

United States District Court
Northern District of California

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

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

Case No. 15-CV-04062-LHK

**ORDER DENYING MOTION TO
DISMISS AS TO THE MERITS OF
PLAINTIFF’S CLAIMS**

Re: Dkt. No. 20

Plaintiff Daniel Matera (“Plaintiff”), individually and on behalf of those similarly situated, alleges that Defendant Google Inc. (“Google”) violated federal and state wiretapping laws in its operation of Gmail, an email service. ECF No. 1 (“Compl.”).¹ Before the Court is Google’s motion to dismiss for failure to state a claim. ECF No. 20. Having considered the parties’ submissions, the relevant law, and the record in this case, the Court DENIES Google’s motion to dismiss as to the merits of Plaintiff’s claims. The Court will issue a separate order on standing issues.

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

1 **I. BACKGROUND**

2 **A. Factual Background**

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

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

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

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

26 As relevant to the instant case, the putative class in *Gmail* included a class of all United
27 States non-Gmail users "who have sent a message to a Gmail user and received a reply or received

1 an email from a Gmail user.” *Id.* at *4. Because non-Gmail users exchange emails with Gmail
 2 users, the *Gmail* plaintiffs alleged that non-Gmail users’ communications were subject to the same
 3 interception, scanning, and analysis as Gmail users. The *Gmail* plaintiffs also sought to represent
 4 (1) end users of Cable One, an ISP that contracted with Google to provide Google Apps-related
 5 services to its customers; (2) users of Google Apps for Education; and (3) Gmail users under the
 6 age of majority.

7 **2. Allegations in the Instant Case**

8 This case involves a subset of the *Gmail* putative class. In the instant case, Plaintiff seeks
 9 to represent non-Gmail users “who have never established an email account with Google, and who
 10 have sent emails to or received emails from individuals with Google email accounts.” Compl.
 11 ¶ 32.

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

22 Google allegedly uses the intercepted contents of Gmail messages for the “distinct
 23 purpose” of creating targeted advertisements and user profiles to be stored indefinitely. *Id.* ¶¶ 21,
 24 28. According to Plaintiff, Google utilizes the user profiles “for purposes of selling to paying
 25 customers, and sending to the profiled communicants, targeted advertising based upon analysis of
 26 these profiles.” *Id.* ¶ 1; *see also id.* ¶ 17 (noting that Google “deliver[s] targeted advertisements
 27 based on these [user] profiles”). Plaintiff allegedly did not consent to Google’s processing of
 28

1 Plaintiff's emails for these purposes. *Id.* ¶¶ 3, 7, 8.

2 **B. Procedural History**

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

5 **1. Procedural History of *Gmail***

6 The first case that comprised the *Gmail* multi-district litigation, *Dunbar v. Google, Inc.*,
7 was filed on November 17, 2010 in the Eastern District of Texas. *See Dunbar v. Google, Inc.*, No.
8 10-CV-00194, ECF No. 1 (E.D. Tex. Nov. 17, 2010). On June 27, 2012, upon Google's motion,
9 the case was transferred to the Northern District of California and assigned to the undersigned
10 judge. *See Dunbar v. Google, Inc.*, No. 12-CV-03305, ECF No. 180 (N.D. Cal. July 23, 2012).

11 While *Dunbar* was pending, five other actions involving substantially similar allegations
12 against Google were filed in this District and throughout the country. *See Scott v. Google, Inc.*
13 (*"Scott I"*), No. 12-CV-03413 (N.D. Cal.); *Scott v. Google, Inc.* (*"Scott II"*), No. 12-CV-00614
14 (N.D. Fla.); *A.K. v. Google, Inc.*, No. 12-CV-01179 (S.D. Ill.); *Knowles v. Google, Inc.*, No. 12-
15 CV-02022 (D. Md.); *Brinkman v. Google, Inc.*, No. 12-CV-00699 (E.D. Pa.). On April 1, 2013,
16 the Judicial Panel on Multidistrict Litigation issued a Transfer Order, centralizing *Dunbar* along
17 with the five other actions in the Northern District of California before the undersigned judge. *See*
18 No. 13-MD-02430, ECF No. 1. The Court later related a seventh case to the multi-district
19 litigation, *Fread v. Google, Inc.*, No. 13-CV-01961 (N.D. Cal.). *See* No. 13-MD-02430, ECF No.
20 29.

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

1 Consolidated Complaint on June 13, 2013. *See* No. 13-MD-02430, ECF No. 44.

2 The Court granted in part and denied in part Google’s motion on September 26, 2013. *See*
3 No. 13-MD-02430, ECF No. 69. As relevant here, the Court denied the motion to dismiss as to
4 plaintiffs’ Wiretap Act claim. Specifically, the Court rejected Google’s contention that any
5 alleged interceptions fell within the “ordinary course” of Google’s business and were therefore
6 exempt from anti-wiretapping statutes. Using the tools of statutory interpretation, the Court
7 concluded that the “ordinary course of business” exception was “narrow and designed only to
8 protect electronic communication service providers against a finding of liability under the Wiretap
9 Act where the interception facilitated or was incidental to provision of the electronic
10 communication service at issue.” *Id.* at 13–22.

11 In addition, the Court rejected Google’s argument that all Gmail users had consented to the
12 alleged interceptions based on Google’s terms of service and privacy policy. The Court concluded
13 that the terms of service and privacy policy did not provide sufficient disclosures to show that
14 Gmail users had consented to the alleged interceptions. *Id.* at 22–26. The Court further rejected
15 Google’s contention that all email users had impliedly consented to the alleged interceptions
16 because all email users, including non-Gmail users, understand that such interceptions are part of
17 how emails are transmitted. *Id.* at 27–28.

18 The Court also held that the *Gmail* plaintiffs could proceed on their claims under section
19 631 of CIPA, California’s anti-wiretapping law. *Id.* at 28–40. The Court first found that section
20 631 applies to email, not just to communications passing over telephone and telegraph wires, lines,
21 or cables. The Court also concluded that Google was not exempt from section 631 liability as a
22 “public utility.” Accordingly, the Court denied Google’s motion to dismiss the *Gmail* plaintiffs’
23 section 631 claim.

24 On January 27, 2014, the Court denied Google’s motion to certify the Court’s order on the
25 motion to dismiss for interlocutory appeal under 28 U.S.C. § 1292(b). *Gmail*, 2014 WL 294441,
26 at *4 (N.D. Cal. Jan. 27, 2014). The Court found that the long and tortured history of the *Dunbar*
27 action and the consolidated multi-district litigation suggested that immediate appeal would not

1 materially advance the termination of the litigation. *Id.* The Court also noted that, regardless of
2 the definition of the “ordinary course of business” exception under the Wiretap Act, further factual
3 development would be necessary to determine whether the alleged interceptions of email fell
4 within the “ordinary course” of Google’s business. *Id.* at *3 n.2.

5 On October 25, 2013, the *Gmail* plaintiffs moved for class certification of a damages class
6 under Federal Rule of Civil Procedure 23(b)(3). No. 13-MD-02430, ECF No. 87-26. On March
7 18, 2014, the Court denied class certification. No. 13-MD-02430, ECF No. 158. Specifically, the
8 Court found that the *Gmail* plaintiffs had failed to meet the predominance requirement, which
9 “tests whether proposed classes are sufficiently cohesive to warrant adjudication by
10 representation.” *Id.* The Court concluded that the question of whether the *Gmail* class members
11 had consented to the alleged interceptions needed to be litigated on an individual rather than
12 classwide basis. The Court further concluded that the individualized inquiries into consent would
13 predominate over questions common to the class and thus denied class certification. On May 12,
14 2014, the Ninth Circuit denied the *Gmail* plaintiffs’ petition for interlocutory review of the Court’s
15 class certification order. No. 13-MD-02430, ECF No. 174.

16 After the Court’s order denying class certification, only the claims of individual plaintiffs
17 remained in the *Gmail* litigation. On May 23, 2014, the plaintiffs in *Dunbar*, *Scott I*, *Scott II*,
18 *Knowles*, *Brinkman*, and *Fread* dismissed with prejudice their individual claims in the *Gmail*
19 multidistrict litigation and in their original individual actions. No. 13-MD-02430, ECF No. 175.
20 On July 14, 2014, the plaintiffs in the last case remaining in the multidistrict litigation, *A.K.*,
21 dismissed with prejudice their individual claims in the *Gmail* multidistrict litigation and in their
22 original individual action. No. 13-MD-02430, ECF No. 177.

23 **2. Procedural History in the Instant Case**

24 Plaintiff filed the complaint on September 4, 2015. ECF No. 1. Like the *Gmail* plaintiffs,
25 Plaintiff asserts violations of the ECPA and CIPA. Plaintiff seeks to represent the following
26 classes:

27 CIPA Class (Count One): All persons in the State of California who have never

1 established an email account with Google, and who have sent emails to or
2 received emails from individuals with Google email accounts.

3 ECPA Class (Count Two): All persons in the United States who have never
4 established an email account with Google, and who sent emails to or received
5 emails from individuals with Google email accounts before December 19,
6 2014.

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

9 On October 29, 2015, Google filed the instant motion to dismiss, ECF No. 20 (“Mot.”),
10 and a request for judicial notice, ECF No. 20-1 (“Google RJN”). On December 4, 2015, Plaintiff
11 opposed the motion to dismiss, ECF No. 29 (“Opp.”), and filed a request for judicial notice, ECF
12 No. 31 (“Pl. RJN”). Google replied on December 22, 2015. ECF No. 33 (“Reply.”).

13 The same day that Google filed the instant motion, Google also moved to temporarily stay
14 the case pending the U.S. Supreme Court’s resolution of *Spokeo, Inc. v. Robins*, No. 13-01339.
15 ECF No. 21. Because this Court concluded that *Spokeo* may impact whether Plaintiff has standing
16 to proceed in this action, this Court granted Google’s motion to stay on February 5, 2016. ECF
17 No. 36. On April 28, 2016, this Court set a case management conference for May 25, 2016. ECF
18 No. 37.

19 The U.S. Supreme Court issued an opinion in *Spokeo* on May 16, 2016. *See Spokeo, Inc.*
20 *v. Robins*, 136 S. Ct. 1540 (2016). At the May 25, 2016 case management conference, this Court
21 lifted the stay in the instant case and ordered supplemental briefing as to the impact of *Spokeo* on
22 Plaintiff’s standing. ECF No. 40. The parties filed simultaneous opening supplemental briefs on
23 June 1, 2016. ECF Nos. 41, 42. The parties filed simultaneous reply supplemental briefs on June
24 13, 2016. ECF Nos. 45, 46. This Court will address issues of standing, including the impact of
25 *Spokeo*, in a separate order.

26 **II. LEGAL STANDARD**

27 **A. Rule 12(b)(6) Motion to Dismiss**

28 Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include “a
short and plain statement of the claim showing that the pleader is entitled to relief.” A complaint

1 that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). Rule 8(a) requires a
2 plaintiff to plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl.*
3 *Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff
4 pleads factual content that allows the court to draw the reasonable inference that the defendant is
5 liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility
6 standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a
7 defendant has acted unlawfully.” *Id.* (internal quotation marks omitted).

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

19 **B. Leave to Amend**

20 If the Court concludes that the complaint should be dismissed, it must then decide whether
21 to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to
22 amend “shall be freely given when justice so requires,” bearing in mind “the underlying purpose
23 of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or
24 technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (ellipsis in
25 original). Nonetheless, a district court may deny leave to amend a complaint due to “undue delay,
26 bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by
27 amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of
28

1 the amendment, and futility of amendment.” *See Leadsinger, Inc. v. BMG Music Publ’g*, 512 F.3d
2 522, 532 (9th Cir. 2008) (brackets omitted).

3 **III. JUDICIAL NOTICE**

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

12 Plaintiff asks for judicial notice of the transcript of the November 2, 2015 oral argument
13 before the U.S. Supreme Court in *Spokeo*, as well as a U.S. Senate Report regarding the passage of
14 the ECPA. *See* Pl. RJN. Google requests judicial notice of Google’s public terms of service dated
15 April 14, 2014; Google’s December 19, 2014 privacy policy, which is quoted in the complaint, as
16 well as archived versions of the privacy policy; Google’s website entitled “Updates: Privacy
17 Policy”; two reports from California Senate Committees; and three bills introduced in the
18 California Legislature. *See* Google RJN. Both Plaintiff’s and Google’s requests for judicial
19 notice are unopposed, and the documents therein are the proper subject of judicial notice. *See*
20 *Anderson v. Holder*, 673 F.3d 1089, 1094 n.1 (9th Cir. 2012) (“Legislative history is properly a
21 subject of judicial notice.”); *Lee v. City of Los Angeles*, 250 F.3d 668, 689 (9th Cir. 2001) (matters
22 of public record), *overruled in part on other grounds by Galbraith v. Cty. of Santa Clara*, 307
23 F.3d 119, 1125–26 (9th Cir. 2002); *Caldwell v. Caldwell*, 2006 WL 618511, at *4 (N.D. Cal. Mar.
24 13, 2006) (publicly accessible websites). Accordingly, the Court GRANTS Plaintiff’s and
25 Google’s unopposed requests for judicial notice.

26 **IV. DISCUSSION**

27 Google moves to dismiss Plaintiff’s claims under: (1) the Electronic Communications
28

United States District Court
Northern District of California

1 Privacy Act of 1986 (the “ECPA” or “Wiretap Act”), 18 U.S.C. § 2510 *et seq.*, and (2)
2 California’s Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 630 *et seq.* As to the Wiretap
3 Act, Google claims that the alleged interception, scanning, and analysis of email falls within the
4 “ordinary course of business” exception to liability. Google also requests certification of an
5 interlocutory appeal on this issue to the Ninth Circuit. As to CIPA, Google asks the Court to
6 decline supplemental jurisdiction and contends that CIPA does not apply to electronic
7 communications like email. The Court first addresses Plaintiff’s Wiretap Act claim then
8 Plaintiff’s CIPA claim.

9 **A. Wiretap Act**

10 **1. Ordinary Course of Business**

11 The Wiretap Act generally prohibits the interception of “wire, oral, or electronic
12 communication[s]” through the use of “any electronic, mechanical, or other device.” 18 U.S.C.
13 § 2511(1). In the instant case, Plaintiff contends that Google violated the Wiretap Act in its
14 operation of the Gmail system by intentionally intercepting the content of emails in order to create
15 user profiles and to provide targeted advertising. Google counters that Plaintiff has not stated a
16 claim with respect to the Wiretap Act because the alleged interceptions fall within the “ordinary
17 course of business” exception to the definition of “any electronic, mechanical, or other device.”
18 Under that exception, “any telephone or telegraph instrument, equipment or facility, or any
19 component thereof . . . being used by a provider of wire or electronic communication service in the
20 ordinary course of its business” is not a “device,” and the use of such an instrument is not
21 prohibited by the Wiretap Act. *Id.* § 2510(5)(a)(ii).

22 Specifically, Google contends that any interception of Plaintiff’s emails occurred in the
23 ordinary course of Google’s business. Google asks the Court to reconsider *Gmail*, which held that
24 the “ordinary course of business” exception “offers protection from liability only where an
25 electronic communication service provider’s interception facilitates the transmission of the
26 communication at issue or is incidental to the transmission of such communication.” *Gmail*, 2013
27 WL 5423918, at *8. The Court first addresses the “ordinary course of business” exception and

United States District Court
Northern District of California

1 *Gmail*'s interpretation of that exception, then addresses Google's challenge to that interpretation.

2 As noted above, the Wiretap Act prohibits the interception of "wire, oral, or electronic
3 communication[s]" through the use of "any electronic, mechanical, or other device." 18 U.S.C.
4 § 2511(1). Specifically, a Wiretap Act violation exists when any person "intentionally intercepts,
5 endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire,
6 oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see also id.* § 2520 (creating a private
7 right of action for violations of § 2511). The Wiretap Act defines "intercept" as "the aural or other
8 acquisition of the contents of any wire, electronic, or oral communication through the use of any
9 electronic, mechanical, or other device." 18 U.S.C. § 2510(4). However, the definition of
10 "electronic, mechanical, or other device" excludes devices:

- 11 (i) furnished to the subscriber or user by a provider of wire or electronic
12 communication service in the ordinary course of its business and being used by the
13 subscriber or user in the ordinary course of its business or furnished by such
14 subscriber or user for connection to the facilities of such service and used in the
15 ordinary course of its business; or
- 16 (ii) being used by a provider of wire or electronic communication service in the
17 ordinary course of its business, or by an investigative or law enforcement officer in
18 the ordinary course of his duties;

19 *Id.* § 2510(5)(a). Accordingly, the Wiretap Act includes two "ordinary course of business"
20 exceptions. The first, under subsection (a)(i), is for users or subscribers of electronic
21 communication services while the second, subsection (a)(ii), applies to the providers of electronic
22 communication services. This case implicates the latter, as Google provides the electronic
23 communication service at issue here, Gmail.

24 The Ninth Circuit has not yet ruled on the scope of the "ordinary course of business"
25 exception in subsection (a)(ii). In *Gmail*, however, the Court analyzed subsection (a)(ii) and
26 rejected Google's contention that any interception of email in that case fell within the "ordinary
27 course" of Google's business. Analyzing the text of the statute, the statutory scheme, case law,
28 and legislative history, the Court concluded that the ordinary course of business exception
protected electronic communication service providers from liability where the interceptions
"facilitated or [were] incidental to provision of the electronic communication service at issue."

United States District Court
Northern District of California

1 *Gmail*, 2013 WL 5423918, at *11. In other words, the Court concluded that there “must be some
2 nexus between the need to engage in the alleged interception and the [provider’s] ultimate
3 business, that is, the ability to provide the underlying service or good.” *Id.*

4 The Court then found that the *Gmail* plaintiffs had plausibly alleged that there was no
5 nexus between Google’s provision of Gmail and the alleged interception and scanning of email for
6 advertising purposes. The Court noted that the *Gmail* plaintiffs alleged that Google’s
7 interceptions of email were “for Google’s own benefit in other Google services unrelated to the
8 service of email or the particular user” and thus “the alleged interception of emails at issue here is
9 both physically and purposively unrelated to Google’s provision of email services.” *Id.* (brackets
10 omitted).

11 In the instant case, similar to *Gmail*, Plaintiff alleges that Google intercepts, scans, and
12 analyzes Plaintiff’s in-transit email for Google’s commercial purposes. Google concedes that the
13 processing of emails alleged here is not within the “ordinary course of business” exception as
14 interpreted by the Court in *Gmail*. However, Google asks the Court to reconsider *Gmail*.
15 Specifically, Google challenges the *Gmail* Court’s interpretation of: (1) the plain meaning of the
16 Wiretap Act, (2) applicable case law, and (3) the statutory scheme. In addition, Google argues
17 that, under the *Gmail* interpretation, the alleged interception, scanning, and analysis of email in the
18 instant case has a sufficient nexus to Google’s business to fall within the “ordinary course of
19 business” exception. The Court addresses these challenges in turn.

20 **a. Plain Meaning**

21 Google contends that the plain meaning of the “ordinary course of business” exception
22 must encompass more than the conduct necessary to the transmission of an electronic
23 communication. Relying on two dictionaries, Google defines “ordinary” as “normal” or “usual”
24 and “business” as “the activity of making, buying, or selling goods or providing services in
25 exchange for money.” Mot. at 9. Based on these definitions, Google contends that Google “need
26 only show that its Gmail-related practices are supported by a legitimate or valid business purpose
27 in order to take advantage of the ‘ordinary course of business’ exception.” *Id.* at 10, 14.

1 The Court disagrees. As the Court stated in *Gmail*, “the presence of the modifier
2 ‘ordinary’ must mean that not everything Google does in the course of its business would fall
3 within the exception.” *Gmail*, 2013 WL 5423918, at *8. Thus, not every practice that is routine
4 or legitimate will fall within the scope of the “ordinary course of business.” *See id.* To give effect
5 to the word “ordinary,” the Court in *Gmail* concluded that the “ordinary course of business”
6 exception applies when there is “some nexus between the need to engage in the alleged
7 interception and the [provider’s] ultimate business, that is, the ability to provide the underlying
8 service or good.” *Id.* at *11.

9 Following *Gmail*, Chief Judge Phyllis Hamilton of this district analyzed the “ordinary
10 course of business” exception and adopted the same “nexus” requirement as *Gmail*. *Campbell v.*
11 *Facebook Inc.*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014). In the instant motion, Google contends
12 that Chief Judge Hamilton adopted a unique view of the “ordinary course of business” exception.
13 Mot. at 17–18; Reply at 11. Upon review of *Campbell*, however, the Court finds no support for
14 Google’s position. Chief Judge Hamilton specifically “agree[d] with the *Gmail* court’s finding
15 that there must be ‘some nexus between the need to engage in the alleged interception and the
16 subscriber’s ultimate business, that is, the ability to provide the underlying service or good.’”
17 *Campbell*, 77 F. Supp. 3d at 844. In addition, like this Court in *Gmail*, Chief Judge Hamilton
18 found that the defendant in that case failed to “indicate a nexus between [the defendant’s] alleged
19 scanning of users’ private messages for advertising purposes and its ability to provide its service.”
20 *Id.*

21 Moreover, Chief Judge Hamilton rejected an interpretation similar to the one offered by
22 Google here. As Chief Judge Hamilton explained, “the statute’s inclusion of the word ‘ordinary’
23 implies some limits on a company’s ability to self-define the scope of the exception. An
24 electronic communications service provider cannot simply adopt any revenue-generating practice
25 and deem it ‘ordinary’ by its own subjective standard.” *Id.* If it were otherwise, an electronic
26 communication service provider could claim that any activity routinely undertaken for a business
27 purpose is within the ordinary course of business, no matter how unrelated the activity is to the

1 provision of the electronic communication service. *See id.* As Chief Judge Hamilton noted, such
2 a reading of the “ordinary course of business” exception is untenable, and would permit electronic
3 communication service providers to effectively exempt themselves from the Wiretap Act. *See id.*

4 The reading of the “ordinary course of business” exception adopted in *Gmail* and
5 *Campbell* is supported by examining the full text of the “ordinary course of business” exception,
6 which exempts from interception any devices “being used *by a provider of wire or electronic*
7 *communication service* in the ordinary course of *its* business.” 18 U.S.C. § 2510(5)(a)(ii)
8 (emphases added). This phrase suggests that Google’s exemption from the Wiretap Act’s
9 prohibition on interception is limited to “its” business as “a provider of . . . electronic
10 communication service.” *Id.*; *see also Campbell*, 77 F. Supp. 3d at 844 (noting that the “use of the
11 word ‘its’ indicates that the court must consider the details of [the electronic communication
12 provider’s] business”). The interpretation of the “ordinary course of business” exception adopted
13 in *Gmail* and *Campbell*, which requires “some nexus between the need to engage in the alleged
14 interception and the [provider’s] ultimate business, that is, the ability to provide the underlying
15 service or good,” thus gives effect to the word “ordinary” as well as to the business of the
16 electronic communication service provider.

17 This Court is not persuaded otherwise by Google’s citation to *In re Google, Inc. Privacy*
18 *Policy Litigation* (“*Google Privacy*”), 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013). In *Google*
19 *Privacy*, the plaintiffs challenged the introduction of a new Google privacy policy that permitted
20 the combination of personal information collected from different Google services—Google search,
21 Gmail, YouTube, Google Maps, Picasa, etc.—in order to create a single user profile. The
22 plaintiffs alleged that this commingling violated the Wiretap Act, and Google moved to dismiss on
23 the basis of the “ordinary course of business” exception. In *Google Privacy*, former U.S.
24 Magistrate Judge Paul Grewal rejected a “narrow read” of the exception that would be “limited to
25 only action taken to deliver the electronic communication.” *Id.* at *10. Instead, Magistrate Judge
26 Grewal found that “Congress specifically chose the broader term ‘business’ that covers more
27 farranging activity.” *Id.* Magistrate Judge Grewal also stated that Congress’s pairing of the term

1 “business” with the terms “ordinary course” further “suggest[ed] an interest in protecting a
2 provider’s customary and routine business practices.” *Id.* Accordingly, Magistrate Judge Grewal
3 found that “the ‘ordinary course of business’ exception is not limited to actions necessary to
4 providing the electronic communication services.” *Id.*

5 The Court respectfully disagrees with *Google Privacy*. As this Court found in *Gmail* and
6 Chief Judge Hamilton found in *Campbell*, the plain meaning of the text of the exception requires a
7 different reading of the “ordinary course of business.” Magistrate Judge Grewal’s reading of the
8 “ordinary course of business” exception to encompass any customary and routine business
9 practice, regardless of the nexus to the electronic communication service, gives too little weight to
10 the word “ordinary” as well as to the electronic service provider’s particular business. *See*
11 *Campbell*, 77 F. Supp. 3d at 844; *Gmail*, 2013 WL 5423918, at *8. In addition, such a reading
12 permits an electronic communication service provider like Google to unilaterally adopt any
13 revenue-generating business practice, deem it “routine,” and exempt itself from the Wiretap Act.
14 As Chief Judge Hamilton noted, it is untenable for electronic communication service providers to
15 “self-define” the scope of their exemption from Wiretap Act liability. *See Campbell*, 77 F. Supp.
16 3d at 844. Thus, Magistrate Judge Grewal’s interpretation of the “ordinary course of business”
17 exception is not supported by the text’s plain meaning.

18 Moreover, the Court in *Gmail* and in the instant case exhaustively addresses applicable
19 case law as well as the statutory scheme. By contrast, Magistrate Judge Grewal’s *Google Privacy*
20 ruling does not mention the statutory scheme and relies on only two cases construing the “ordinary
21 course of business” exception, *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012),
22 and *Hall v. Earthlink Network, Inc.*, 396 F.3d 500 (2d Cir. 2005). The Court in *Gmail* and in the
23 instant case extensively analyzes both *Kirch* and *Hall*, and finds that these cases support the *Gmail*
24 and *Campbell* courts’ interpretation of the “ordinary course of business” exception. Further, the
25 Court in *Gmail* and in the instant case finds that additional case law and the statutory scheme—not
26 addressed by Magistrate Judge Grewal in *Google Privacy*—support the *Gmail* and *Campbell*
27 courts’ interpretation of the “ordinary course of business” exception. *Kirch*, *Hall*, additional

1 applicable case law, and the statutory scheme are discussed further in sections IV.A.1.b–d below.

2 In sum, under the plain meaning of the Wiretap Act, the “ordinary course of business”
3 exception protects an electronic communication service provider’s interception of email where
4 there is “some nexus between the need to engage in the alleged interception and the [provider’s]
5 ultimate business, that is, the ability to provide the underlying service or good.” *Gmail*, 2013 WL
6 5423918, at *11. The Court next addresses the case law supporting this interpretation of the
7 “ordinary course of business” exception.

8 **b. Applicable Case Law: *Kirch* and *Hall***

9 Google contends that two cases support reading the “ordinary course of business”
10 exception to encompass all of an electronic communication service provider’s routine business
11 practices: *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), and *Hall v.*
12 *Earthlink Network, Inc.*, 396 F.3d 500 (2d Cir. 2005). This Court relied on both of these cases in
13 *Gmail* to conclude that not all interceptions of email by an electronic communication service
14 provider fall within the “ordinary course of business” exception.

15 In *Kirch*, the Tenth Circuit affirmed a grant of summary judgment in favor of Embarq, an
16 ISP, where Embarq had intercepted only data incidental to its provision of the internet service. In
17 that case, Embarq placed a device on its servers that redirected users’ Internet traffic to a third-
18 party company, NebuAd, which tracked the websites that Embarq’s users visited and used that
19 information to target ads. 702 F.3d at 1247. The Tenth Circuit held that Embarq had not violated
20 the Wiretap Act because the ISP could not be liable for NebuAd’s interceptions. *Id.* at 1249.
21 Further, Embarq itself did not review any of the raw data that NebuAd collected. *Id.* at 1250.
22 Rather, Embarq had “access to no more of its users’ electronic communications” than Embarq
23 necessarily had as an ISP. *Id.* Because Embarq’s ordinary course of business as an ISP required
24 Embarq to have access to data that was transmitted over its equipment, the Tenth Circuit
25 concluded that “Embarq’s access [to the data] was in the ordinary course of its core business *as an*
26 *ISP transmitting data over its equipment.*” *Id.* at 1249–50 (emphasis added). In *Gmail*, the Court
27 found that “*Kirch* stands only for the narrow proposition that interceptions incidental to the

1 provision of the alleged interceptor’s internet service fall within the ‘ordinary course of business’
2 exception.” *Gmail*, 2013 WL 5423918, at *8.

3 Google counters that the “ordinary course of business” exception as interpreted by *Kirch*
4 exempts all of an ISP’s routine and legitimate business practices from the Wiretap Act. According
5 to Google, the Tenth Circuit found that Embarq’s interception of user data fell within Embarq’s
6 “ordinary course of business” even though Embarq “extracted a subset of the data for purposes of
7 delivering targeted advertisements.” Mot. at 13. However, Google misreads *Kirch*. Embarq did
8 *not* extract any user data for purposes of delivering targeted advertisements. Indeed, it was crucial
9 to the Tenth Circuit’s analysis that “the only access Embarq had to the data *extracted by NebuAd*
10 was in its capacity as an ISP, not because of any special relationship with NebuAd or the
11 [extraction of data by NebuAd].” *Kirch*, 702 F.3d at 1249 (emphasis added).

12 Further, the Tenth Circuit construed the “ordinary course of business” exception to apply
13 only to interceptions incidental to the provision of the internet service: “Embarq’s access was in
14 the ordinary course of its core business *as an ISP transmitting data over its equipment*” and “in the
15 ordinary course of *providing Internet services as an ISP*.” *Id.* at 1246, 1249 (emphases added).
16 The Tenth Circuit did not mention the reasoning of the district court below, which did not reach
17 the issue of Embarq’s “ordinary course of business” defense but nonetheless stated in dicta that the
18 defense “appears to have merit” because Embarq’s actions “further legitimate business purposes
19 and . . . behavioral advertising is a widespread business and is commonplace on the Internet.” *See*
20 *Kirch*, 2011 WL 3651359, at *9 n.42 (D. Kan. Aug. 19, 2011). Instead, the Tenth Circuit focused
21 on Embarq’s provision of a communication service and—as this Court did in *Gmail*—analyzed
22 whether the alleged interception facilitated or was incidental to Embarq’s provision of that service.
23 *See Kirch*, 702 F.3d at 1249 (noting that “Embarq’s access was in the ordinary course of its core
24 business *as an ISP transmitting data over its equipment*” (emphasis added)). Accordingly, *Kirch*
25 “stands only for the narrow proposition that interceptions incidental to the provision of the alleged
26 interceptor’s internet service fall within the ‘ordinary course of business’ exception.” *Gmail*, 2013
27 WL 5423918, at *8.

1 In the second case relied upon by Google, *Hall*, the plaintiff had a dispute with his ISP,
2 Earthlink, that resulted in the termination of the plaintiff's email account. However, Earthlink
3 continued to receive emails that were sent to the user's address even after the termination, and the
4 user complained that the receipt of email constituted an unlawful "interception" under the Wiretap
5 Act. *Hall*, 396 F.3d at 502. The Second Circuit affirmed a grant of summary judgment in favor of
6 Earthlink because Earthlink's continued receipt of emails was within the ordinary course of
7 business. *Id.* at 505. The Second Circuit noted that Earthlink "used its routers, servers and other
8 computer equipment as part of its e-mail service to all customers, including [plaintiff]." *Id.* In
9 addition, Earthlink presented testimony that Earthlink routinely continued to receive and store
10 emails after an account was canceled and more critically that Earthlink "did not have the ability to
11 bounce e-mail back to senders after the termination of an account." *Id.* Accordingly, the alleged
12 interceptions in *Hall* were an incidental part of Earthlink's ability to provide email services.

13 Google interprets *Hall* to apply the "ordinary course of business" exception to any standard
14 business practice, whether or not the practice is necessary to providing the electronic
15 communication service. Mot. at 12. *Hall*, however, does not support Google's argument. As
16 stated above, the Second Circuit noted that the devices used to "intercept" the plaintiff's email
17 were the same as those "used . . . as part of [Earthlink's] e-mail service to all customers." *Hall*,
18 396 F.3d at 505. Moreover, the Second Circuit specifically noted that Earthlink "did not have the
19 ability to bounce e-mail back to senders after the termination of an account." *Id.* (expressing
20 concern that ISPs would be liable for provision of "their basic services"). These statements
21 demonstrate that the Second Circuit relied upon the fact that Earthlink's receipt of Plaintiff's email
22 was part of and incidental to Earthlink's provision of email services.

23 In both *Kirch* and *Hall*, the only information to which the defendant ISPs had access was
24 collected by the devices that provided internet or email services. *Kirch*, 702 F.3d at 1250; *Hall*,
25 396 F.3d at 505. By contrast, Plaintiff here alleges that Google used devices "separate from the
26 devices that are instrumental to sending and receiving email" to intercept, scan, and analyze the
27

1 putative class’s emails.² Compl. ¶¶ 1, 19, 22–23. Thus, Google is thus less like Embarq or
 2 Earthlink and more akin to NebuAd, the third party in *Kirch* that intercepted data for the purpose
 3 of providing targeted advertising—a purpose separate and apart from the provision of internet
 4 service. *Cf. Kirch*, 702 F.3d at 1248. Because NebuAd settled with the plaintiffs in *Kirch*, the
 5 Tenth Circuit’s opinion does not deal with NebuAd’s liability. *Id.* at 1248 n.2, 1249 (“[W]e need
 6 not address whether NebuAd intercepted any of the Kirches’ electronic communications.”).
 7 However, both *Kirch* and *Hall* exempted ISPs from liability where the alleged interceptions were
 8 incidental to the provision of the ISP’s internet or email service. Accordingly, the Court finds that
 9 *Kirch* and *Hall* support the Court’s construction of the “ordinary course of business” exception in
 10 *Gmail*, which found that the exception applies “only where an electronic communication service
 11 provider’s interception facilitates the transmission of the communication at issue or is incidental to
 12 the transmission of such communication.” *Gmail*, 2013 WL 5423918, at *8.

13 **c. Applicable Case Law: Cases Interpreting § 2510(5)(a)(i) of the Wiretap Act**

14 In addition to challenging the Court’s interpretation of *Kirch* and *Hall*, Google takes issue
 15 with the citations in *Gmail* to decisions construing the “ordinary course of business” exception of
 16 § 2510(5)(a)(i), which applies to users and subscribers of electronic communication services.
 17 Mot. at 13–14. By contrast, as noted above, Google is covered by subsection (a)(ii), which applies
 18 to electronic communication service providers. Google contends that the “far different context of
 19 the[] cases” interpreting subsection (a)(i) limits their relevance, and, regardless, that the subsection
 20

21 _____
 22 ² On April 30, 2014, Google ceased intercepting, scanning, and analyzing, for advertising
 23 purposes, the contents of emails transmitted via Google Apps for Education. *See Corley v.*
 24 *Google, Inc.*, 16-CV-00473-LHK, ECF No. 73 at 17 (N.D. Cal.) (statement of Google).
 25 Accordingly, it appears that Google is able to provide the Gmail service without intercepting,
 26 scanning, and analyzing the content of email for advertising purposes.

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

1 (a)(i) cases do not support the reading of the “ordinary course of business” exception adopted in
2 *Gmail*.

3 In *Gmail*, the Court noted that in the context of subsection (a)(i), “courts have held,
4 consistent with the textual limitation that ‘ordinary’ imposes on ‘course of business,’ that not
5 everything that a company may want to do falls within the ‘ordinary course of business’
6 exception.” *Gmail*, 2013 WL 5423918, at *8. This reading of the “ordinary course of business”
7 exception is clearly supported by the cases cited in *Gmail*. See *Watkins v. L.M. Berry & Co.*, 704
8 F.2d 577, 582 (11th Cir. 1983) (“The phrase ‘in the ordinary course of business’ cannot be
9 expanded to mean anything that interests a company.”); *Adams v. City of Battle Creek*, 250 F.3d
10 980, 984 (6th Cir. 2001) (providing that the “ordinary course of business” requires that a device’s
11 use be “for a legitimate business purpose,” “routine,” and “with notice”); *Arias v. Mut. Cent.*
12 *Alarm Serv., Inc.*, 202 F.3d 553, 559 (2d Cir. 2000) (finding ordinary course of business exception
13 applied when “[l]egitimate business reasons” supported the challenged activity); *Berry v. Funk*,
14 146 F.3d 1003, 1009 (D.C. Cir. 1998) (noting that the challenged business practice must “be
15 justified by a valid business purpose” or “at least must be shown to be undertaken normally”).

16 Google, by contrast, reads the subsection (a)(i) cases to define “ordinary” as “legitimate”
17 and “routine,” and thus contends that routine business practices justified by a business purpose fall
18 within the “ordinary course of business.” However, as the Court explained in *Gmail*, the
19 subsection (a)(i) cases suggest that a business practice is “legitimate” (and thus within the
20 “ordinary course of business”) only when there is “some nexus between the need to engage in the
21 alleged interception and the subscriber’s ultimate business, that is, the ability to provide the
22 underlying service or good.” *Gmail*, 2013 WL 5423918, at *11. For example, in *Arias*, the
23 Second Circuit found that it was within an alarm company’s ordinary course of business to record
24 all incoming and outgoing calls because maintaining records of the calls was instrumental “to
25 ensure that [the alarm company’s] personnel are not divulging sensitive customer information, that
26 events are reported quickly to emergency services, that customer claims regarding events are
27 verifiable, and that the police and other authorities may rely on these records in conducting any

1 investigations.” 202 F.3d at 559 (internal quotation marks and alterations omitted).

2 Similarly, the Tenth Circuit addressed an employer’s installation of a telephone monitoring
3 device on the phone lines in departments where employees interacted with the public. *James v.*
4 *Newspaper Agency Corp.*, 591 F.2d 579 (10th Cir. 1979). The Tenth Circuit concluded that such
5 activity was within the employer’s ordinary course of business because of “concern by
6 management over abusive language used by irate customers when called upon to pay their bills,
7 coupled with the possible need to give further training and supervision to employees dealing with
8 the public.” *Id.* at 581. In other words, both the Second and Tenth Circuits analyzed whether a
9 nexus existed between the challenged interception and the defendant’s business.

10 As another example, in *Watkins*, the Eleventh Circuit addressed a situation in which an
11 employer listened in on an employee’s personal phone call wherein the employee discussed a job
12 interview. The Eleventh Circuit held that an employer could only listen to an employee’s phone
13 call for the purpose of determining whether a call is for personal or business purposes, and thus
14 the employer “was obliged to cease listening as soon as she had determined that the call was
15 personal, regardless of the contents of the legitimately heard conversation.” *Watkins*, 704 F.2d at
16 584. Applying that principle, the Eleventh Circuit found that the alleged interception was not
17 within the employer’s ordinary course of business even though the conversation was “obviously of
18 interest and concern to [the employer].” *Id.* at 582–83.

19 Likewise, the Sixth Circuit in *Berry* rejected “the general principle that any call whose
20 subject is business, if monitored, is necessarily done in the ordinary course of business even if not
21 authorized by a company monitoring policy and not known to employees.” *Berry*, 146 F.3d at
22 1009. Thus, examining the facts of the subsection (a)(i) cases reveals that an employer’s
23 interception of communications falls within the “ordinary course of business” only when the
24 interception has a nexus to the defendant’s ability to provide the underlying service, not when the
25 interceptions serve any conceivable business purpose. This limitation, applied to electronic
26 communication service providers in the context of subsection (a)(ii), means that the “ordinary
27 course of business” exception applies if the electronic communication service provider

United States District Court
Northern District of California

1 “demonstrate[s] the interception facilitated the communication service or was incidental to the
2 functioning of the provided communication service.”³ *Gmail*, 2013 WL 5423918, at *8.

3 **d. Statutory Scheme**

4 Google next challenges *Gmail*’s interpretation of the statutory scheme. The Court in
5 *Gmail* highlighted another provision of the Wiretap Act, 18 U.S.C. § 2511(2)(a)(i), which
6 provides protection for individual employees of a communication service provider. This section
7 provides:

8 It shall not be unlawful under this chapter for an operator of a switchboard, or an
9 officer, employee, or agent of a provider of wire or electronic communication
10 service, whose facilities are used in the transmission of a wire or electronic
11 communication, to intercept, disclose, or use that communication in the normal
12 course of his employment while engaged in any activity which is a necessary
incident to the rendition of his service or to the protection of the rights or property
of the provider of that service, except that *a provider of wire communication
service to the public shall not utilize service observing or random monitoring
except for mechanical or service quality control checks.*

13 18 U.S.C. § 2511(2)(a)(i) (emphasis added). Google points out that the Court in *Gmail*
14 erroneously stated that the limitation in this section on the use of “service observing or random
15 monitoring” applies to electronic communication service providers, when this limitation applies
16 only to wire communication service providers. *See Gmail*, 2013 WL 5423918, at *9. However,
17 the distinction between wire and electronic communication service providers in this section is less
18 important than the distinction between activities that are, or are not, incidental to the provision of
19 the communication service. This second distinction is reflected in the ECPA’s legislative history:

20 In applying the second clause only to wire communications, this provision reflects
21 an important technical distinction between electronic communications and
22 traditional voice telephone service. The provider of *electronic communications*

23 ³ The Court notes that the subsection (a)(i) cases address when interception is within the ordinary
24 course of an electronic communication service *user’s* ordinary course of business. *See, e.g., Arias*,
25 202 F.3d at 559 (discussing ordinary course of business of an alarm company); *Berry*, 146 F.3d at
26 1005–06, 1010 (discussing the business practice of the State Department operations center in
27 monitoring telephone calls). By contrast, the subsection applicable to electronic communication
28 service providers like Google, subsection (a)(ii), refers to *the electronic communication service
provider’s* ordinary course of business. *Kirch* and *Hall*, discussed above, analyzed subsection
(a)(ii). Both *Kirch* and *Hall* stand for the proposition that interceptions that facilitated or were
incidental to the provision of the electronic communication service fall within the “ordinary course
of business” exception.

1 *services may have to monitor a stream of transmissions in order to properly route,*
 2 *terminate, and otherwise manage the individual messages they contain. These*
 3 *monitoring functions, which may be necessary to the provision of an electronic*
 4 *communication service, do not involve humans listening in on voice conversations.*
 5 *Accordingly, they are not prohibited. In contrast, the traditional limits on service*
 6 *“observing” and random “monitoring” do refer to human aural interceptions and*
 7 *are retained with respect to voice or “wire” communications.*

8 Pl. RJN Ex. B, at 20. As the Court noted in *Gmail*, this legislative history “suggests that Congress
 9 intended to protect electronic communication service providers from liability when the providers
 10 were monitoring communications for the purposes of ensuring that the providers could
 11 appropriately route, terminate, and manage messages.” *Gmail*, 2013 WL 5423918, at *10. It does
 12 not suggest that Congress intended to provide protection from liability for any interception that
 13 benefits an electronic communication service provider’s business model. Accordingly, the Court
 14 finds that § 2511(2)(a)(i) supports interpreting the “ordinary course of business” exception in
 15 § 2510(5)(a)(ii) to require an electronic communication service provider to “show some link
 16 between the alleged interceptions at issue and its ability to operate the communication system.”
 17 *Id.*

18 In sum, having considered Google’s arguments, the Court concludes that the Court’s
 19 interpretation of the “ordinary course of business” exception in *Gmail* is correct. The plain
 20 language of the “ordinary course of business” exception, the applicable case law, and the statutory
 21 scheme do not support reading the “ordinary course of business” exception to apply to any
 22 interceptions that serve any conceivable business purpose. Rather, the exception offers protection
 23 from liability “only where an electronic communication service provider’s interception facilitates
 24 the transmission of the communication at issue or is incidental to the transmission of such
 25 communication” and there is “some nexus between the need to engage in the alleged interception
 26 and the [provider’s] ultimate business, that is, the ability to provide the underlying service or
 27 good.” *Gmail*, 2013 WL 5423918, at *8, *11.

28 **e. Existence of a Nexus**

Assuming that *Gmail*’s interpretation of the “ordinary course of business” exception
 applies, Google contends that there is a nexus between the interceptions alleged here and Google’s

United States District Court
Northern District of California

1 ability to provide Gmail. According to Google, the alleged interception of email enables Google
2 to provide targeted advertising, which in turn generates the revenue necessary for Google to
3 provide Gmail. Mot. at 15. Google further contends that “the use of data to target ads is routine
4 and legitimate commercial behavior.” *Id.*

5 On a motion to dismiss, the Court “accept[s] factual allegations in the complaint as true
6 and construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek*, 519
7 F.3d at 1031. Plaintiff alleges that Google intercepts emails for purposes of creating user profiles
8 and targeting advertising through “distinct piece[s] of Google’s infrastructure” that are “separate
9 from the devices that are instrumental to sending and receiving email.” Compl. ¶¶ 2, 19. Plaintiff
10 further alleges that Google “intercepts Gmail for the distinct purpose of acquiring and retaining
11 user data and creating targeted advertising,” which is separate from “the functioning of the
12 provided communication service.” *Id.* ¶ 28. Taking the foregoing as true, Plaintiff plausibly
13 alleges that Google’s alleged interceptions neither facilitate the provision of email services, nor are
14 they an incidental effect of providing these services. Thus, at the motion to dismiss stage, the
15 Court can not say that Google’s alleged interception of email is within the “ordinary course of
16 business” as a matter of law.

17 Moreover, on April 30, 2014, Google ceased intercepting, scanning, and analyzing, for
18 advertising purposes, the contents of emails transmitted via Google Apps for Education. *See*
19 *Corley*, 16-CV-00473-LHK, ECF No. 73 at 17 (statement of Google). Accordingly, Google is
20 able to provide the Gmail service to at least some users without intercepting, scanning, and
21 analyzing the content of email for advertising purposes. This strongly suggests that the alleged
22 interception, scanning, and analysis of email neither facilitates nor is incidental to the provision of
23 Google’s electronic communication service. Plaintiff plausibly alleges that Google’s alleged
24 interceptions of email are outside of the ordinary course of Google’s business.

25 For the reasons stated above, Google’s motion to dismiss Plaintiff’s Wiretap Act claim is
26 DENIED. *See Gmail*, 2013 WL 5423918, at *11 (denying motion to dismiss when “the alleged
27 interception of emails at issue here is both physically and purposively unrelated to Google’s
28

1 provision of email services”); *Campbell*, 77 F. Supp. 3d at 844 (denying motion to dismiss when
 2 “the court cannot find any facts alleged in the complaint or facts presented by Facebook that
 3 indicate a nexus between Facebook’s alleged scanning of users’ private messages for advertising
 4 purposes and its ability to provide its service”); *Dunbar v. Google, Inc.*, 2011 WL 12907501, at *4
 5 (E.D. Tex. May 23, 2011) (“The applicability of the ‘ordinary course of business’ exception
 6 therefore cannot be resolved at the pleading stage.”).

7 **2. Interlocutory Appeal**

8 Should the Court deny Google’s motion to dismiss Plaintiff’s Wiretap Act claim, Google
 9 asks the Court to certify the following question to the Ninth Circuit: “Whether Google’s
 10 automated scanning of emails in providing Google services falls within the ‘ordinary course of its
 11 business’ exception, 18 U.S.C. § 2510(a)(ii), to the Wiretap Act.” Mot. at 16. The Court may, in
 12 its discretion, certify an interlocutory order for appellate review when the Court is of “the opinion
 13 that such order involves a controlling question of law as to which there is substantial ground for
 14 difference of opinion and that an immediate appeal from the order may materially advance the
 15 ultimate termination of the litigation.” 28 U.S.C. § 1292(b). Section 1292(b) “is a departure from
 16 the normal rule that only final judgments are appealable, and therefore must be construed
 17 narrowly.” *James v. Price Stern Sloan, Inc.*, 283 F.3d 1064, 1067 n.6 (9th Cir. 2002); *see also In*
 18 *re Cement Antitrust Litig.*, 673 F.2d 1020, 1026 (9th Cir. 1982) (“[T]he legislative history of
 19 1292(b) indicates that this section was to be used only in exceptional situations in which allowing
 20 an interlocutory appeal would avoid protracted and expensive litigation.”).

21 The Court finds that Google has not established the exceptional circumstances necessary to
 22 “invoke the narrow exception to the final judgment rule embodied in 28 U.S.C. § 1292(b).”
 23 *Couch v. Telescope Inc.*, 611 F.3d 629, 633 (9th Cir. 2010). First, the question that Google seeks
 24 to certify is not a purely legal one. Rather, additional factual development is necessary as to how
 25 Google scanned email as well as how the alleged interceptions relate to Google’s provision of
 26 Gmail. As the Court noted in denying Google’s motion to certify an interlocutory appeal in
 27 *Gmail*, “[r]egardless of which definition [of the ‘ordinary course of business’ exception] is

1 adopted, the Court finds that factual development would be necessary in determining whether
2 Google’s interceptions fall within the ‘ordinary course of business’ exception. For example, the
3 Court cannot determine based on the pleadings alone what is ‘necessary,’ ‘customary or routine,’
4 or ‘instrumental’ to Google’s business.” *Gmail*, 2014 WL 294441, at *3 (N.D. Cal. Jan. 27,
5 2014). Consequently, “[a]n interlocutory appeal prior to any discovery would deprive the
6 appellate court of a factual record that likely would aid its consideration of the legal questions
7 presented.” *See Lenz v. Universal Music Corp.*, 2008 WL 4790669, at *7 (N.D. Cal. Oct. 28,
8 2008). Moreover, while Google seeks to certify the question of whether the “automated scanning
9 of emails in providing Google services falls within the ‘ordinary course of its business’
10 exception,” a proper question for interlocutory appeal “must be stated at a high enough level of
11 abstraction to lift the question out of the details of the evidence of facts of a particular case.”
12 *Sateriale v. RJ Reynolds Tobacco Co.*, 2015 WL 3767424, at *2 (C.D. Cal. June 17, 2015). These
13 factors weigh against granting interlocutory appeal. *See id.*; *Lenz*, 2008 WL 4790669, at *7.

14 Second, the Court finds that an immediate appeal will not materially advance the ultimate
15 termination of this litigation but rather will delay resolution of this case. Even if Google were to
16 prevail on appeal on the issue for which Google seeks certification, Plaintiff’s CIPA claim will
17 need to be litigated. Plaintiff’s CIPA claim is premised on the same alleged intercepting,
18 scanning, and analyzing of email underlying Plaintiff’s Wiretap Act claim, and will require the
19 parties to engage in very similar discovery. Consequently, “an interlocutory appeal will not allow
20 the parties to avoid protracted litigation [but] will simply create the prospect of two separate
21 appeals.” *Wadler v. Bio-Rad Labs., Inc.*, 2015 WL 8753292, at *2 (N.D. Cal. Dec. 15, 2015); *see*
22 *also Sonoda v. Amerisave Mortg. Corp.*, 2011 WL 3957436, at *2 (N.D. Cal. Sept. 7, 2011)
23 (“When litigation will be conducted in substantially the same manner regardless of our decision,
24 the appeal cannot be said to materially advance the ultimate termination of the litigation.”).

25 Moreover, if Google were truly concerned about receiving a ruling from the Ninth Circuit
26 on the scope of the “ordinary course of business” exception, Google could have chosen to litigate
27 and appeal any of the individual cases in *Gmail*. The Court denied class certification in *Gmail* on

1 March 18, 2014, leaving only individual claims remaining. That ruling was over two years ago.
2 Had Google chosen to litigate any of the individual claims in *Gmail* through appeal, Google likely
3 would have received a ruling from the Ninth Circuit by now. Instead, Google and all the
4 individual plaintiffs stipulated to dismissals with prejudice by July 14, 2014. No. 13-MD-02430,
5 ECF Nos. 175, 177. Accordingly, the Court is not persuaded that exceptional circumstances exist
6 to delay the instant litigation in order for Google to appeal an issue that Google could have
7 appealed two years ago.

8 Because Google has failed to show a “controlling question of law” on which an immediate
9 appeal “may materially advance the ultimate termination of litigation,” certification of an
10 interlocutory appeal is improper and the Court need not determine whether there is “substantial
11 ground for difference of opinion.” *See* 28 U.S.C. § 1292(b). For the reasons discussed above, and
12 respecting the high bar imposed for interlocutory appeal, the Court sees no reason to view the
13 instant issue as an “exceptional situation[.]” warranting interlocutory appeal. *In re Cement*
14 *Antitrust Litig.*, 673 F.2d at 1026; *see also U.S. Rubber Co. v. Wright*, 359 F.2d 784, 785 (9th Cir.
15 1966) (noting that § 1292(b) “was not intended merely to provide review of difficult rulings in
16 hard cases”). The Court DENIES Google’s motion to certify an interlocutory appeal to the Ninth
17 Circuit.

18 B. CIPA

19 Google moves to dismiss Plaintiff’s CIPA claim on two grounds: (1) the Court should
20 decline supplemental jurisdiction; and (2) section 631 of CIPA does not apply to email
21 communications and thus does not apply to the conduct alleged here. The Court addresses these
22 arguments respectively.

23 1. Supplemental Jurisdiction

24 Where a federal court has original jurisdiction over a claim, the court has supplemental
25 jurisdiction over “all other claims that are so related to claims in the action within [the court’s]
26 original jurisdiction that they form part of the same case or controversy under Article III of the
27 United States Constitution.” 28 U.S.C. § 1367(a); *see also Trs. of Constr. Indus. & Laborers*

1 *Health & Welfare Tr. v. Desert Valley Landscape & Maint., Inc.*, 333 F.3d 923, 925 (9th Cir.
2 2003) (upholding the constitutionality of supplemental jurisdiction). Nonfederal claims are part of
3 the same “case” as federal claims when they “derive from a common nucleus of operative [facts]
4 and are such that a plaintiff ‘would ordinarily be expected to try them in one judicial proceeding.’”
5 *Finley v. United States*, 490 U.S. 545, 549 (1989) (quoting *United Mine Workers of Am. v. Gibbs*,
6 383 U.S. 715, 725 (1966)), *superseded by statute on other grounds as stated in Exxon Mobil Corp.*
7 *v. Allapattah Servs., Inc.*, 545 U.S. 546, 558 (2005). A district court has the discretion to decline
8 supplemental jurisdiction under subsection 1367(a) if: (1) the claim raises a novel or complex
9 issue of state law; (2) the claim substantially predominates over the claim or claims over which the
10 district court has original jurisdiction; (3) the district court has dismissed all claims over which it
11 has original jurisdiction, or (4) in exceptional circumstances, there are other compelling reasons
12 for declining jurisdiction. 28 U.S.C. § 1367(c). The district court’s discretion to decline
13 supplemental jurisdiction is informed by the values of economy, convenience, fairness, and
14 comity. *Gibbs*, 383 U.S. at 726.

15 Google does not contest that Plaintiff’s CIPA claim is “part of the same case or
16 controversy” as Plaintiff’s federal Wiretap Act claim and thus that supplemental jurisdiction is
17 proper. However, Google asks the Court to exercise its discretion to decline supplemental
18 jurisdiction because Plaintiff’s CIPA claim “raise[s] a novel or complex issue of State law” that
19 California courts have not addressed. Mot. at 18–20 (quoting 28 U.S.C. § 1367(c)(1)).⁴ Google
20 specifically points to a lack of binding authority regarding whether section 631 of CIPA applies to
21 electronic communications like email.

22 Two California state courts have suggested, without providing analysis, that section 631
23 applies to electronic communications. *See Speaker v. Andrews*, 2015 WL 6859816, at *5 (Cal. Ct.
24

25 ⁴ Google also argues that, should the Wiretap Act claim be dismissed, the Court should decline to
26 exercise supplemental jurisdiction over Plaintiff’s CIPA claim because the Court would lack
27 original jurisdiction over any claim. Mot. at 18–19. The Court need not address this argument
28 because the Court denies Google’s motion to dismiss Plaintiff’s Wiretap Act claim, as discussed
above.

1 App. Nov. 9, 2015) (assuming that plaintiff would be entitled to damages under section 631 if
2 plaintiff could establish a prima facie case that defendant read her private emails); *Diamond v.*
3 *Google, Inc.*, CIV-1202715 (Cal. Super. Ct., Marin Cty. Aug. 14, 2013) (finding, without analysis,
4 that allegations of email interception are sufficient to state a claim under section 631).

5 Additionally, three federal district courts have determined that section 631 applies to electronic
6 communications. *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 936 (N.D. Cal.
7 2015) (concluding that CIPA applies to electronic communications); *Campbell*, 77 F. Supp. 3d at
8 848 (applying CIPA to electronic communications); *Gmail*, 2013 WL 5423918, at*20–21
9 (analyzing text and case law to determine that CIPA applies to electronic communications).

10 Nonetheless, Google is correct that no binding authority exists as to whether section 631 of CIPA
11 applies to electronic communications. Therefore, according to Google, Plaintiff’s CIPA claim
12 arguably “raises a novel or complex issue of State law.” 28 U.S.C. § 1367(c)(1).

13 Novelty alone does not determine whether a district court should decline supplemental
14 jurisdiction. *Allen v. City of Los Angeles*, 92 F.3d 842, 846 (9th Cir. 1996) (exercising
15 supplemental jurisdiction over a novel issue of state law because the values of “economy,
16 convenience and fairness [were] best addressed by the court retaining jurisdiction”), *overruled on*
17 *other grounds by Acri v. Varian Assocs., Inc.*, 114 F.3d 999, 1001–02 (9th Cir. 1997). Instead, the
18 U.S. Supreme Court has made clear that the Court should consider economy, convenience,
19 fairness, and comity. *Gibbs*, 383 U.S. at 726.

20 In the instant case, the Court finds that the values of economy, convenience and fairness
21 are best advanced by the Court’s retention of jurisdiction over Plaintiff’s CIPA claim. *See Allen*,
22 92 F.3d at 846. The Wiretap Act and CIPA are both wiretapping statutes prohibiting the
23 unauthorized interception of communications. *Gmail*, 2013 WL 5423918, at *5–6, *12–13. As
24 such, both claims require analysis of Google’s terms of service and privacy policies to determine
25 whether Gmail and non-Gmail users consent to the alleged interceptions. *See id.* In addition, both
26 claims in the instant case arise from the same underlying conduct: Google’s alleged interception
27 and reading of emails sent to and received by Gmail users before December 19, 2014, which

1 Google analyzed for purposes of creating user profiles and targeted advertising. Compl. ¶¶ 42–70.
2 Although Plaintiff’s CIPA claim also alleges post-December 19, 2014 intercepting, scanning, and
3 analysis of email, Google allegedly used the same devices to intercept, scan, and analyze email at
4 all relevant times. *See id.* ¶¶ 19–23. Because Plaintiff’s Wiretap Act and CIPA claims arise from
5 a common nucleus of fact and have similar legal underpinnings, the two claims will be subject to
6 similar discovery and sources of proof. Accordingly, declining supplemental jurisdiction would
7 be duplicative and inefficient. *See NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 838
8 (N.D. Cal. 2014) (exercising supplemental jurisdiction when federal and state claims involved the
9 same underlying conduct and similar sources of proof); *Lerma v. NTT McKee Retail Ctr., LLC*,
10 2011 WL 4948667, at *6 (N.D. Cal. Oct. 18, 2011) (forcing a plaintiff to bring “a separate, nearly
11 identical case in state court alleging the same facts” would waste judicial resources).

12 Moreover, the undersigned judge has previously determined the legal issue presented. *See*
13 *Gmail*, 2013 WL 5423918, at *20–21. In *Gmail*, the plaintiffs sued Google under both the
14 Wiretap Act and CIPA for “intercept[ing], read[ing], and acquir[ing] the content of emails that
15 were sent or received by Gmail user[s]” for the purpose of creating user profiles and targeted
16 advertising. *Id.* at *1. The Court examined the text of section 631 and California Supreme Court
17 decisions, and concluded that section 631 applies to electronic communications like email. *Id.* at
18 *20–21. Given that the instant case alleges substantially similar conduct by Google over a
19 substantially similar time period, the undersigned judge is “intimately familiar” with the facts
20 underlying Plaintiff’s CIPA claim, in addition to the legal issues. *See Allen*, 92 F.3d at 846.
21 Therefore, exercising supplemental jurisdiction over Plaintiff’s CIPA claim substantially advances
22 judicial economy, convenience and fairness. *Id.*

23 Further, Plaintiff’s CIPA claim does not predominate over Plaintiff’s Wiretap Act claim.
24 As previously stated, Plaintiff’s Wiretap Act and CIPA claims have related factual and legal
25 underpinnings. *See* Compl. ¶¶ 42–70. Therefore, “[t]he state law claim[] do[es] not predominate
26 because the underlying conduct is the same and will likely involve similar sources of proof.”
27 *NetApp*, 41 F. Supp. 3d at 838. In light of the foregoing, the Court elects to retain supplemental
28

United States District Court
Northern District of California

1 jurisdiction over Plaintiff’s CIPA claim.

2 **2. Merits**

3 Section 631 of CIPA establishes liability for:

4 [a]ny person who, by means of any machine, instrument, or contrivance, or in any
5 other manner, intentionally taps, or makes any unauthorized connection, whether
6 physically, electrically, acoustically, inductively, or otherwise, with any telegraph
7 or telephone wire, line, cable, or instrument, including the wire, line, cable, or
8 instrument of any internal telephonic communication system, or who willfully and
without the consent of all parties to the communication, or in any unauthorized
manner, *reads, or attempts to read, or to learn the contents or meaning of any
message, report, or communication while the same is in transit or passing over any
wire, line, or cable,* or is being sent from, or received at any place within this state
. . . .

9 Cal. Penal Code § 631 (emphasis added). In *Gmail*, the Court concluded that this provision
10 applies to email and thus that the interception of email without consent violates California law.
11 *Gmail*, 2013 WL 5423918, at *20–21.

12 In the instant case, Google asks the Court to reconsider the *Gmail* holding. Google
13 specifically argues that (a) CIPA is limited to communications that pass over telephone and
14 telegraph wires, and thus does not apply to email; (b) legislative intent demonstrates that CIPA is
15 limited to eavesdropping, not email privacy; (c) *Gmail* mistakenly concluded that California
16 statutes generally apply to new technologies and thus CIPA applies to email; and (d) amendments
17 to a related statute without corresponding amendments to CIPA demonstrate an intent not to apply
18 section 631 to email. The Court addresses Google’s arguments respectively.

19 **a. Plain Language of CIPA**

20 The Court begins with the statutory text. In particular, there are two clauses in section 631.
21 The first clause of section 631 creates liability for any individual who “intentionally taps, or
22 makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or
23 instrument.” Cal. Penal Code § 631. The second clause of the statute creates liability for any
24 individual who “reads, or attempts to read, or to learn the contents or meaning of any message,
25 report, or communication while the same is in transit or passing over any wire, line, or cable, or is
26 being sent from, or received at any place within this state.” *Id.* As this Court noted in *Gmail*, the
27 second clause of section 631, as opposed to the first clause, is not limited to communications

United States District Court
Northern District of California

1 passing over “telegraph or telephone” wires, lines, or cables. *See Gmail*, 2013 WL 5423918, at
2 *20. Rather, the plain language of the second clause prohibits the unauthorized interception of
3 communications passing over “any wire, line, or cable.” Cal. Penal Code § 631 (emphasis added).
4 This language encompasses email communications, which pass over wires, lines, or cables.

5 Google concedes that the limitation of “telegraph or telephone” in the first clause of the
6 statute is not explicitly repeated in the second clause, but argues that it is “nonsensical” to assume
7 that the California Legislature intended section 631 to cover two categories of wires, lines, and
8 cables. Mot. at 25 n.25. However, the Court finds no reason to conclude that the limitation of
9 “telegraph or telephone” on “wire, line, cable, or instrument” in the first clause of the statute
10 should be imported to the second clause of the statute. In other words, while the first clause of
11 section 631 explicitly applies to “instrument[s]” in addition to “wire[s], line[s], [and] cable[s],” the
12 second clause applies only to “wire[s], line[s], [and] cable[s].” This difference in coverage
13 between the first and second clauses suggests that the Legislature intended two separate clauses
14 applying to different types of communications. *See Gmail*, 2013 WL 5423918, at *20.
15 Accordingly, the Court rejects Google’s argument that the second clause of CIPA is limited to
16 telephone and telegraph communications, and finds that CIPA applies to email.

17 **b. Legislative Intent**

18 The Court turns to Google’s contention that legislative intent indicates that CIPA does not
19 apply to email. Mot. at 20–21. Google highlights section 630 of CIPA, which is titled
20 “Legislative finding and intent.” Section 630 states:

21 The Legislature hereby declares that advances in science and technology have led
22 to the development of new devices and techniques for the purpose of
23 eavesdropping upon private communications and that the invasion of privacy
24 resulting from the continual and increasing use of such devices and techniques has
25 created a serious threat to the free exercise of personal liberties and cannot be
26 tolerated in a free and civilized society.

27 Cal. Penal Code § 630. Google points out that Black’s Law Dictionary defines eavesdropping as
28 “secretly listening to the private conversation of others without their consent.” Relying upon this
definition, Google contends that “CIPA should not be interpreted to reach technologies like email

1 that cannot be ‘eavesdropped’ in any sense of the word.” Mot. at 20.

2 However, Google ignores that Black’s Law Dictionary provides a second definition of
3 eavesdropping, which is “a clandestine attempt to overhear or intercept others’ private
4 communication.” See Black’s Law Dictionary (10th ed. 2014). The alleged interception,
5 scanning, and analysis of Plaintiff’s private communications fall squarely within this definition of
6 eavesdropping.

7 Moreover, Google fails to acknowledge the next paragraph in section 630, “Legislative
8 finding and intent”: “The Legislature by this chapter intends to protect the right of privacy of the
9 people of this state.” This expression of intent is broader than protection against “eavesdropping.”
10 Moreover, the California Legislature chose to “protect the right of privacy of the people of this
11 state” by enacting the prohibitions in section 631. Indeed, the California Supreme Court has
12 repeatedly found that the California Legislature intended CIPA to establish strong privacy
13 protections. For example, the California Supreme Court has stated: “In enacting [CIPA], the
14 Legislature declared in broad terms its intent to protect the right of privacy of the people of this
15 state from what it perceived as a serious threat to the free exercise of personal liberties that cannot
16 be tolerated in a free and civilized society. This philosophy appears to lie at the heart of virtually
17 all the decisions construing [CIPA].” *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (internal
18 quotation marks, alterations, and citations omitted); *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985)
19 (finding it is “probable” that the California Legislature designed section 631 as a catch all to
20 “proscrib[e] attempts to circumvent other aspects of the Privacy Act, e.g., by requesting a
21 secretary to secretly transcribe a conversation over an extension, rather than tape recording it in
22 violation of section 632”); *Tavernetti v. Superior Court*, 22 Cal. 3d 187, 195 (1978) (“Th[e]
23 forceful expression of the constitutional stature of privacy rights [in California] reflects a concern
24 previously evinced by the Legislature in enacting the invasion of privacy provisions of the Penal
25 Code.”).

26 In light of this intent, the California Supreme Court has instructed courts to interpret CIPA
27 in the manner that “fulfills the legislative purpose of [CIPA] by giving greater protection to

1 privacy interests.” *Flanagan*, 27 Cal. 4th at 775. Thus, when faced with two possible
 2 interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the
 3 interpretation that provides the greatest privacy protection. *See Ribas*, 38 Cal. 3d at 360–61. This
 4 Court, when applying California law, “must apply the law as it believes the California Supreme
 5 Court would apply it.” *Kairy v. SuperShuttle Int’l*, 660 F.3d 1146, 1150 (9th Cir. 2011).
 6 In light of section 630’s statement that CIPA is intended to “protect the right of privacy of the
 7 people this this state,” and the California Supreme Court’s findings about the legislative intent of
 8 CIPA, the Court concludes that the California Supreme Court would find that legislative intent
 9 supports the application of CIPA to email.

10 **c. Application of Statutes to New Technologies**

11 Next, Google argues that CIPA does not apply to email because email did not exist at the
 12 time of CIPA’s enactment. Mot. at 22. Thus, according to Google, the California Legislature
 13 could not have envisioned the application of CIPA to email.

14 The California Supreme Court, however, regularly reads statutes to apply to new
 15 technologies where such a reading would not conflict with the statutory scheme. The California
 16 Supreme Court stated this principle plainly in *Apple Inc. v. Superior Court*, 56 Cal. 4th 128, 137
 17 (2013) (ellipsis in original): “Fidelity to legislative intent does not ‘make it impossible to apply a
 18 legal text to technologies that did not exist when the text was created. . . . Drafters of every era
 19 know that technological advances will proceed apace and that the rules they create will one day
 20 apply to all sorts of circumstances they could not possibly envision.” Thus, that a technology did
 21 not exist at the time of a statute’s enactment does not necessarily preclude the application of the
 22 statute to that technology. *See id.* at 139–41.

23 As another example, in *Davis v. Pacific Telephone & Telegraph*, 127 Cal. 312, 316 (1899),
 24 the California Supreme Court interpreted the term “telegraph” functionally based on the type of
 25 communication that was enabled. Specifically, the California Supreme Court held that the phrase
 26 “*telegraph* lines” in a criminal law proscribing the cutting of lines included *telephone* lines
 27 because “[t]he idea conveyed by each term is the sending of intelligence to a distance . . . [thus]

1 the term ‘telegraph’ means any apparatus for transmitting messages by means of electric currents
2 and signals, and embraces within its meaning the narrower word ‘telephone.’” *Davis*, 127 Cal. at
3 316.

4 In the instant motion, Google contends that *Davis* is inapposite because the California
5 Supreme Court rejected *Davis* in *Sunset Telephone & Telegraph Co. v. City of Pasadena*, 161 Cal.
6 265 (1911). However, *Sunset Telephone* did not in fact reject *Davis*. Instead, *Sunset Telephone*
7 concluded that *Davis*’s interpretation of the word “telegraph” in the context of the California Penal
8 Code did not govern the interpretation of the word “telegraph” as used in a provision of the
9 California Civil Code addressing public grants to use public streets and highways. 161 Cal. at
10 274–75. *Sunset Telephone* noted that public grant statutes are strictly construed in favor of the
11 public, and thus found that a statute granting telegraph companies the right to use public streets
12 and highways should be read narrowly and thus did not permit telephone companies the same
13 right. *Id.* at 273, 279–80. The rules of construction applicable to public grant statutes do not
14 apply to CIPA. Moreover, since *Sunset Telephone*, the California Supreme Court has reaffirmed
15 *Davis* and *Davis*’s inclusion of “telephone” within the term “telegraph.” *See, e.g., People v.*
16 *Trieber*, 28 Cal. 2d 657, 661 (1946); *Ex parte Cannon*, 167 Cal. 142, 143–44 (1914).

17 Because the California Supreme Court regularly reads statutes to apply to new
18 technologies where such a reading would not conflict with the statutory scheme, the Court is
19 unpersuaded by Google’s argument that CIPA can not apply to email because email did not exist
20 at the time of CIPA’s enactment.

21 Further, the Court sees no conflict between the statutory scheme and applying CIPA to
22 email. Google contends that exposing electronic communication service providers like Google to
23 “massive potential liability” for routine business conduct would be inconsistent with the statutory
24 scheme. Mot. at 23–25. However, Plaintiff alleges that the interceptions at issue in the instant
25 case do not facilitate and are not incidental to Google’s provision of email services. *See Compl.*
26 ¶¶ 19, 22–23, 28 (“Google intercepts Gmail for the distinct purpose of acquiring and retaining user
27 data and creating targeted advertising . . .”). Thus, taking Plaintiff’s allegations as true, liability

1 for the interceptions alleged does not threaten Google’s ability to provide electronic
 2 communication services. Moreover, Google may seek the consent of its users and other parties to
 3 these communications for any interceptions that Google wishes to undertake. *See* Cal. Penal Code
 4 § 631(a) (providing that interception is unlawful if done “without the consent of all parties to the
 5 communication”). Accordingly, the Court concludes that neither the statutory scheme nor the fact
 6 that email did not exist at the time of CIPA’s enactment prohibit the application of section 631 to
 7 email.

8 **d. Legislative History**

9 Lastly, the Court addresses Google’s argument that amendments to California’s Wiretap
 10 Act, Cal. Penal Code § 629.50 *et seq.*, without corresponding amendments to CIPA, demonstrate
 11 that section 631 does not apply to email. California’s Wiretap Act governs interceptions of wire
 12 and electronic communications by law enforcement. Google points to two instances, in 1995 and
 13 2010, in which the California Legislature amended California’s Wiretap Act to expressly cover
 14 electronic communications, but did not make corresponding amendments to CIPA. *See* Google
 15 RJN Exs. I, J (California Bill Analyses by a California Senate Committee). In 1995, the
 16 California Senate Judiciary Committee noted in its bill analysis that “[i]t is not clear that
 17 California law specifically protects e-mail and other electronic communications from improper
 18 interception by either private parties or law enforcement” and asked whether, “as a corollary” to
 19 the extension of California’s Wiretap Act, “the privacy laws [should] be amended to expressly
 20 protect electronic communications from interception by anyone in the absence of a court order.”
 21 *Id.* Ex. I, at 4. Google contends that the failure of the Legislature to amend CIPA shows that
 22 CIPA should not cover email, and highlights the U.S. Supreme Court’s statement that “[w]hen
 23 Congress amends one statutory provision but not another, it is presumed to have acted
 24 intentionally.” *See Gross v. FBL Fin. Servs., Inc.*, 557 U.S. 167, 174 (2009).

25 *Gross* is distinguishable. In *Gross*, Congress amended the ADEA and Title VII at the
 26 same time, and only the Title VII amendments included a particular provision at issue in the case.
 27 *Id.* The U.S. Supreme Court held that “negative implications raised by disparate provisions are

1 strongest when the provisions were considered simultaneously when the language raising the
2 implication was inserted.” *Id.* at 175(internal quotation marks omitted). By contrast, here Google
3 points to no bill amending CIPA that was contemporaneous with the amendments expanding
4 California’s Wiretap Act. *See* Google RJN Exs. K–M (highlighting earlier proposed amendments
5 to CIPA, in 1986 and 1990).

6 Nor does Google point to any bill in which the California Legislature considered and
7 rejected amending CIPA to include email. The California Supreme Court has stated that
8 legislative inaction may indicate many things, including the “sheer pressure of other and more
9 important business, political considerations, or a tendency to trust to the courts to correct their own
10 errors.” *Cty. of L.A. v. Workers’ Comp. Appeals Bd.*, 30 Cal. 3d 391, 403–04 (1981) (internal
11 quotation marks omitted). In the absence of any amendments to CIPA contemporaneous with the
12 amendments to California’s Wiretap Act, or the affirmative rejection of a proposal to apply CIPA
13 to email, the Court finds minimal value in the Legislature’s inaction with respect to amending
14 CIPA.

15 In sum, in light of the plain language of section 631, the legislative intent underlying CIPA
16 to protect privacy, and the California Supreme Court’s approach to applying statutes to new
17 technologies, the Court finds that *Gmail*’s application of section 631 to email was correct. The
18 Court notes that following *Gmail*, two courts in this district have applied section 631 to electronic
19 communications similar to email. *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d at 936
20 (holding that section 631 applies to “electronic communications”); *Campbell*, 77 F. Supp. 3d at
21 848 (finding that plaintiffs stated a claim under section 631 when defendant allegedly intercepted
22 online Facebook messages). By contrast, Google points to no case in which a court has concluded
23 that section 631 does not apply to email. In line with the foregoing analysis and the weight of
24 authority, the Court DENIES Google’s motion to dismiss Plaintiff’s CIPA claim.

25 **V. CONCLUSION**

26 For the foregoing reasons, the Court DENIES Google’s motion to dismiss as to the merits
27 of Plaintiff’s claims.

1 **IT IS SO ORDERED.**

2
3 Dated: August 12, 2016

Lucy H. Koh

4
5 LUCY H. KOH
United States District Judge

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
United States District Court
Northern District of California