
**(continued)**

	<b>Page</b>
<i>Kirch v. Embarq Mgmt. Co.</i> , 702 F.3d 1245 (10th Cir. 2012).....	8, 9, 10
<i>Kirch v. Embarq Mgmt. Co.</i> , No. 10-cv-2047, 2011 WL 3651359 (D. Kan. Aug. 19, 2011) .....	16
<i>Kline v. Sec. Guards, Inc.</i> , 386 F.3d 246 (3d Cir. 2004).....	13
<i>Klump v. Nazareth Area Sch. Dist.</i> , 425 F. Supp. 2d 622 (E.D. Pa. 2006) .....	13
<i>Kopko v. Miller</i> , 892 A.2d 766 (Pa. 2006) .....	5
<i>LaCourt v Specific Media, Inc.</i> , No. 10-cv-1256, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) .....	25
<i>In re Marriage of Baltins</i> , 212 Cal. App. 3d 66 (1989).....	18
<i>Mazza v. Am. Honda Motor Co., Inc.</i> , 666 F.3d 581 (9th Cir. 2012).....	28, 29, 30
<i>Minotty v. Baudo</i> , 42 So.3d 824 (Fla. Dist. Ct. App. 2010) .....	5
<i>Montegna v. Yodle, Inc.</i> , No. 12-cv-0647, 2012 WL 3069969 (S.D. Cal. July 27, 2012) .....	26
<i>Mortensen v. Bresnan Commc'n, LLC</i> , No. 10-cv-0013, 2010 WL 5140454 (D. Mont. Dec. 13, 2010).....	16
<i>Penkava v. Yahoo!, Inc.</i> , No. 12-cv-3414 PSG LHK (N.D. Cal.) ECF No. 1.....	4
<i>People v. Chavez</i> , 44 Cal. App. 4th 1144 (1996) .....	22
<i>Pub. Util. Dist. No. 1 v. IDACORP, Inc.</i> , 379 F.3d 641 (9th Cir. 2004).....	27
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	19, 21

**TABLE OF AUTHORITIES**  
(continued)

		<b>Page</b>
3	<i>Smith v. Trusted Universal Standards in Elec. Transactions, Inc.</i> ,	
4	No. 09-cv-4567, 2011 WL 900096 (D.N.J. Mar. 15, 2011).....	14, 19, 21
5	<i>Standiford v. Standiford</i> ,	
6	598 A.2d 495 (Md. Ct. Spec. App. 1991) .....	5
7	<i>Stanislaus Food Prods. Co. v. USS-POSCO Indus.</i> ,	
8	782 F. Supp. 2d 1059 (E.D. Cal. 2011).....	6
9	<i>State v. Komisarjevsky</i> ,	
10	No. CR07241860, 2011 WL 1032111 (Conn. Super. Ct. Feb. 22, 2011).....	23
11	<i>State v. Lott</i> ,	
12	879 A.2d 1167 (N.H. 2005) .....	20
13	<i>State v. Roden</i> ,	
14	279 P.3d 461 (Wash. Ct. App. 2012) .....	20
15	<i>State v. Townsend</i> ,	
16	57 P.3d 255 (Wash. 2002).....	20
17	<i>Taylor v. Indus. Accident Comm’n</i> ,	
18	216 Cal. App. 2d 466 (1963).....	16
19	<i>Ting v. AT&amp;T</i> ,	
20	319 F.3d 1126 (9th Cir. 2003).....	27
21	<i>United States v. Van Poyck</i> ,	
22	77 F.3d 285 (9th Cir. 1996).....	14
23	<i>United States v. Verdin-Garcia</i> ,	
24	516 F.3d 884 (10th Cir. 2008).....	19
25	<i>In re Vistaprint Corp. Mktg. &amp; Sales Pracs. Litig.</i> ,	
26	No. 08-md-1994, 2009 WL 2884727 (S.D. Tex, Aug. 31, 2009), <i>aff’d</i> , 392 F. App’x	
27	327 (5th Cir. 2010).....	16
28	<i>Weiner v. ARS Nat’l Servs., Inc.</i> ,	
	887 F. Supp. 2d 1029 (S.D. Cal. 2012) .....	26
	<i>Zephyr v. Saxon Mortg. Servs., Inc.</i> ,	
	873 F. Supp. 2d 1223 (E.D. Cal. 2012).....	29

# TABLE OF AUTHORITIES

## (continued)

Page

### STATUTES

#### 18 Pa. C.S.

§ 5701.....	5
§ 5702.....	8
§ 5704(4).....	14
§ 5725.....	13
§§ 5741-43 .....	7

15 U.S.C. § 6502(d) .....	17, 18
---------------------------	--------

#### 18 U.S.C.

§ 2510.....	6, 11
§ 2511.....	14, 19
§ 2701.....	6, 7

Ala. Code 1975 § 13A-11-30.....	28
---------------------------------	----

Cal. Fam. Code § 6701(c) .....	16, 17
--------------------------------	--------

#### Cal. Penal Code

§ 629.....	23, 24
§ 630.....	6, 29
§ 631.....	6, 21, 22, 25
§ 632.....	<i>passim</i>
§ 637.2.....	24, 28

#### Fla. Stat.

§ 934.02.....	8
§ 934.03.....	5, 14
§§ 934.21-23 .....	7



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

**TABLE OF AUTHORITIES**  
**(continued)**

	<b>Page</b>
Md. Code, Cts. & Jud. Proc.	
§ 10-401 .....	7, 8
§ 10-402 .....	5, 7, 14
§ 10-410 .....	28
<b>OTHER AUTHORITIES</b>	
34 C.F.R. 99.31 .....	13
<i>Black’s Law Dictionary</i> (9th ed. 2009) .....	22
Restatement (Second) of Contracts § 175 (1981) .....	18

1 **NOTICE OF MOTION AND MOTION TO DISMISS**

2 PLEASE TAKE NOTICE that on September 5, 2013, at 1:30 p.m., defendant Google Inc.  
3 (“Google”) will and hereby does move to dismiss Plaintiffs’ Consolidated Individual and Class  
4 Action Complaint (the “Complaint”). Google’s Motion to Dismiss is made pursuant to Rules  
5 12(b)(1) and (6) of the Federal Rules of Civil Procedure, and is based on this Notice of Motion  
6 and Motion, the accompanying Memorandum of Points and Authorities and other pleadings in  
7 support of the Motion, and all pleadings on file in this matter, and upon such other matters as may  
8 be presented to the Court at the time of the hearing or otherwise.

9 **STATEMENT OF ISSUES TO BE DECIDED**

10 1. Have Plaintiffs stated a claim that the automated processing of email in Google’s  
11 Gmail service violates the Federal Wiretap Act, as amended by the Electronic Communications  
12 Privacy Act (“ECPA”), and its Florida, Maryland, and Pennsylvania state law analogues  
13 (collectively the “wiretap statutes”), where:

- 14 • The wiretap statutes exempt providers of an electronic communication service (an  
15 “ECS”) like Google from liability based on conduct in the ordinary course of business  
16 and the Complaint confirms that the alleged “interceptions” occur as part of Google’s  
17 normal processes in providing the Gmail service;  
18 • ECPA precludes liability where a single party to a communication consents to the  
19 alleged “interception,” and all Gmail users contractually agree to the scanning of email  
20 as part of using Google’s services;  
21 • The state wiretap statutes preclude liability where both parties to a communication  
22 consent, and case law holds that all users of email necessarily give implied consent to  
23 the automated processing of their emails;  
24 • The Pennsylvania wiretap statute applies only to the senders, not the recipients of, an  
25 electronic communication.

26 2. Have Plaintiffs stated a claim that Google’s automated processing of email violates  
27 the California Invasion of Privacy Act (“CIPA”), where:

- 28 • The express terms and legislative history of CIPA confirm that the statute excludes  
email;  
• The only Plaintiffs purporting to bring a CIPA claim are non-California residents who  
allege no connection with California;  
• CIPA allows a claim only for injured persons and Plaintiffs allege no harm of any kind  
from the automated processing of their emails.

1     **I.     INTRODUCTION.**

2           This case involves Plaintiffs’ effort to criminalize ordinary business practices that have  
3     been part of Google’s free Gmail service since it was introduced nearly a decade ago. While  
4     Plaintiffs are differently situated (some are Gmail users; others are non-Gmail users who  
5     exchange emails with Gmail users), their claims boil down to the same core allegation: that  
6     Google commits an illegal “interception” when it applies automated (non-human) scanning to  
7     emails involving Gmail users—even though the processes at issue are a standard and fully-  
8     disclosed part the Gmail service. This claim fails as matter of law for multiple reasons.

9           First, all of the federal and state wiretap laws at issue specifically exempt ECS providers  
10    from liability based on conduct in their ordinary course of business. These protections reflect the  
11    reality that ECS providers like Google *must* scan the emails sent to and from their systems as part  
12    of providing their services. While Plaintiffs go to great lengths to portray Google in a sinister  
13    light, the Complaint actually confirms that the automated processes at issue are Google’s ordinary  
14    business practices implemented as part of providing the free Gmail service to the public. This is  
15    fatal to Plaintiffs’ claims.

16          Second, the wiretap statutes also preclude liability where either a single party to the  
17    communication (for the federal statute) or both parties (for the state statutes) have expressly or  
18    impliedly consented to the practices at issue. Here, all Plaintiffs who are Gmail users consented  
19    to the automated scanning of their emails (including for purposes of delivering targeted  
20    advertising) in exchange for using the Gmail service, thus precluding any claim under federal  
21    law. Moreover, multiple courts have held that *all* email senders impliedly consent to the  
22    processing of their emails by virtue of the fact that email cannot be sent or delivered without  
23    some form of electronic processing. This combination of express and implied consent bars  
24    Plaintiffs’ claims in their entirety, under both the federal and state wiretap statutes.

25          Third, the CIPA claim brought by certain Plaintiffs is even farther afield than the  
26    wiretapping claims above because CIPA does not apply to emails *at all*, as confirmed by both the  
27    express terms and legislative history of the statute. In fact, the California Legislature specifically  
28    considered *and rejected* proposals to expand the statute to cover emails. And even if CIPA could

1 be interpreted to cover emails, both implied consent and choice of law rules would preclude the  
2 CIPA Plaintiffs from relying on the statute. As residents of Alabama and Maryland whose emails  
3 have no alleged connection to California, these Plaintiffs cannot invoke the protections of  
4 California law and bypass the laws of the states in which they reside simply because they want to  
5 avoid the requirements and limitations of their local laws.

6 Last, Plaintiffs' claims should be rejected because they would lead to anomalous results  
7 with far-ranging consequences beyond the allegations in the Complaint. Plaintiffs' theory—that  
8 any scanning of email content by ECS providers is illegal—would effectively criminalize routine  
9 practices that are an everyday aspect of using email. Indeed, Plaintiffs' effort to carve out spam  
10 filtering and virus detection from their claims underscores the fact that their theory of liability  
11 would *otherwise* encompass these common services that email users depend on. Notwithstanding  
12 these limited carve-outs, Plaintiffs' theory would still sweep up a host of common features that  
13 benefit consumers. For example, Plaintiffs' theory of liability would prevent ECS providers from  
14 providing features that allow users to sort their emails using automated filters or even to search  
15 their emails for specific words—because these features necessarily involve the scanning of email  
16 content and would thus be an illegal “interception” under Plaintiffs' theory. The Court should not  
17 allow the Complaint to proceed on this sweeping basis.

## 18 **II. STATEMENT OF FACTS.**

### 19 **A. Gmail.**

20 Gmail is one of the most popular web-based email services in the world with over 400  
21 million users. Like all email providers, Google applies automated systems for the delivery of  
22 email. As part of this processing, Google's automated systems scan email content to filter out  
23 spam, detect computer viruses, and provide various features, including functions that allow users  
24 to search their email messages, automatically sort incoming email, and others. These systems are  
25 also used to display advertisements targeted to email content, as Google has disclosed since the  
26 inception of Gmail nearly a decade ago. The revenues from these advertisements enable Google  
27 to provide the Gmail service for free to the public. Gmail's advertising-based business model is  
28 similar to that of other free email services offered by Yahoo, AOL, and Hotmail. Yahoo, the very

1 web-based email service one named Plaintiff uses, also generates revenue from scanning email  
2 content to deliver targeted advertising.<sup>1</sup> The processes related to Google’s automated scanning  
3 are completely automated and involve no human review.

4 **B. Google Apps.**

5 “Google Apps” is a suite of Google products that includes Gmail. Google Apps enables  
6 its users—which can include businesses, educational organizations, and Internet service providers  
7 (“ISPs”)—to provide email services to their employees, students, or customers.<sup>2</sup> These email  
8 services are operated by Gmail but can be customized in certain ways. Cable One, Inc. (“Cable  
9 One”) is an ISP and the Universities of Hawaii (“Hawaii”) and of the Pacific (“UoP”) are two  
10 educational institutions that provide email services to their users (including Plaintiffs Dunbar,  
11 Castillo, and Fread) through Google Apps. (Compl. ¶¶ 8, 14, 100, 101.)

12 **C. Google’s Terms and Disclosures.**

13 The Google Terms of Service (“TOS”) and Privacy Policy in effect during the majority of  
14 the class period required users of Gmail to agree that “advertisements may be targeted to the  
15 content of information stored on [Google’s] Services, queries made through [Google’s] Services  
16 or other information.”<sup>3</sup> (Declaration of Aaron Rothman (hereinafter “Rothman Declaration” or  
17 “Rothman Decl.”) ¶ 11, Exh. E at § 17.1.) The Privacy Policy has essentially stated throughout  
18 the class period that Google could use information from users to “[p]rovide, maintain, protect,  
19 and improve [its] services (including advertising services) and develop new services.” (*Id.* at  
20 ¶ 15, Exh. I; *see also id.* at ¶¶ 13-16, Exhs. G-J.)

21 In addition to these contractual terms, Google also provides a variety of disclosures  
22 throughout its website and within Gmail itself explaining that automated processing is applied to  
23 Gmail messages and that email content is scanned to deliver targeted ads. Several of these

---

24 <sup>1</sup> *See* Declaration of Kyle Wong (hereinafter “Wong Decl.”), Exh. AA. In fact, attorneys for  
25 Plaintiff Dunbar filed a class action against Yahoo in this district claiming nearly identical  
26 allegations as brought here. (Compl. §§ 9-15 *Penkava v. Yahoo!, Inc.*, No. 12-cv-3414 PSG LHK  
(N.D. Cal.) ECF No. 1.) The case was subsequently dismissed with prejudice while Yahoo’s  
27 motion to dismiss was pending. (*See* Wong Decl., Exh. PP.)

28 <sup>2</sup> *See, e.g.*, <http://www.google.com/enterprise/apps/education/> and  
<http://www.google.com/enterprise/apps/business/>.

<sup>3</sup> The TOS defined Google’s “Services” as “Google’s products, software, services and web sites,”  
including Gmail. (*See* Rothman Decl., Ex. F at §1.1.)

disclosures are detailed in the Rothman Declaration.

**D. Plaintiffs, Their Consent to Automated Processing, and Their Claims.**

Plaintiffs Dunbar, Fread, Carrillo, and J.K. (through A.K.) (collectively, “Gmail Plaintiffs”) are Gmail or Google Apps users. (Compl. ¶¶ 224, 233, 345, 248.) Plaintiff Dunbar has a Google Apps account through his ISP, Cable One. Plaintiffs Fread and Carrillo have used Google Apps accounts provided by the universities they attend (Hawaii and UoP). J.K. is a minor who uses a Gmail account. These Gmail Plaintiffs claim that Google violated ECPA, 18 U.S.C. §§ 2511(1)(a) and (1)(d), by unlawfully intercepting and using their electronic communications. (*Id.* ¶ 216.) Each of these Gmail Plaintiffs are bound by the TOS, Privacy Policy, or both.<sup>4</sup>

Plaintiffs Brinkman, Knowles, and Brent Scott are residents of Pennsylvania, Maryland, and Florida respectively. They allege that they used their non-Gmail email accounts to communicate with Gmail users. (Compl. ¶¶ 10, 12, 13.) Based on these communications, these Plaintiffs claim that Google violated the state wiretap laws of their respective home states, Fla. Stat. §§ 934.03 *et seq.*; Md. Code, Cts. & Jud. Proc. §§ 10-402 *et seq.*; 18 Pa. C.S. §§ 5701 *et seq.*, by unlawfully intercepting and using their electronic communications (Compl. ¶¶ 332-384.) Because these states’ wiretap laws are directly modeled on ECPA and are virtually identical to it in form and substance,<sup>5</sup> the claims of these Plaintiffs and the Gmail Plaintiffs (collectively, the “Wiretapping Plaintiffs”) are considered and analyzed together below.

---

<sup>4</sup> Plaintiff Dunbar concedes that he is bound by the Cable One Apps TOS and Google’s Privacy Policy. (Wong Decl., Exh. OO.) The relevant terms in the Cable One Apps TOS are virtually identical to, if not the same as, those terms in the Google TOS discussed above. (Rothman Decl. ¶ 7.) With respect to Plaintiffs Fread and Carrillo, as also discussed in the Rothman Declaration, the contracts between Google and Hawaii and UoP (i) incorporate the Privacy Policy, including its description of how Google processes data and (ii) require Hawaii and UoP to obtain the necessary consent from end users, like Fread and Carrillo, for Google to provide the Gmail service. (*Id.* ¶¶ 8 and 9, Exhs. C and D.) Plaintiff J.K. alleges that he created his Gmail account “via the ‘Create An Account’ link on Gmail’s homepage.” (Wong Decl., Exh. EE at ¶ 10.) As explained in the Rothman Declaration, a user who signs up in this manner must affirmatively agree to the TOS and Privacy Policy. (Rothman Decl. ¶ 6, Exh. A.) Moreover, at certain times during the class period, Google’s Create an Account web page explained that in “Gmail, you won’t see blinking banner ads. Instead, *we display ads you might find useful that are relevant to the content of your messages.*” (*Id.* (emphasis added).) As such, each named Plaintiff is bound by the TOS, Privacy Policy, or both.

<sup>5</sup> *See, e.g., Minotty v. Baudo*, 42 So. 3d 824 (Fla. Dist. Ct. App. 2010); *Deibler v. State*, 776 A.2d 657 (Md. Ct. App. 2001); *Kopko v. Miller*, 892 A.2d 766, 773 (Pa. 2006). As such, these statutes are to be construed in line with federal law under ECPA. *Minotty*, 42 So. 3d at 827; *Standiford v. Standiford*, 598 A.2d 495, 498 (Md. Ct. Spec. App. 1991); *Commonwealth v. Blystone*, 549 A.2d

1 Plaintiffs Brad Scott and Harrington, residents of Maryland and Alabama respectively,  
2 seek relief under California’s Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 630-632.  
3 These Plaintiffs (collectively, the “CIPA Plaintiffs”) have non-Gmail email accounts through  
4 which they exchanged emails with Gmail users. Plaintiffs Brinkman, Knowles, Brent Scott, Brad  
5 Scott, and Harrington are referred to collectively as the “non-Gmail Plaintiffs.”

6 While Plaintiffs seek to represent eight separate classes of Gmail and non-Gmail users  
7 under five causes of action, (Compl. ¶¶ 388-392), all Plaintiffs allege the same core theory of  
8 liability: that Google’s automated scanning of emails is an illegal interception of their electronic  
9 communications without their consent. Plaintiffs claim that Google’s systems “read[] each and  
10 every message” as part of the regular course of providing the Gmail service to its users. (*Id.* ¶ 3.)  
11 Plaintiffs purport to carve out spam filtering and virus detection from their claims, (*see, e.g., id.*  
12 ¶¶ 43, 45), but their claims otherwise apply to *all* forms of scanning, regardless of the purpose or  
13 the benefits to Gmail users provided by scanning.

### 14 **III. APPLICABLE STANDARDS.**

15 This Motion is governed by Rule 12(b)(6) as interpreted in *Bell Atl. Corp. v. Twombly*,  
16 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). Under these standards, the court  
17 is “free to ignore legal conclusions, unsupported conclusions, unwarranted inferences and  
18 sweeping legal conclusions cast in the form of factual allegations.” *Stanislaus Food Prods. Co. v.*  
19 *USS-POSCO Indus.*, 782 F. Supp. 2d 1059, 1064 (E.D. Cal. 2011); *see also Caviness v. Horizon*  
20 *Cnty. Learning Ctr., Inc.*, 590 F.3d 806, 812 (9th Cir. 2010).

### 21 **IV. ARGUMENT**

#### 22 **A. The Wiretapping Claims Fail Because the Alleged Scanning Practices Are** 23 **Part of Google’s Ordinary Course of Business as an ECS Provider.**

##### 24 **1. The Wiretap Statutes Exempt ECS Providers from Liability.**

25 The overall structure of ECPA<sup>6</sup> reflects Congress’s careful effort to ensure that ECPA’s

26 81 (Pa. 1988). For purposes of this motion, the only relevant difference between ECPA and these  
27 laws concerns their requirement of dual, as opposed to single, party consent, as discussed below.

28 <sup>6</sup> As background, ECPA “amended the Federal wiretap law” and was “divided into Title I, which  
governs unauthorized interceptions of electronic communications, 18 U.S.C. §§ 2510-2522, and  
Title II, which governs unauthorized access to stored communications, 18 U.S.C. §§ 2701-2711.”  
*Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503 (2d Cir. 2005).

1 provisions regarding the “interception” of electronic communications will not interfere with ECS  
2 providers’ ability to engage in their normal business practices. In enacting ECPA, Congress  
3 recognized that “provider[s] of electronic communications services may have to monitor a stream  
4 of transmissions in order to properly route, terminate, and otherwise manage the individual  
5 messages they contain,” and that such monitoring “may be necessary to the provision of an  
6 electronic communication service.” (Wong Decl., Exh. BB [S. Rep. No. 99-541] at p. 20). With  
7 respect to email in particular, Congress noted that “the providers of electronic mail create  
8 electronic copies of private correspondence for later reference,” and that “[t]his information is  
9 *processed for the benefit of the user.*” *Id.* at 3 (emphasis added). *See also In re DoubleClick*  
10 *Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (explaining that emails must be  
11 “temporarily stored by electronic communications services incident to their transmission – for  
12 example, when an email service stores a message until the addressee downloads it”).

13 Given these realities, Congress clarified that ECS providers can lawfully receive and  
14 access electronic communications involving their users—the very things that Plaintiffs contend are  
15 unlawful. For instance, while Section 2701 generally prohibits parties from accessing electronic  
16 communications in electronic storage, this provision “does not apply with respect to conduct  
17 authorized . . . by the . . . entity providing a wire or electronic communications service.” 18  
18 U.S.C. § 2701(c)(1). In other words, ECS providers are expressly authorized to access the  
19 communications sent to their systems. Title II prohibits ECS providers only from *disclosing* the  
20 electronic communications of their users, which is not at issue here (and even this general bar is  
21 subject to specific exceptions that allow an ECS provider to disclose communications in some  
22 circumstances). *See* 18 U.S.C. §§ 2701-2703.<sup>7</sup> *See, e.g., Bohach v. City of Reno*, 932 F. Supp.  
23 1232, 1236 (D. Nev. 1996) (Section 2701 “allows service providers to do as they wish when it  
24 comes to accessing communications”); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d  
25 Cir. 2003) (no ECPA liability under Section 2701 where ECS provider searched the contents of  
26 text messages in its systems).

---

27 <sup>7</sup> The state wiretapping statutes at issue include analogous terms. *See* Fla. Stat. §§ 934.21-23;  
28 Md. Code, Cts. & Jud. Proc. §§ 10-402 to -404; 18 Pa. C.S. §§ 5741-43; *see also* Appendix.



1 Similarly, Title I, relating to the interception of communications, contains several terms  
2 that exempt ECS providers from liability. Most importantly, Section 2510(5)(a)(i) excludes from  
3 the definition of “device” the equipment of an ECS provider used to access electronic  
4 communications “in the ordinary course of its business.”<sup>8</sup> Thus, a “Wiretap Act claim requires, at  
5 a minimum, (a) an ‘electronic communication’ and (b) interception of that communication by  
6 someone *other than* ‘a provider of wire or electronic communication service ... in the normal  
7 course of’ business . . . ” *In re Google, Inc. Privacy Policy Litig.*, No. 12-cv-1382 PSG, 2012 WL  
8 6738343, at \*5 (N.D. Cal. Dec. 28, 2012) (emphasis added) (“*In re Google Privacy Policy*”).

9 Other provisions further clarify that an ECS provider’s normal practices are not an illegal  
10 “interception” under Section 2510. *See, e.g.*, 18 U.S.C. § 2511(2)(a)(i) (permitting employees  
11 and agents of an ECS provider “to intercept, disclose, or use” electronic communications being  
12 transmitted by the ECS for normal business purposes including “the protection of the rights or  
13 property of the” ECS provider); *id.* (permitting ECS providers to engage in “service observing”  
14 and “random monitoring” of electronic communications while prohibiting the same for wire (*e.g.*,  
15 telephone and telegraph) communications).

16 The rationale underlying these provisions is to ensure that ECS providers can deliver  
17 electronic communications and provide related services to their users without incurring liability  
18 under the provisions of the statute aimed at illicit behavior. As the Second Circuit explained in  
19 *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005), these provisions exempting  
20 ECS providers from liability must be applied consistently; otherwise, ECS providers “would  
21 constantly be intercepting communications under ECPA because their basic services involve the  
22 ‘acquisition of the contents’ of electronic communication.”

## 23 2. Courts Have Consistently Dismissed Claims Against ECS Providers 24 Involving Circumstances Similar to Those Alleged Here.

25 Applying this statutory scheme, courts have consistently rejected claims by plaintiffs  
26 attempting to characterize the normal business practices of ECS providers like Google as an  
27 illegal “interception” under the wiretapping statutes.

28 <sup>8</sup> The state wiretapping statutes at issue include analogous terms. *See* Fla. Stat. § 934.02(4)(a)2;  
Md. Code, Cts. & Jud. Proc. § 10-401(4)(i); 18 Pa. C.S. § 5702; *see also* Appendix.

1 For example, in *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), the  
2 plaintiffs alleged that the defendant, an ISP, unlawfully “intercepted their Internet  
3 communications” by extracting information about their Internet browsing histories for the  
4 purpose of delivering targeted advertisements. *Id.* at 1245-48. The court affirmed the dismissal  
5 of the claim as a matter of law because all of the data at issue (plaintiffs’ Internet browsing  
6 histories) was obtained in the course of defendant’s business as an ISP. *Id.* at 1246, 1250-51.  
7 The fact that the ISP extracted a subset of the data for purposes of delivering targeted  
8 advertisements had no affect on the analysis “because [defendant’s] access was in the ordinary  
9 course of its core business as an ISP transmitting data over its equipment.” *Id.* at 1249. *See also*  
10 *id.* at 1250-51 (explaining that the advertising delivery system at issue “gave [the defendant]  
11 access to no more of [the plaintiffs’] electronic communications than it had in the ordinary course  
12 of its business as an ISP.”).

13 Judge Grewal applied these same considerations to dismiss an ECPA claim in the specific  
14 context of a claim alleging that Google “intercepted” its users’ information. In *In re Google*  
15 *Privacy Policy*, the plaintiffs alleged that “an interception occurred when their content from one  
16 Google product was . . . combined with information from another Google product that also was  
17 stored on Google’s servers.” 2012 WL 6738343, at \*5-6. The claims in that matter were far  
18 broader than here; plaintiffs alleged that Google accesses and uses information from dozens of  
19 Google products, including Gmail, without consent to serve targeted advertisements and for other  
20 allegedly improper purposes. (Wong Decl., Exh. CC.) But as Judge Grewal recognized, even if  
21 Google’s access and use of the information at issue exceeded the scope of Google’s terms, there  
22 was no viable claim for an “interception” because “[a]n interception claim under the Wiretap Act  
23 also requires the use of a defined ‘device,’ which cannot include Google’s own systems . . .” *In*  
24 *re Google Privacy Policy*, 2012 WL 6738343 at \*5 (emphasis added). *See also id.* at \*6 (“the  
25 inescapably plain language of [ECPA] . . . excludes from the definition of a ‘device’ a provider’s  
26 own equipment used in the ordinary course of business.”). Because the complaint did not allege  
27 the use of a “device” outside of Google’s own systems, the Court dismissed the complaint as a  
28 matter of law. *Id.*

1 This case is no different. Plaintiffs’ wiretapping claims fail because they do not allege the  
2 use of “a defined ‘device’” distinct from “*Google’s own systems.*” *Id.* at \*5 (emphasis added).  
3 Instead, the Complaint confirms that the alleged “interceptions” involve only Google’s own  
4 equipment used in its capacity as an ECS provider. (*See* Compl., ¶¶ 22-92 (describing various  
5 Google servers and systems with no allegation of any non-Google device).) This alone mandates  
6 dismissal. *In re Google Privacy Policy*, 2012 WL 6738343 at \*5.<sup>9</sup>

7 Moreover, the Complaint repeatedly confirms that the purpose of the alleged  
8 “interceptions” is to implement normal functions within the ordinary course of Google’s business.  
9 Specifically, Plaintiffs complain that Google scans information from its users (the emails sent to  
10 and from Gmail users) in order to extract a subset of information (keywords and other  
11 information from the emails) “for the purpose of delivering content-based advertising.”<sup>10</sup> (*See*  
12 Compl. ¶¶ 22-91, 259(g) (describing Google’s processing of emails and alleging that Google does  
13 so to deliver advertising).) This is strikingly similar to the facts in *Kirch*, in which the defendant  
14 provided information from its users (their Internet activity) to a third party so that a subset of that  
15 information (“customer requests for highly trafficked commercial websites”) could be used “to  
16 deliver online advertising thought likely to be interest users who visited those websites.” 702  
17 F.3d at 1247-48. As in *Kirch*, there is no illegal “interception” here because all of the email  
18 information at issue in Plaintiffs’ claims stems from Google “access ... in the ordinary course of  
19 its core business as [ECS provider] transmitting data over its equipment.” *Id.* at 1249. Notably in  
20 *Kirch*, the defendant was accused, unlike here, of providing its users’ information to a *third party*.

21 In short, there is no illegal “interception” here because Plaintiffs’ own allegations confirm  
22 that the alleged practices at issue are part of Google’s ordinary course of business.

### 23 3. Plaintiffs’ Efforts to Plead around the “Ordinary Course of Business” 24 Exemption Fail.

25 <sup>9</sup> *See also Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, No. 07-cv-1029, 2007 WL 4394447, at \*4  
(E.D. Pa Dec. 13, 2007) (“The drive or server on which an email is received does not constitute a  
26 device for purposes of the Wiretap Act.”).

27 <sup>10</sup> Plaintiffs also note various other alleged purposes for Google’s automated scanning, which  
28 further confirm that Google’s practices are implemented for ordinary business reasons. (*See*  
Compl. ¶ 288 (alleging that Google scans emails for “commercial advantage and profits”); *id.* at  
¶ 338 (alleging that Google scans emails to reduce certain “traffic acquisition costs”).) Seeking  
profits and lowering costs are, of course, normal business purposes.

1        Rather than alleging any facts to show an illegal “interception,” Plaintiffs seek to avoid  
2 the “ordinary course of business” exemption by claiming that Google’s practices are not an  
3 “industry standard” practice. (Compl. ¶ 262.) Plaintiffs further suggest that Google’s Gmail-  
4 related practices, including the delivery of targeted advertising, fall outside of the exemption  
5 because they are not a necessary “service of a provider of an electronic communication service.”  
6 (Compl. ¶¶ 264-65.)

7        But the “ordinary course of business” exemption does not turn on whether an alleged  
8 practice is necessary for an ECS provider to deliver an electronic communication. Nor does the  
9 exemption turn on whether an ECS provider’s practices conform to Plaintiffs’ subjective notion  
10 of the prevailing “industry standard.” Indeed, it would be nonsensical to assume that Congress  
11 intended to deprive an ECS provider of the “ordinary course of business” exemption simply  
12 because it chooses to run its business differently (or better) than its competitors.

13        Instead, the exemption applies broadly to protect an ECS provider’s acts in the “course of  
14 *its* business.” 18 U.S.C. 2510(5)(a)(ii)(emphasis added). For example, in *Hall*, the plaintiff  
15 argued that his email service provider did not act in the ordinary course of its business by  
16 continuing to deliver emails to customers who had terminated their accounts. 396 F.3d at 505.  
17 The Second Circuit did not inquire whether this practice was necessary to the defendant’s  
18 business of delivering emails or whether it was consistent with prevailing industry standard.  
19 Instead, the Court applied the “ordinary course of business” exemption because it was the email  
20 service provider’s *own* internal “practice at the time to continue to receive and store e-mails . . .  
21 after any account was cancelled.” *Id.*

22        Similarly, the *In re Google Privacy Policy* plaintiffs alleged that Google’s unique  
23 combination of products, including Gmail, allows it to target advertisements in a way that has no  
24 industry equivalent. (*See, e.g.,* Wong Exh. CC at ¶ 17 (alleging that Google’s products, including  
25 Gmail, provide it with “targeted advertising capabilities” that “surpass those offered by social  
26 networks, such as Facebook.”).) Yet these allegations did not deter Judge Grewal from applying  
27 the “ordinary course of business exemption,” as discussed above. *In re Google Privacy Policy*,  
28 2012 WL 6738343 at \*5-6. In reaching that conclusion, the Court found no need to consider

1 whether Google’s practices conform to an “industry standard” for the “services of an electronic  
2 communications service provider” (Compl. ¶¶ 262, 264-65), because those considerations are  
3 simply irrelevant.

4 The same result applies here: notwithstanding Plaintiffs’ effort to plead around the  
5 “ordinary course of business” exemption, all wiretapping claims fail for the simple reason that the  
6 alleged conduct at issue is undisputedly part of *Google’s* ordinary business practices as an ECS  
7 provider (and a provider of a free service at that).

#### 8 **4. Plaintiffs’ Theory of Liability Would Lead to Absurd Results.**

9 More generally, Plaintiffs’ wiretapping claims should be rejected because they would  
10 criminalize an ECS provider’s normal methods for processing emails and other electronic  
11 communications. Indeed, Plaintiffs’ theory of liability—that the scanning of email content by an  
12 ECS provider is an illegal “interception”—directly conflicts with Title II, which expressly permits  
13 an ECS provider to “access” electronic communications sent to its systems (and even to disclose  
14 such communications in certain circumstances). The Court should not allow Plaintiffs to pursue a  
15 theory of an illegal “interception” that creates these sorts of irreconcilable conflicts within the  
16 statutory scheme. *See Hibbs v. Winn*, 542 U.S. 88, 101 (2004) (“A statute should be construed so  
17 that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or  
18 insignificant.”) (citation omitted); *Bayview Hunters Point Cmty. Advocates v. Metro. Transp.*  
19 *Comm’n*, 366 F.3d 692, 700 (9th Cir. 2004) (A statute “should not be interpreted in a way which  
20 is internally contradictory or that renders other provisions of the same statute inconsistent or  
21 meaningless.”) (citation and quotation omitted).

22 In practice, Plaintiffs’ theory would prevent ECS providers from providing a host of  
23 normal services that Congress could not possibly have intended to criminalize as an illegal  
24 “interception.” For example, an ECS provider could not allow users to sort their emails using  
25 automated filters because any such system would require scanning the contents of the emails  
26 being delivered to the user, thus running afoul of Plaintiffs’ theory. Nor could an ECS provider  
27 provide even basic features like allowing users to search their own emails for particular key terms  
28 because doing so would, again, involve the scanning of email content. And while Plaintiffs have

1 removed spam filtering and virus detection from their claims, these selective carve-outs simply  
2 underscore the fact that their sweeping theory of liability would *otherwise* encompass these basic  
3 (and desirable) features of email.<sup>11</sup>

4 In short, Plaintiffs’ interpretation would render large swaths of the statutory scheme  
5 meaningless while making it virtually impossible for ECS providers to provide normal services to  
6 their users. The Court should not allow Plaintiffs to proceed on this basis.

7 **5. The Pennsylvania Wiretap Statute Applies Only to the Senders, Not**  
8 **the Recipients of a Communication.**

9 A further basis exists under Pennsylvania law to reject Plaintiff Brinkman’s claim of an  
10 alleged “interception.” Section 5725 of the Pennsylvania statute only authorizes a private right of  
11 action for a person “whose wire, electronic or oral communication is intercepted, disclosed or  
12 used . . .” 18 Pa. C.S. § 5725. Pennsylvania courts have interpreted this to mean “that the cause  
13 of action belongs to the person with whom the communication originated, not the recipient.”  
14 *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622, 633 (E.D. Pa. 2006) (citing *Kline v. Sec.*  
15 *Guards, Inc.*, 386 F.3d 246, 257 (3d Cir. 2004)). In *Klump*, the plaintiff lacked standing under  
16 section 5725 because the allegedly intercepted communications were sent *to* him, and therefore  
17 he could not meet the first requirement of the prima facie case. *Id.* at 633. To the extent that  
18 Plaintiff Brinkman seeks to bring claims for emails that she received but did not author (Compl.  
19 §§ 365, 391), she has no private right of action and her claim must be dismissed. *Id.*

20 **B. Plaintiffs’ Claims Also Fail Under the Consent Defenses of the Wiretap**  
21 **Statutes at Issue.**

22 In addition to the lack of any illegal “interception,” the Wiretapping Plaintiffs’ claims also  
23 fail for the additional reason that the senders and recipients of the emails at issue have all

---

24 <sup>11</sup> The wiretapping claims of Plaintiffs Fread and Carrillo are further undermined by the Family  
25 Educational Rights and Privacy Act of 1974 (“FERPA”). Plaintiffs Fread and Carrillo allege that  
26 Google violated the Wiretap Act by processing their emails on behalf of the universities at which  
27 they are enrolled. But Plaintiffs admit that Google’s actions were taken under contracts with each  
28 university, in which the university outsourced its email processing to Google. Even assuming,  
arguendo, that FERPA applies here, the law permits schools to “outsource[] institutional services  
or functions,” including provision of email services. *See* 34 C.F.R. 99.31(a)(1)(i)(B). A party  
such as Google, to whom this function has been outsourced, is deemed a “school official,” and as  
such may access and use student records, even without student consent. *Id.* The Court should not  
construe an “interception” under the Wiretap Act in a manner that would criminalize conduct that  
is expressly permitted under FERPA and its implementing regulations.

1 necessarily consented to the processing of their emails by Google.

2 The consent defense to a wiretap claim can be based on the terms of an express  
3 agreement. *See, e.g., Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-  
4 cv-4567, 2011 WL 900096, at \*10-11 (D.N.J. Mar. 15, 2011) (“[B]y subscribing to [Microsoft’s  
5 email service], each Microsoft customer consents to Microsoft intercepting and filtering all of his  
6 email communications.”). Consent can also be implied from the overall circumstances of a  
7 particular communication. *See, e.g., United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996)  
8 (consent may be “implied in fact from surrounding circumstances . . .”) (citation and quotation  
9 omitted).

10 Under federal law, the consent of a *single* party to a communication is complete defense  
11 to any liability and so the consent of the Gmail user alone is sufficient to bar a claim. *See* 18  
12 U.S.C. § 2511(2)(d). The state wiretap statutes at issue also provide a defense where both parties  
13 to the communication consent to the alleged interception. Fla. Stat. § 934.03(2)(d); Md. Code,  
14 Cts. & Jud. Proc. § 10-402(c)(3); 18 Pa. C.S. § 5704(4).

15 **1. The Gmail Plaintiffs Expressly Consent to Automated Scanning,**  
16 **Precluding Any Claim under ECPA.**

17 The single-party consent defense under federal law precludes the Gmail Plaintiffs’ claims  
18 as a matter of law because they expressly consented to automated scanning in exchange for using  
19 the free Gmail service. The Gmail Plaintiffs concede that by signing up for, or using, their Gmail  
20 or Google Apps accounts (Compl. ¶¶ 219, 223, 233, 241, 247), they are contractually bound to  
21 Google’s terms. Indeed, they devote much of the Complaint to attacking the disclosures in the  
22 TOS and Privacy Policy in an effort to avoid this express contractual consent.

23 Because the Gmail Plaintiffs are bound to Google’s TOS and/or Privacy Policy, they have  
24 expressly consented to the scanning disclosed in these terms. For example, the TOS in effect  
25 during the majority of the proposed class period informed users that Google’s services, including  
26 Gmail, are supported by advertising revenue and that Google may display advertising targeted to  
27 the content of user information, including emails in Gmail accounts: “[A]dvertisements may be  
28

1 targeted to the content of information stored on the Service<sup>12</sup>, queries made through the Service or  
2 other information.” (Rothman Decl., ¶ 11, Exh. E, at § 17.1.) This TOS further provided that  
3 “Google reserves the right . . . to pre-screen, review, flag, filter . . . any or all Content from any  
4 Service.” (*Id.* at § 8.3.) The Google Privacy Policies throughout the class period declared in  
5 varying but clear terms that Google may use the information from users to “[p]rovide, maintain,  
6 protect, and improve our services (including advertising services) and develop new services.”  
7 (*Id.*, ¶ 16, Exh. I; *see also id.* ¶¶ 13-16, Exhs. G-J.)

8 Google updated its TOS and Privacy Policy on March 1, 2012. These updated versions  
9 (which are currently in effect, but for an unrelated change in the Privacy Policy in July 2012) also  
10 explained, and required users to agree to, the automated scanning practices at issue. The updated  
11 TOS notifies users that “Google’s privacy policies explain how we treat your personal data and  
12 protect your privacy,” and that “[b]y using our Services, you agree that Google can use such data  
13 in accordance with our privacy policies.” (*Id.*, ¶ 12, Exh. F.) The updated Privacy Policy, in turn,  
14 explains that Google collects information that users generate while using Google’s services,  
15 including Gmail, and can use information from “all of [Google’s] services to provide, maintain,  
16 protect and improve them, to develop new ones, and to protect Google and [its] users.” (*Id.* ¶ 16,  
17 Exh. J.) The Privacy Policy further specifies that Google “also use[s] this information to offer  
18 you tailored content – like giving you more relevant search results and ads.” (*Id.*)

19 These express terms plainly encompass Google’s scanning of email content as part of  
20 providing the Gmail service. Because the Gmail Plaintiffs are bound to these terms as a condition  
21 of using Gmail<sup>13</sup>, they cannot pursue a claim under ECPA, which precludes liability based on a  
22 single party’s consent. *Kirch v. Embarq Mgmt. Co.*, No. 10-cv-2047, 2011 WL 3651359, at \*7-8  
23 (D. Kan. Aug. 19, 2011) (finding consent based on defendant’s terms of service); *Deering v.*  
24 *CenturyTel, Inc.*, No. 10-cv-0063, 2011 WL 1842859, at \*1-3 (D. Mont. May 16, 2011)

25 <sup>12</sup> “Services” is a defined term that includes broadly covers all Google services, including Gmail.  
(*See* Rothman Decl., Ex. E at §1.1.)

26 <sup>13</sup> As referenced in note 4, the Cable One Apps TOS that Plaintiff Dunbar agreed to includes  
27 essentially identical terms as the Google TOS referenced above (with minor differences as noted  
28 in the Rothman Declaration) and links to the same Google Privacy Policy. Further, Hawaii and  
UoP were contractually required to obtain the necessary consent from end users, like Fread and  
Carrillo, for Google to provide the Gmail service.



(dismissing ECPA against ISP based on users' consent to privacy policy).<sup>14</sup>

## 2. Minors like Plaintiff J.K. Cannot Avoid the Terms They Agreed To.

Trying to wriggle free from these binding terms, Plaintiff J.K. (one of the Gmail Plaintiffs) claims he "could not have consented" because he is sixteen years old and his agreement is thus "void" under California law. (Compl. ¶¶ 250, 275.) To support this assertion, Plaintiff J.K. relies principally on Section 6701(c)<sup>15</sup> of the Family Code, which provides that contracts with minors are void if they "relat[e] to any personal property not in the immediate possession or control of the minor." Cal. Fam. Code § 6701(c). But there is nothing in the Family Code or any authority applying the statute suggesting that an agreement in which a minor provides consent to the use of his information is a contract concerning "personal property." Compare *Taylor v. Indus. Accident Comm'n*, 216 Cal. App. 2d 466, 473 (1963) (applying the predecessor statute to Section 6701 with identical terms and holding that hard copies of newspapers are "personal property"). Moreover, Plaintiff J.K.'s express consent to the automated processing of his emails cannot fall within the scope of Section 6701(c) because Plaintiff's emails are "within [his] possession or control." Like all Gmail users, Plaintiff J.K. is in full control of the emails in his Gmail account and can select what emails to send, which emails to retain, and which to delete. Under these circumstances, the contractual consent that Plaintiff J.K. gave to Google does not fall within either the terms or the underlying purpose of Section 6701(c).

Even if the California Family Code could be construed to invalidate Plaintiff J.K.'s

---

<sup>14</sup> See also *Mortensen v. Bresnan Commc'n, LLC*, No. 10-cv-0013, 2010 WL 5140454, at \*3-5 (D. Mont. Dec. 13, 2010) (dismissing ECPA claim against ISP based on its users' consent in the account agreement, privacy policy, and other posted notices); *In re Vistaprint Corp. Mktg. & Sales Pracs. Litig.*, No. 08-md-1994, 2009 WL 2884727, at \*9 (S.D. Tex. Aug. 31, 2009), *aff'd*, 392 F. App'x 327 (5th Cir. 2010) (dismissing ECPA claim based on consent); *Borninski v. Williamson*, No. 02-cv-1014, 2005 WL 1206872, at \*12-13 (N.D. Tex. May 17, 2005) (no ECPA violation where plaintiff signed agreement and expressly consented to defendant's monitoring of his communications).

<sup>15</sup> The Complaint also refers in passing to Section 6701(a), which provide that contracts with minors are deemed void if they involve a "delegation of power." (Compl. ¶ 274.) But apart from parroting the statutory term, Plaintiffs allege no facts to show how Google's terms could fall within this provision. In addition to these categories of void contracts, California law also allows minors to disaffirm an otherwise enforceable contract in limited circumstances under Section 6710. Plaintiff J.K., however, does not specify that he seeks to disaffirm his contract under this provision and asserts only that his agreement is void under Section 6701. See *Berg v. Traylor*, 148 Cal. App. 4th 809, 820 (2007) (a minor's disaffirmance must be reflected in an "unequivocal intent to repudiate [the contract's] binding force and effect.") (citation and quotation omitted).

1 express consent, it would be preempted by the federal Children’s Online Privacy Protection Act  
2 (“COPPA”), 15 U.S.C. §§ 6501-08. COPPA reflects Congress’s judgment that operators of  
3 websites *can* obtain and use information from teens like Plaintiff J.K. by obtaining their consent.  
4 Under COPPA, an “operator of a website or online service” cannot deal directly with a minor and  
5 must obtain parental consent in order to “collect” or “use” the “personal information” of a  
6 “child”—but *only where the child is “under the age of 13.”* *Id.* §§ 6501(1), 6502(a)(1),  
7 (b)(1)(A). In enacting these terms, Congress specifically considered *and rejected* a parental  
8 consent requirement for teens like Plaintiff J.K. (*See* Wong Decl., Exh. JJ [the “COPPA FAQ”],  
9 No. 11] (“In enacting [COPPA], Congress determined to apply the statute’s protections only to  
10 children under 13”).)

11 Rather than requiring parental consent, the regulatory scheme of COPPA encourages  
12 websites to obtain consent directly from teens in connection with the use of their information. As  
13 the Federal Trade Commission (“FTC”) explains in its COPPA FAQ: “Although COPPA does  
14 not apply to teenagers, the FTC is concerned about teen privacy and does believe that strong,  
15 more flexible, protections may be appropriate for this age group.” (*Id.*) To illustrate these  
16 alternative “protections” for teens, the COPPA FAQs refer to a separate FTC Report that  
17 encourages websites to obtain “affirmative express consent” from teens in certain circumstances  
18 (while emphasizing that consent “may not be necessary in every advertising campaign directed to  
19 teens”). (*See* Wong Decl., Exh. KK). To ensure consistent application of these standards,  
20 COPPA expressly preempts any state law that treats the use of “personal information” in a  
21 manner that “inconsistent” with COPPA. *See* 15 U.S.C. § 6502(d).

22 This federal statutory scheme bars Plaintiff J.K. from using the California Family Code to  
23 invalidate the “affirmative express consent” that he gave to Google—consent that Google was not  
24 only allowed to obtain but *encouraged* to obtain from Plaintiff J.K. under COPPA.

25 **3. Plaintiffs Fread and Carrillo Cannot Avoid Their Express Consent by**  
26 **Claiming They Were Pressured into Using Gmail.**

27 Nor can Plaintiffs Fread and Carrillo avoid Google’s terms merely by suggesting that they  
28 felt pressured to use their university email accounts operated through Google Apps. For example,

1 Fread alleges that he initially avoided using his email account knowing it would be processed  
2 similarly to Gmail, but was forced to acquiesce “in order to send and receive official [university]  
3 communications.” (Compl. ¶ 233.) Plaintiff Carrillo similarly claims he used his university  
4 account due only to a “forced migration process,” although he concedes he clicked to agree to the  
5 “terms and conditions” and “privacy policy” associated with the new account. (*Id.* ¶ 241.)

6 These vague assertions do nothing to undermine the enforceability of the terms that are  
7 binding on these Plaintiffs. Under California law, a party may avoid a contract under a claim of  
8 duress only if it can show that “a party intentionally used threats or pressure to induce action or  
9 nonaction to the other party’s detriment” where “[t]he coercion . . . induce[d] the assent of the  
10 coerced party, who has no reasonable alternative to succumbing.” *In re Marriage of Baltins*, 212  
11 Cal. App. 3d 66, 84 (1989) (citing Restatement (Second) of Contracts § 175(1)(1981)) (other  
12 citations and internal quotation omitted). While these Plaintiffs suggest they felt pressured by  
13 circumstances to use their email accounts, they do they not allege that this pressure was due to  
14 any “threats or coercion” by Google or that they lacked “a reasonable alternative,” as would be  
15 needed to invalidate their express contractual consent under state law. Moreover, courts have  
16 held that the continued use of a form of communication that an individual knows may be  
17 monitored or recorded is sufficient to supply consent under the Wiretap Act—even if there was no  
18 meaningful choice. *See, e.g., United States v. Verdin-Garcia*, 516 F.3d 884, 894 (10th Cir. 2008)  
19 (“A prisoner’s voluntarily made choice—even a Hobson’s choice—to use a telephone he knows  
20 may be monitored implies his consent to be monitored.”).

21 Accordingly, Plaintiffs Fread’s and Carrillo’s individual allegations are irrelevant as a  
22 matter of law and do not undermine the express consent they gave.<sup>16</sup>

23  
24  
25 <sup>16</sup> As a separate basis for avoiding express consent, Plaintiffs make a vague reference to Section  
26 2511(2)(d), which provides that the consent defense is inapplicable where a communication is  
27 “intercepted for the purpose of committing any criminal or tortious act . . .” (Compl. ¶ 281.) This  
28 provision applies only where the defendant acted with a specific intent to cause injury. *See, e.g.,*  
*In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d at 515 (discussing Section 2511(2)(d) at  
length and noting congressional intent to invalidate consent only where “the party acts in any way  
with an intent to injure the other party”) (emphasis omitted). Here, the Complaint is devoid of a  
single allegation to show that Google had the specific intent to harm its Gmail users.

1                   **4. The Non-Gmail Plaintiffs Also Impliedly Consent to the Automated**  
2                   **Processing of Their Messages.**

3                   The state law wiretap claims of the Non-Gmail Plaintiffs fail for similar reasons. While  
4                   the non-Gmail Plaintiffs are not bound to Google's contractual terms, they nonetheless impliedly  
5                   consent to Google's practices by virtue of the fact that *all* users of email must necessarily expect  
6                   that their emails will be subject to automated processing.

7                   Just as a sender of a letter to a business colleague cannot be surprised that the recipient's  
8                   assistant opens the letter, people who use web-based email today cannot be surprised if their  
9                   communications are processed by the recipient's ECS provider in the course of delivery. Indeed,  
10                  "a person has no legitimate expectation of privacy in information he voluntarily turns over to  
11                  third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). In particular, the Court noted  
12                  that persons communicating through a service provided by an intermediary (in the *Smith* case, a  
13                  telephone call routed through a telephone company) must necessarily expect that the  
14                  communication will be subject to the intermediary's systems. For example, the Court explained  
15                  that in using the telephone, a person "voluntarily convey[s] numerical information to the  
16                  telephone company and 'expose[s]' that information to its equipment *in the ordinary course of*  
17                  *business*." *Id.* at 744 (emphasis added).

18                  The same is true of email sent through an ECS provider. As numerous courts have held,  
19                  the automated processing of email is so widely understood and accepted that the act of sending an  
20                  email constitutes implied consent to automated processing as a matter of law. *See, e.g., State v.*  
21                  *Townsend*, 57 P.3d 255, 260 (Wash. 2002) (finding that sender of email impliedly consented to  
22                  interception of his email because "in order for e-mail to be useful it must be" subjected to  
23                  automated processes, such as being "recorded on another computer's memory."); *Commonwealth*  
24                  *v. Proetto*, 771 A.2d 823, 829 (Pa. Super. Ct. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003) ("Any  
25                  reasonably intelligent person, savvy enough to be using the Internet, however, would be aware of  
26                  the fact that messages are received in a recorded format, by their very nature, and can be  
27                  downloaded or printed by the party receiving the message. By the very act of sending a  
28                  communication over the Internet, the party expressly consents to the recording of the message.");

1 *State v. Lott*, 879 A.2d 1167, 1172 (N.H. 2005) (sender of instant messages “implicitly  
2 consented” to the interception of his communications where he voluntarily sent instant messages  
3 knowing that, by the medium’s nature, his messages would be automatically recorded).<sup>17</sup>

4 Similarly here, non-Gmail users who send emails to Gmail recipients must expect that  
5 their emails will be subjected to Google’s normal processes as the ECS provider for their intended  
6 recipients. Indeed, when the non-Gmail Plaintiffs filed their initial complaints, some specifically  
7 alleged that they *continued to send emails to Gmail users* despite their knowledge of Google’s  
8 automated scanning (as confirmed in their complaints).<sup>18</sup> This ongoing use shows that Google’s  
9 automated scanning was completely immaterial to these Plaintiffs’ decisions to communicate with  
10 Gmail users and suggests that they were aware of Google’s automated scanning all along. In fact,  
11 Plaintiff Fread’s own allegations confirm that Google’s automated scanning is common  
12 knowledge among non-Gmail users. Plaintiff Fread alleges he spent months trying to avoid using  
13 his Google Apps account, due to his awareness of and apparent concern about Google’s email  
14 processing. (Compl. ¶ 233.) So too, the non-Gmail Plaintiffs must have expected that their  
15 emails to Gmail recipients would be subject to automated processing by Google in its capacity as  
16 the ECS provider for their intended recipients. As in *Smith*, these Plaintiffs cannot claim  
17 ignorance because they “voluntarily conveyed” emails to Google as an ECS provider and  
18 “‘expose[d]’ that information to [Google’s] equipment in the ordinary course of business.” 442  
19 U.S. at 744. Under these circumstances, the non-Gmail Plaintiffs have impliedly consented to  
20 Google’s automated scanning. Thus, in combination with the express consent of the Gmail  
21 recipients (as discussed above), their communications are subject to the dual-party consent  
22 defenses of the state wiretapping laws and their claims must be dismissed as a matter of law.

23  
24 <sup>17</sup> See also *State v. Roden*, 279 P.3d 461, 466 (Wash. Ct. App. 2012) (finding that the defendant  
25 “impliedly consented” to a law enforcement officer’s interception of his text messages because  
26 “as a user of text message technology,” the defendant necessarily “understood that [his drug  
27 dealer’s cell phone] would record and store the text messages that he sent”); *Commonwealth v.*  
28 *Maccini*, No. 06-cv-0873, 2007 WL 1203560, at \*3 (Mass. Super. Ct. Apr. 23, 2007) (holding  
that, given the nature of email communications, law enforcement’s “receipt and recording of the  
defendant’s communications was not secret but rather was *with the defendant’s knowledge and*  
*implicit consent.*” (emphasis added)).

<sup>18</sup> See Wong, Decl., Exh. EE (J.K. Compl. ¶ 21); Exh. FF (Knowles Compl. ¶ 20); Exh. GG  
(Brinkman Compl. ¶ 15); Exh. II (Scott II Compl. ¶ 15).

1 In sum, the Wiretapping Plaintiffs’ claims fail in their entirety due to both the “ordinary  
2 course of business” exemption and the consent defenses applicable under ECPA and the state  
3 wiretapping statutes at issue.<sup>19</sup>

4 **C. The CIPA Claim Also Fails as a Matter of Law for Multiple Reasons.**

5 **1. CIPA Does Not Apply to Email Communications.**

6 The CIPA claim fares no better because the statute, enacted in 1967, was never intended  
7 to apply, and by its terms cannot be applied, to emails. On its face, Section 631 of CIPA is  
8 limited to interceptions that involve “telephone and telegraph” communications. *See* Cal. Penal  
9 Code § 631.<sup>20</sup> The first clause of Section 631 expressly refers to wiretapping of a “*telegraph or*  
10 *telephone wire, line, cable, or instrument.*” *Id.* (emphasis added). The second clause covers other  
11 forms of interception that involve “read[ing]” or “learn[ing] the contents” of a communication,  
12 but reiterates that liability only applies if the communication is “in transit or passing over *any*  
13 *wire, line, or cable,* or is being sent from, or received at any place within this state.” *Id.*  
14 (emphasis added). While the term “telegraph or telephone” is not repeated in the second clause, it  
15 would be nonsensical to assume that the Legislature intended to cover two totally different  
16 categories of “wire[s], line[s], or cable[s]” in two clauses of the same single-sentence provision.  
17 For this reason, California courts have interpreted Section 631 as focusing on telephone and  
18 telegraph communications alone. *See People v. Chavez*, 44 Cal. App. 4th 1144, 1150 (1996)  
19 (explaining that “[w]iretapping refers to the interception by any method of *telegraphic or*  
20 *telephonic communications*”) (emphasis added).

21 Section 632 similarly excludes electronic communications. In particular, Section 632 is  
22 targeted at “[e]avesdropping.” *See* Cal. Penal Code § 632. Obviously, one cannot “eavesdrop”  
23 on an email or other purely electronic communication in any normal sense of the word. *See*

---

24 <sup>19</sup> These same considerations apply to the Gmail Plaintiffs and CIPA Plaintiffs as well. As to the  
25 Gmail Plaintiffs, even if the Court does not find express contractual consent as to the Gmail  
26 Plaintiffs, their claims would be barred based on implied consent given their continuing use of  
27 their Gmail accounts, even after discovering Google’s alleged scanning of their emails. *See* note  
28 18, *supra*. Also, CIPA provides for a defense based on consent and should be dismissed on this  
basis, in addition to the CIPA-specific reasons set forth herein. *See* Cal. Penal Code §§ 631-632.

<sup>20</sup> The full text of Sections 631 and 632 are set forth in the attached Appendix of Relevant  
Statutes for the court’s convenience.

1 *Black's Law Dictionary*, 588 (9th ed. 2009) (defining “eavesdropping” as “[t]he act of secretly  
2 listening to the private conversation of others without their consent.”). While Section 632 also  
3 refers to the “record[ing]” of confidential communications, that reference must be interpreted  
4 consistently with the overall statute, which plainly focuses on oral communications. *See* Cal.  
5 Penal Code § 632.

6 Construing these terms, a California court has specifically held that *CIPA does not apply*  
7 *to the automated processing of emails in the Gmail system*. In *Diamond v. Google Inc.*, No.  
8 CIV-1202715, the Marin County Superior Court dismissed the Section 632 claim because the  
9 plaintiff had not explained “how Google could have possibly ‘overheard’ the emails ‘by means of  
10 any electronic amplifying or recording device’” for purposes of the statute. The court also held  
11 that Section 631 cannot be expanded beyond its express limitations to telephone and telegraph  
12 equipment, explaining that “the words ‘telegraph or telephone’ ... can only be reasonably  
13 construed to apply to” Section 631 as a whole. (*See* Wong Decl., Exh. LL at p. 2.) The court thus  
14 dismissed the Section 631 claim because “Plaintiff allege[d] no facts allowing email  
15 communications to be characterized as ‘telephone’ or ‘telegraph’ transmissions.” (*Id.*) The same  
16 common sense analysis should be applied here.

17 Indeed, any contrary interpretation of CIPA as encompassing emails would be nonsensical  
18 because the Legislature could not possibly have contemplated email when it enacted the statute in  
19 1967. As the Supreme Court has long cautioned, “[i]t is not the function of the judiciary, because  
20 of discoveries after the [initial enactment of a statute], to broaden the provisions of that act so that  
21 it will include corporations or companies that were not, and could not have been at that time,  
22 within the contemplation of Congress.” *City of Richmond v. S. Bell Tel. & Tel. Co.*, 174 U.S.  
23 761, 774-776 (1899) (holding that statute applying to “telegraph lines” could not be applied to  
24 telephone technology implemented after the statute’s enactment).<sup>21</sup> Plaintiffs’ claims violate this

25 <sup>21</sup> *See also State v. Komisarjevsky*, No. CR07241860, 2011 WL 1032111, at \*3 (Conn. Super. Ct.  
26 Feb. 22, 2011) (News reports sent via Twitter do not fall within a rule related to “broadcasting”  
27 because the rule predated Twitter and “[c]ourts traditionally have proceeded with caution in  
28 extending old legislation to new technologies.”) (citation omitted); *Deacon v. Pandora Media, Inc.*, 901 F. Supp. 2d 1166, 1172-75 (N.D. Cal. 2012) (statutory terms related to “selling,” “renting” and “lending” music could not be applied to online music streaming because streaming technology could not have been contemplated at the time of the statute’s enactment).

1 basic rule by rewriting CIPA to encompass email technology that simply did not exist when the  
2 statute was enacted.

3 In fact, after CIPA’s initial enactment, *the Legislature specifically considered and*  
4 *rejected proposals to expand the statute to cover emails*. In 1995, the Legislature expanded  
5 Penal Code Section 629 (a related statute to CIPA that regulates interception of communications  
6 by law enforcement) to cover certain types of electronic communications. In considering the bill,  
7 the Senate Judiciary Committee observed that “[i]t is not clear that California law specifically  
8 protects e-mail and other electronic communications from improper interception by either private  
9 parties or law enforcement.” (Wong Decl., Exh. MM at p. 4.) It thus posed the question  
10 “SHOULD, AS A COROLLARY TO THE EXTENSION OF THE WIRETAP LAW [Section  
11 629] TO ELECTRONIC COMMUNICATIONS, THE PRIVACY LAWS [CIPA] BE  
12 AMENDED TO EXPRESSLY PROTECT ELECTRONIC COMMUNICATIONS FROM  
13 INTERCEPTION ....” (*Id.* at 4 (caps in original).) Ultimately, the Legislature opted to amend  
14 *only* Section 629 while declining to expand CIPA in similar fashion. (*Id.*)

15 In 2010, Section 629 was expanded again to cover additional forms of electronic  
16 communications. As the Senate Committee on Public Safety explained, the language of Section  
17 629 at the time—which was already *broad*er than CIPA—still did not cover emails and other  
18 forms of electronic communications. (*See* Wong Decl. Exh. NN (Senate Analysis stating that  
19 “[t]his bill ... updates California’s wiretapping law to include interception of communications by  
20 e-mail, blackberry, instant messaging by phone and other forms of contemporaneous two way  
21 electronic communication.”).) Again, the Legislature decided to amend *only* Section 629, leaving  
22 the limitations of Sections 631 and 632 intact.

23 In sum, the express terms of the statute, the applicable rules of statutory interpretation, and  
24 legislative history all confirm that CIPA does not reach email communications.

## 25 **2. Plaintiffs Also Have No Article III Standing to Pursue a CIPA Claim.**

26 The CIPA Plaintiffs’ claim also fails for an additional and equally fundamental reason:  
27 they allege no facts to show they suffered an injury-in-fact sufficient to confer standing under  
28



1 Article III of the Constitution.<sup>22</sup> While Ninth Circuit authority may be read to permit standing  
2 based on the violation of certain statutory rights without independent allegations of harm, this  
3 applies *only* to statutes that specifically allow persons who meet the express statutory criteria to  
4 bring a claim without any showing of injury. *In re iPhone Application Litig.*, No. 11-md-2250,  
5 2011 WL 4403963, at \*6 (N.D. Cal. Sept. 20, 2011) (finding that plaintiffs had no Article III  
6 standing because they “do not allege a violation of [a] statute which does not require a showing of  
7 injury.”). In contrast, CIPA expressly provides that a civil claim can be brought only by a  
8 “*person who has been injured.*” Cal. Penal Code § 637.2 (emphasis added). Accordingly,  
9 Plaintiffs cannot pursue a CIPA claim without establishing the standing requirements of both  
10 CIPA and Article III.

11 Here, the CIPA Plaintiffs fail to allege any concrete injury stemming from the automated  
12 processing of the emails they sent to the Gmail system. While they vaguely assert that Google  
13 improperly used information contained in their emails, this Court has held that merely alleging  
14 the “collection and tracking of . . . personal information” is insufficient to confer standing under  
15 Article III. *See In re iPhone Application Litig.*, 2011 WL 4403963, at \*5; *see also LaCourt v*  
16 *Specific Media, Inc.*, No. 10-cv-1256, 2011 WL 1661532, at \*3-4 (C.D. Cal. Apr. 28, 2011)  
17 (plaintiffs had no Article III standing to bring claims involving use of Flash cookies to track  
18 Internet activity). Plaintiffs’ allegations here are no different, and their CIPA claim similarly fails  
19 for lack of Article III standing.

### 20 **3. Plaintiffs Also Fail to Allege Any Connection with California.**

21 In addition to alleging injury, the CIPA Plaintiffs must also show that their  
22 communications have some contact with California. Section 631 specifically regulates the  
23 interception of communications “while the same [are] in transit or passing over any wire, line, or  
24 cable, or [are] being sent from, or received at *any place within this state.*” Cal. Penal Code §  
25 631(a) (emphasis added). This same limitation applies to Section 632. *See Kearney v. Salomon*

---

26 <sup>22</sup> Under Article III, “a plaintiff must show (1) it has suffered an ‘injury in fact’ that is (a)  
27 concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the  
28 injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed  
to merely speculative, that the injury will be redressed by a favorable decision.” *Friends of the*  
*Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

1 *Smith Barney, Inc.*, 39 Cal. 4th 95, 119 (2006) (explaining that Section 632 “protect[s] against the  
2 secret recording of any confidential communication that is sent from or received *at any place*  
3 *within California.*”) (emphasis added). Here, the CIPA Plaintiffs (who reside in Alabama and  
4 Maryland) do not allege that any of their emails have any connection to California. For example,  
5 they make no effort to allege that they ever sent a single email to a recipient in California, even  
6 though that information is obviously within their knowledge. The CIPA claims of these Plaintiffs  
7 should be dismissed given this basic failure of pleading.

8 **D. The Section 632 Claim Fails for Additional Reasons.**

9 **1. Plaintiffs Allege no Facts to Show that Their Emails Were**  
10 **“Confidential Communications” within the Meaning of the Statute.**

11 Section 632 applies only to “confidential communication[s],” defined as communications  
12 made “in circumstances” that “reasonably indicate” a “desire[]” that the communications “be  
13 confined to the parties thereto.” Cal. Penal Code § 632(c). This definition excludes  
14 communications made “in any . . . circumstance in which the parties . . . may reasonably expect  
15 that the communication may be overheard or recorded.” *Id.* Applying this requirement, courts  
16 have consistently dismissed Section 632 claims where plaintiffs allege that they subjectively  
17 expected their communications to be confidential, without pleading additional facts to  
18 demonstrate that the communication falls within the scope of Section 632. *See, e.g., Faulkner v.*  
19 *ADT Servs., Inc.*, 706 F.3d 1017, 1021 (9th Cir. 2013) (affirming dismissal of Section 632 claim  
20 where plaintiff alleged that he expected his communication to be confined to the parties, but did  
21 not allege sufficient facts to show he had an “objectively reasonable” expectation that the  
22 communication would not be recorded).<sup>23</sup>

23 Similarly here, the CIPA Plaintiffs claim they had no “knowledge or expectation” that the  
24 emails they sent to Gmail users would be processed by Google. (Compl. at ¶ 316.) But beyond

---

25 <sup>23</sup> *See also Montegna v. Yodle, Inc.*, No. 12-cv-0647, 2012 WL 3069969, at \*3 (S.D. Cal. July 27,  
26 2012)(dismissing Section 632 claim where plaintiff alleged recording of a “confidential”  
27 conversations but failed “to allege any facts regarding [the plaintiffs’] relationship with [the other  
28 parties to the communication]” or “the content or nature of the calls.”); *Weiner v. ARS Nat’l*  
*Servs., Inc.*, 887 F. Supp. 2d 1029, 1033 (S.D. Cal. 2012) (dismissing Section 632 claim where  
plaintiff failed to allege the relationship between the parties to the communication, or that the  
communication contained any “personal information.”)

1 those conclusory assertions, they plead no actual facts to show their emails were sent under  
2 “circumstances” that would “reasonably indicate” a “desire[]” that the emails “be confined to the  
3 parties.” *See* Cal. Penal Code § 632(c). Among other omitted facts, the CIPA Plaintiffs do not  
4 describe the content or nature of a single email they sent to a Gmail user<sup>24</sup>; nor do they describe  
5 their prior experiences with email services to suggest any basis for their expectations.<sup>25</sup> As in  
6 *Faulkner*, “too little is asserted in the complaint about the particular relationship between the  
7 parties, and the particular circumstances of the [communications at issue], to lead to the plausible  
8 conclusion that an objectively reasonable expectation of confidentiality would have attended such  
9 a communication.” 706 F.3d at 1020.

10 **2. Federal Law Preempts Any Claim that an ECS Provider’s Operations**  
11 **Constitute an Illegal “Recording” under Section 632.**

12 As set forth above, ECPA set forth a comprehensive scheme related to ECS providers,  
13 which allows providers of email services like Google to “store” and “access” emails sent to its  
14 systems. In enacting these provisions, Congress expressed specific concern that conflicting state  
15 standards could “discourage potential customers from using innovative communications systems”  
16 and “discourage [ECSs and Remote Computing Services (“RCS”)] from developing new  
17 innovative forms of telecommunications and computer technology.” (Wong Decl., Exh. BB at p.  
18 5.) Reflecting these legislative concerns, courts have found that ECPA preempts overlapping  
19 state law regulations of electronic communications. *See In re Google, Inc. Street View Elec.*  
20 *Commc’ns Litig.*, 794 F. Supp. 2d 1067, 1084-85 (N.D. Cal. 2011) (holding that ECPA preempts  
21 state wiretap statutes because the statute “comprehensively regulate[s] the interception of  
22 electronic communications such that the scheme leaves no room in which the states may further  
23 regulate.”); *Bunnell v. MPAA*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (ECPA preempts  
24 CIPA claim regarding access to emails).

25 Under these standards, Plaintiffs cannot seek to impose liability on Google for “recording”

26 <sup>24</sup> For example, there could be no reasonable expectation of confidentiality if the CIPA Plaintiffs’  
27 emails with Gmail users were sent to large groups of recipients or were sent with the express  
28 expectation that they would be forwarded to others, among other circumstances that would  
preclude application of Section 632.

<sup>25</sup> For example, if Plaintiffs used Yahoo mail, they would have known that automated scanning of  
emails to deliver advertising is a common industry practice not limited to Gmail. *See* n.11, *supra*.

1 the emails that are sent to Gmail recipients because ECPA specifically allows Google to receive  
2 and store electronic such communications in its capacity as an ECS provider. Even if CIPA could  
3 be interpreted to apply to emails at all, Plaintiffs' Section 632 claim based on Google's  
4 "recording" of emails is preempted as a matter of law because it is in direct conflict with federal  
5 law.<sup>26</sup> See *Ting v. AT&T*, 319 F.3d 1126, 1137 (9th Cir. 2003) ("Even where Congress has not  
6 entirely displaced state regulation in a specific area, state law is preempted to the extent that it  
7 actually conflicts with federal law."); *Pub. Util. Dist. No. 1 v. IDACORP, Inc.*, 379 F.3d 641, 650  
8 (9th Cir. 2004) ("Under the obstruction strand of conflict preemption, an aberrant or hostile state  
9 rule is preempted to the extent it actually interferes with the methods by which the federal statute  
10 was designed to reach [its] goal.").

11 **E. The CIPA Claim Should Also be Dismissed under Choice of Law Principles.**

12 Apart from the various defects above, choice-of-law principles preclude the CIPA  
13 Plaintiffs—as residents of Alabama and Maryland—from invoking CIPA and bypassing the law  
14 of their local jurisdictions.<sup>27</sup> Under the "governmental interest" analysis<sup>28</sup>, (1) a court  
15 "determines whether the relevant law of each of the potentially affected jurisdictions" differ, (2)  
16 "if there is a difference, the court examines each jurisdiction's interest in the application of its  
17 own law . . . to determine whether a true conflict exists," and (3) if a true conflict exists, the court  
18 must weigh "the interest of each jurisdiction in the application of its own law to determine which  
19 state's interest would be more impaired if its policy were subordinated to the policy of the other  
20 state . . . ." *Mazza*, 666 F.3d at 590. These standards mandate application of Alabama and  
21 Maryland law here.

22  
23 <sup>26</sup> Plaintiffs also refer in conclusory terms to the "eavesdropping" element of Section 632, but  
cannot seriously contend that the automated processing of emails by computer systems amounts  
to "eavesdropping" on a communication.

24 <sup>27</sup> Choice of law determinations in class actions are routinely resolved at the pleading stage. See,  
25 e.g., *Frezza v. Google, Inc.*, No. 12-cv-0237, 2013 WL 1736788, at \*5 (N.D. Cal. Apr. 22, 2013)  
(stating that *Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581 (9th Cir. 2012) was "not only  
26 relevant but controlling" and dismissing UCL claims because North Carolina law applied); *Banks*  
27 *v. Nissan N. Am., Inc.*, No. 11-cv-2022, 2012 U.S. Dist. LEXIS 37754, at \*3 (N.D. Cal. Mar. 20,  
2012) (dismissing nationwide class action claim predicated on California law because "such  
allegations are inappropriate, pursuant to the Ninth Circuit's reasoning in *Mazza* . . .").

28 <sup>28</sup> "A federal court sitting in diversity must look to the forum state's choice of law rules to  
determine the controlling substantive law." *Mazza*, 666 F.3d 589-90 (citation omitted).

1       ***The potentially applicable laws differ:*** As compared to CIPA, Alabama and Maryland  
2 law are substantially more limited in terms of the scope of liability, enforcement mechanisms, and  
3 available remedies. Under Alabama law, (1) the interception of electronic communications is  
4 permitted where a single party consents, Ala. Code 1975 § 13A-11-30, and (2) enforcement is left  
5 to the discretion of state government, with no right of action for private plaintiffs, Ala. Code 1975  
6 §§ 13A-11-30 to 13A-11-37. In contrast, CIPA requires the consent of all parties to a  
7 communication and allows a private right of action for injured persons. (See above). Maryland  
8 law also differs materially from CIPA. Maryland does not allow claimants to seek injunctive  
9 relief and limits civil recovery to actual damages or “liquidated damages computed at the rate of  
10 \$100 a day for each day of violation or \$1,000, whichever is higher.” Md. Code, Cts. & Jud.  
11 Proc. §10-410(a)(1). In contrast, CIPA allows claimants to seek both injunctive relief and “the  
12 greater of” \$5,000 or three times the amount of any actual damages. Cal. Penal Code § 637.2(a).  
13 In short, CIPA is directly at odds with limitations that Alabama and Maryland have imposed in  
14 their respective statutes governing the interception of communications.

15       ***California has no interest in applying CIPA to the claims of non-residents:*** On its face,  
16 CIPA indicates that its purpose is to protect California residents, not to regulate in-state business  
17 practices that might impact non-Californians: “The Legislature by this chapter *intends to protect*  
18 *the right of privacy of the people of this state.*” Cal. Penal Code § 630 (emphasis added).  
19 Reflecting that statement of legislative purpose, the California Supreme Court has recognized that  
20 “the principal purpose of [CIPA] is to protect the privacy of confidential communications of  
21 *California residents while they are in California.*” *Kearney*, 39 Cal. 4th at 119-120 (italics in  
22 original); *see also Zephyr v. Saxon Mortg. Servs., Inc.*, 873 F. Supp. 2d 1223, 1231 (E.D. Cal.  
23 2012) (“the purpose of [CIPA] does not appear to be to regulate out-of-state commerce or  
24 conduct, but to protect California residents”).<sup>29</sup>

25       This express purpose makes clear that California has no interest in applying CIPA to

---

26  
27       <sup>29</sup> *See also Kearney*, 39 Cal. 4th at 124 (noting that “one of the principal purposes underlying  
28 [CIPA]” was “protecting *individuals in California*”); *id* at 126 (noting “California’s concern for  
the privacy of *the state’s consumers*”); *id.* at 125 (noting that CIPA reflects the Legislature’s  
effort to “increase the protection of *California consumers’* privacy”) (emphases added).

1 claims brought by *non*-California residents, particularly where the communications at issue have  
2 no alleged link to California. This lack of a cognizable state interest is dispositive and precludes  
3 Plaintiffs from relying on California law. *Kearney*, 39 Cal. 4th at 109 (If “only one of the states  
4 has an interest in having its law applied,” there is “no problem in choosing the applicable rule of  
5 law” as the law of the state having an interest.) (citation and quotation omitted)).

6 ***In contrast, Alabama and Maryland have a strong interest in applying their own laws:***

7 As a general matter, “[e]very state has an interest in having its law applied to its resident  
8 claimants.” *Mazza*, 666 F.3d at 591-92 (citation and quotation omitted). Moreover, each state  
9 has a valid “interest in shielding out-of-state businesses from what the state may consider to be  
10 excessive litigation.” *Id.* at 592. As the Ninth Circuit explained:

11 In our federal system, states may permissibly differ on the extent to  
12 which they will tolerate a degree of lessened protection for  
13 consumers to create a more favorable business climate for the  
14 companies that the state seeks to attract to do business in the state  
15 . . . Each of our states also has an interest in being able to assure  
individuals and commercial entities operating within its territory that  
applicable limitations on liability set forth in the jurisdiction’s law  
will be available to those individuals and businesses in the event  
they are faced with litigation in the future.

16 *Id.* at 592-93 (citation and quotation omitted).<sup>30</sup> Given these considerations, the Ninth Circuit  
17 reversed an order applying California law to the claims of non-residents because “[t]he district  
18 court did not adequately recognize that each foreign state has an interest in applying its law to  
19 transactions within its borders and that, if California law were applied to the entire class, foreign  
20 states would be impaired in their ability to calibrate liability to foster commerce.” *Id.* at 593.

21 The same considerations preclude the CIPA Plaintiffs from applying CIPA in place of the  
22 laws of their local jurisdictions. As in *Mazza*, both Alabama and Maryland “would be impaired  
23 in their ability to calibrate liability to foster commerce” if the CIPA Plaintiffs were allowed to  
24 avoid their local laws and assert a CIPA claim. *Id.* For example, even though Alabama has

25 <sup>30</sup> Moreover, the CIPA Plaintiffs’ effort to impose California law on the other 49 states would  
26 violate the Dormant Commerce Clause, particularly as applied to communications that have no  
27 connection to California. *See Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 (1989) (“a statute that  
28 directly controls commerce occurring wholly outside the boundaries of a State exceeds the  
inherent limits of the enacting State’s authority and is invalid regardless of whether the statute’s  
extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical  
effect of the regulation is to control conduct beyond the boundaries of the State.”)

1 decided that its residents should have no private right of action to challenge an alleged  
2 interception, that legislative judgment would be entirely subverted if Alabama residents like  
3 Plaintiff Harrington could bring a CIPA claim. Similarly, the limited remedies specified under  
4 Maryland law would be meaningless if Maryland residents like Plaintiff Brad Scott could simply  
5 ignore those limitations and assert a claim under CIPA. In short, allowing Plaintiffs to bypass the  
6 restrictions of their local laws by invoking CIPA would effectively rob Alabama and Maryland of  
7 any ability to determine the appropriate scope of liability for claims brought by their residents.  
8 *Mazza* precludes this result. *See id.* at 591-94.

9 Indeed, the CIPA Plaintiffs' effort to impose California law on a nationwide class outside  
10 of California is in direct conflict with the claims of other Plaintiffs. While the CIPA Plaintiffs are  
11 seeking to impose CIPA to override all other state wiretapping statutes outside of California,  
12 Plaintiffs Knowles, Brinkman, and Brent Scott have chosen to rely, *not* on CIPA, but on the  
13 wiretapping statutes of their respective states of residence (Maryland, Pennsylvania, and  
14 Florida).<sup>31</sup> (*See* Compl. at ¶¶ 341, 361, 383.) The Court should not allow the CIPA Plaintiffs to  
15 force all non-Gmail users outside of California to rely on CIPA when three of their fellow  
16 Plaintiffs have expressly rejected the application of California law and insisted that local law  
17 must apply to their own claims and the claims of the non-Gmail users in their respective states.

18 **V. CONCLUSION.**

19 For all of the reasons above, Plaintiff's Complaint should be dismissed in its entirety.

20 Dated: June 13, 2013

21 COOLEY LLP  
22 MICHAEL G. RHODES (116127)  
23 WHITTY SOMVICHIAN (194463)  
24 KYLE C. WONG (224021)  
25  
26 /s/ Whitty Somvichian  
27 Whitty Somvichian (194463)  
28 Attorneys for Defendant GOOGLE INC.

1319718/SF

---

31 This inherent conflict is most obvious in the case of Plaintiffs Scott and Knowles. Both are Maryland residents seeking to represent a class that includes non-Gmail users in Maryland – yet Scott seeks to impose CIPA whereas Knowles has chosen to rely on Maryland law.