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

QUINN EMANUEL URQUHART & SULLIVAN, LLP
KATHLEEN M. SULLIVAN (242261)
(kathleensullivan@quinnemanuel.com)
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Attorneys for Defendant
GOOGLE INC.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE GOOGLE INC. GMAIL LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

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

DEFENDANT GOOGLE INC.'S MOTION FOR § 1292(b) CERTIFICATION FOR INTERLOCUTORY REVIEW; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

Date: October 29, 2013
Time: 10:00 a.m.
Place: Courtroom 8 – 4th floor

Judge: Hon. Lucy H. Koh

Trial Date: Not yet set

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

NOTICE OF MOTION AND MOTION FOR CERTIFICATION FOR INTERLOCUTORY REVIEW

PLEASE TAKE NOTICE that on October 29, 2013, at 10:00 a.m., before the Honorable Lucy H. Koh, defendant Google Inc. ("Google") will and hereby does move the Court to certify its September 26, 2013 Order, ECF No. 70 (the "Order") denying in part Google's Motion to Dismiss Plaintiffs' Consolidated Individual and Class Action Complaint (the "Complaint") for interlocutory appellate review pursuant to 28 U.S.C. § 1292(b). Google's motion is based upon this notice, the accompanying memorandum of points and authorities, the pleadings on file in these actions, arguments of counsel, and any other matters that the Court deems appropriate.

STATEMENT OF ISSUES TO BE DECIDED

1. Whether the Court should certify the Order for interlocutory appeal under 28 U.S.C. § 1292(b) because it involves the following controlling questions of law as to which there is substantial ground for difference of opinion and because an immediate appeal may materially advance the ultimate termination of the litigation:

   a. Whether automated scanning of emails like that performed by Google in providing Google services falls within the "ordinary course of its business" exception, 18 U.S.C. § 2510(5)(a)(ii), to federal wiretapping liability under 18 U.S.C. § 2511(1).

   b. Whether automated scanning of emails like that performed by Google is protected by the "prior consent" exception, 18 U.S.C. § 2511(2)(d), to federal wiretapping liability under 18 U.S.C. § 2511(1).

MEMORANDUM OF POINTS AND AUTHORITIES

PRELIMINARY STATEMENT

This Court's ruling that Google might be found liable for illegal wiretapping because of its operation of its Gmail system made national headlines,[1] and has already spurred copycat litigation

[1] *See, e.g.*, Timothy B. Lee, *No, Gmail's Ad-Targeting Isn't Wiretapping*, WASHINGTON POST, Sept. 28, 2013, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/28/heres-whats-wrong-with-this-weeks-ruling-that-google-may-be-

(footnote continued)

against other email service providers.[2] Such widespread attention is not surprising, for the Court's ruling was a novel interpretation of wiretapping statutes enacted and amended by Congress long before the rise of the Internet and never since updated to reflect the new technological and commercial realities of the Internet age. Few questions could be more appropriate for interlocutory review to the Ninth Circuit in order to obtain guidance on whether the Court's novel interpretation of now-antiquated statutory provisions in an unanticipated context is correct.

First, the Order presents two controlling questions of law, neither of which has ever been addressed by the Ninth Circuit: namely, the scope of the "ordinary course of its business" exception under 18 U.S.C. § 2510(5)(a)(ii), as applied to Internet services like Google's automated scanning of Gmail users' emails for the alleged purpose of creating targeted email advertisements and user profiles; and the scope of the "prior consent to … interception" exception under 18 U.S.C. § 2511(2)(d), as applied to such email services as Gmail in light of Google's Terms of Service and Privacy Policies and users' awareness of automated processing of emails. Each question depends on interpretation of the text, structure, and legislative history of the Electronic Communications Privacy Act ("ECPA"), purely legal questions that are appropriate for the Circuit's *de novo* review.

Second, a substantial ground for difference of opinion exists as to resolution of these novel issues of law, and reasonable judges examining the same text, legislative history, and sparse case law could well arrive at different conclusions. For example, while the Court construed the term "business" in the phrase "ordinary course of its business" as narrowly limited to "the transmission of emails," a reasonable jurist could give "business" a broader interpretation based on the text of the statute. A reasonable jurist could also disagree with the Court's conclusion that "consent" to "interception" requires consenting to the particular purposes for which interception is used.

---

wiretapping-its-customers/; Claire Cain Miller, *Google Accused of Wiretapping in Gmail Scans*, N.Y. TIMES, Oct. 1, 2013, *available at* http://www.nytimes.com/2013/10/02/technology/google-accused-of-wiretapping-in-gmail-scans.html.

[2] *See, e.g.*, *Kevranian v. Yahoo!, Inc.*, No. 5:13-cv-04547-HRL, ECF No. 1 (N.D. Cal. Oct. 2, 2013).

Third, an immediate appeal would materially advance the ultimate termination of the litigation. Reversal on either issue would warrant dismissal of the federal claims (and by extension the parallel state claims), sparing the parties and the Court from wasting resources on discovery and trial. And if the Ninth Circuit affirms this Court's rulings, its guidance on these issues will help ensure the proper conduct of the remainder of the case and provide important guidance for other companies facing the same issues.

For all these reasons, Google respectfully submits that the Order presents such important issues of first impression on controlling questions of law that certification for interlocutory appeal is warranted. For similar reasons, this Court certified for interlocutory review an order denying a motion to dismiss a class action in *In re Google Inc. Street View Electronic Communications Litigation*, No. C 10-md-02184 JW, ECF No. 90 (N.D. Cal. July 18, 2011) (Ware, J.), which likewise presented novel questions about the construction of ECPA in the Internet context. Here, as in *Street View*, the Order "involves a controlling question of law as to which there is a credible basis for a difference of opinion" and "certification would materially advance the litigation under Section 1292(b)." *Id.* at 2-3 (citations omitted). And here, as in *Street View*, because "novel questions of first impression are presented," there is reason to "find that a substantial ground for difference of opinion exists' … 'without first awaiting development of contradictory precedent.'" *Id.* at 2 n.2 (citations omitted).

STATEMENT OF FACTS

A. Google and Gmail

Google is one of the most successful technology companies in the world. Google offers a suite of free web-based products to billions of people worldwide—most notably, its eponymous search engine, as well as other services such as its video-sharing service, YouTube, and its email service, Gmail. Google offers Gmail accounts, as it does most of its services, *free of charge*. And receiving displays of targeted advertisements is well understood as a *quid pro quo* for having a free Gmail account—much as watching television commercials is a necessary corollary of watching a program on a broadcast network. Revenues derived from such advertisements are what allow Google to provide Gmail free to over 400 million users worldwide.

The more targeted the ad, the more relevant and valuable it is to both the consumer and the advertiser. Thus, as part of delivering pertinent advertisements to Gmail users, Google's automated systems analyze words contained in emails transmitted on the Gmail system. The results of this automated scanning are used to improve Google's services and to enable Google to continue to provide Gmail for free.[3]

B. Google's Terms of Service and Privacy Policies

While Google's Terms of Service ("TOS") and Privacy Policies in effect during the class period underwent revisions, the core of those policies as relevant to this action has been consistent. These policies expressly cover all Google services, including Gmail—there is no dispute that the Gmail service is one of the many "Services" included in Google's TOS and Privacy Policies. Before March 1, 2012, the TOS provided in relevant part that: "Some of the Services are supported by advertising revenue and may display advertisements and promotions. *These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.*" (Rothman Decl., Ex. E ¶ 17 (emphasis added).) The TOS also provided that "Google reserves the right … to pre-screen, review, flag, [or] filter … any or all Content from any Service." (*Id.* ¶ 8.3.)[4] After March 1, 2012, these provisions were revised to inform users that, when they "upload or otherwise submit content to our Services," they give Google "a worldwide license to use … [and] create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services) … and distribute such content[] … for the limited purposes of operating, promoting, and improving our Services, and to develop new ones." (Rothman Decl., Ex. F.)

The Privacy Policy, which is incorporated into the TOS, provides in relevant part:

> *When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads,* to help you connect with people or to make sharing with others quicker

[3] The arguments herein apply to all of the forms of Gmail implicated by the Complaint, including Google's operation of email on behalf of Internet Service Providers and Google Apps for Education. (*See* Order at 3-4.)

[4] "Content" is defined as "all information ... which you may have access to as part of, or through your use of, the Services." (Rothman Decl., Ex. E ¶ 8.1.)

> and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy. …
>
> *We collect information to provide better services to all of our users* – from figuring out basic stuff like which language you speak, to more complex things like *which ads you'll find most useful or the people who matter most to you online.* …
>
> ***Information we get from your use of our services.*** *We may collect information about the services that you use and how you use them*, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes [device information; log information, which "may include" details of use of service, telephony log information, Internet protocol address, device event information, and cookies; location information; unique application numbers; local storage; and cookies and anonymous identifiers].…
>
> *We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.*…

(Rothman Decl., Ex. J) (emphases added).[5]

C. The Order

Plaintiffs allege, *inter alia*, that Google's automated scanning of emails violates 18 U.S.C. § 2511(1)(a) of ECPA. In denying Google's motion to dismiss, this Court rejected (Order at 13-22) Google's argument (ECF No. 44 at 6-13) that automated scanning of users' emails to improve Google's services is not an "interception" under ECPA because any such scanning is subject to the "ordinary course of … business" exception set forth in 18 U.S.C. § 2510(5)(a)(ii). The Court held that "[t]he exception offers protection from liability *only* where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication." (Order at 13 (emphasis added); *see also id.* at 15.) And the Court further narrowed the "ordinary course of … business" exception by stating that "the exception would apply here *only* if the alleged interceptions were an instrumental part *of the transmission of email*." (*Id.* at 13 (emphases added).) The Court also held that,

[5] Before March 1, 2012, Google's Privacy Policy had similar language. (*See, e.g.*, Rothman Decl., Ex. G. ("In order to provide our full range of services, we may collect the following types of information," including "[i]nformation you provide," "[c]ookies," "[l]og information," "[u]ser communications," "[a]ffiliated sites," "[l]inks," and "[o]ther sites" for purposes including "the display of customized content and advertising" and "[d]eveloping new services").) Additional terms are also applicable as to certain types of users and in certain time periods.

because Google's Privacy Policies allegedly did not specify that the content of emails that pass through Gmail systems may be used for targeted advertising or creating alleged user profiles, Plaintiffs had plausibly alleged "that Google exceeded the scope of its own Privacy Policy, [and thus] the section 2510(5)(a)(ii) exception cannot apply." (*Id.* at 22.)

The Court also rejected (Order at 22-28) Google's alternative argument (ECF No. 44 at 13-14) that "the senders and recipients of the emails at issue have all necessarily consented to the processing of their emails by Google," both expressly insofar as Gmail users agree to Google's Terms of Service and Privacy Policies (*id*. at 13-16), and impliedly insofar as non-Gmail users understand and accept that email is automatically processed (*id.* 19-21.) The Court held that Gmail users' acceptance of Google's Terms of Service and Privacy Policies "does not establish explicit consent" (*id*. at 24) and that "non-Gmail users" not subject to Google's Terms of Service or Privacy Policies have not "impliedly consented to Google's interception of their emails to Gmail users" (*id*. at 28).

As the Court agreed, Plaintiffs' claims under Maryland's and Florida's respective anti-wiretapping statutes are derivative of, and thus rise and fall with, Plaintiffs' ECPA claims. (Order at 42.) The Court dismissed claims brought under CIPA § 632 (*id.* at 40-42) and Pennsylvania's anti-wiretapping statute (*id.* at 43), and while the Court granted leave to amend these claims, Plaintiffs have informed Google (ECF No. 72 at 2) they do not intend to do so.

ARGUMENT

Google respectfully requests that the Court certify two discrete issues for interlocutory appellate review:

1. Whether automated scanning of emails like that performed by Google in providing Google services falls within the "ordinary course of its business" exception, 18 U.S.C. § 2510(5)(a)(ii), to federal wiretapping liability under 18 U.S.C. § 2511(1).

2. Whether automated scanning of emails like that performed by Google is protected by the "prior consent" exception, 18 U.S.C. § 2511(2)(d), to federal wiretapping liability under 18 U.S.C. § 2511(1).

A district court may, in its discretion, certify an order for interlocutory appeal if it: (1) "involves a controlling question of law"; (2) on which there is "substantial ground for difference of opinion"; and (3) "an immediate appeal … may materially advance the ultimate

termination of the litigation." 28 U.S.C. § 1292(b). *See, e.g., Regal Stone Ltd. v. Longs Drug Stores Cal., L.L.C.*, 881 F. Supp. 2d 1123, 1130-31 (N.D. Cal. 2012) (certifying order for interlocutory appeal); *Ritz Camera & Image, LLC v. Sandisk Corp.*, 2011 WL 3957257, at *3 (N.D. Cal. Sept. 7, 2011) (same). And where an order "involves a new legal question or is of special consequence," a district court "*should not hesitate* to certify an interlocutory appeal." *Mohawk Indus., Inc. v. Carpenter*, 558 U.S. 100, 111 (2009) (emphasis added).

Because each of these requirements is easily satisfied here as to both issues presented, the Court "should not hesitate" to grant the instant motion. *Id.*

I. THE COURT SHOULD CERTIFY THE QUESTION OF THE PROPER SCOPE OF THE "ORDINARY COURSE OF ITS BUSINESS" EXCEPTION UNDER 18 U.S.C. § 2510(5)(a)(ii)

ECPA in relevant part permits an action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). However, the definition of "electronic, mechanical, or other device" excludes:

> any telephone or telegraph instrument, equipment or facility, or any component thereof,
>
> (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
>
> (ii) *being used by a provider of wire or electronic communication service in the ordinary course of its business*, or by an investigative or law enforcement officer in the ordinary course of his duties; ….

Id. § 2510(5)(a) (emphasis added). Thus, use of equipment or a facility by an electronic communication service ("ECS") "in the ordinary course of its business" is not an interception under § 2511(1)(a).

In construing § 2510(5)(a)(ii), the Court held that the phrase "ordinary course of its business" requires that the ECS provider "demonstrate the interception facilitated the

communication service or was incidental to the functioning of the provided communication service." (Order at 15.) According to the Court, under such a construction, the Complaint plausibly alleges that "there is no … nexus between Google's interceptions and its ability to provide the electronic communication service at issue in this case," (*id.* at 19), with that service narrowly defined as "transmission of email" (*id.* at 13.) The Court further held, based on a D.C. Circuit decision involving § 2510(5)(a)(i), that Google's actions fall outside the "ordinary course of its business" exception of § 2510(5)(a)(ii) because Plaintiffs plausibly allege that "Google's Privacy Policies explicitly limit the information that Google may collect to an enumerated list of items, and that this list does not include the content of emails." (Order at 21 (citing *Berry v. Funk*, 146 F.3d 1003 (D.C. Cir. 1998)).)

The Court's ruling on its construction of § 2510(5)(a)(ii) involves a controlling question of law on which there is substantial ground for difference of opinion, and as to which an immediate appeal may materially advance the ultimate termination of the litigation. The Court should therefore certify the Order on this issue.

A. Interpretation of the "Ordinary Course of Its Business" Exception Involves a Controlling Question of Law

The Court resolved a pure question of law that will be subject to *de novo* review on appeal: the proper construction of a provision of ECPA. *See, e.g.*, *Lively v. Wild Oats Markets, Inc.*, 456 F.3d 933, 938 (9th Cir. 2006) ("We … review *de novo* a district court's interpretation and construction of a federal statute."); *Metrophones Telecomms., Inc. v. Global Crossing Telecomms., Inc.*, 423 F.3d 1056, 1063 (9th Cir. 2005) (similar).[6] As the Court explained, its construction of § 2510(5)(a)(ii) was based on the "statutory text, case law, statutory scheme, and legislative history" of the provision. (Order at 19.) These are purely legal inquiries, not dependent on a factual record.

[6] The Ninth Circuit has also accepted § 1292(b) certifications for questions involving application of law to a particular set of facts where the legal conclusion was sufficiently important. *See Steering Comm. v. United States*, 6 F.3d 572, 575-76 (9th Cir. 1993).

In addition, the issue is "controlling" because "resolution of the issue on appeal could materially affect the outcome of litigation in the district court." *In re Cement Antitrust Litig.*, 673 F.2d 1020, 1026 (9th Cir. 1982). "Although resolution of an issue need not necessarily terminate an action in order to be 'controlling,' it is clear that a question of law is 'controlling' if reversal of the district court's order would terminate the action." *Klinghoffer v. S.N.C. Achille Lauro Ed Altri-Gestione Motonave Achille Lauro in Amministrazione Straordinaria*, 921 F.2d 21, 24 (2d Cir. 1990) (internal citations omitted). Here, reversal of the Order on this issue could terminate the entire action.[7] *See, e.g., Reese v. BP Exploration (Alaska) Inc.*, 643 F.3d 681, 688 (9th Cir. 2011) (controlling question where reversal would remove most claims, noting that "neither § 1292(b)'s literal text nor controlling precedent requires that the interlocutory appeal have a final, dispositive effect on the litigation"); *In re Google Inc. Street View Elec. Commc'ns Litig.*, No. C 10-md-02184 JW, ECF No. 90 (N.D. Cal. July 18, 2011) (certifying order for review of ECPA question, notwithstanding grant of leave to amend state-law claim). In addition, permitting appellate review on this issue at an early stage will avoid the significant costs and burdens of class certification, discovery, depositions, expert discovery, and motion practice—all of which may be unnecessary if the Ninth Circuit reverses. *See, e.g., Helman v. Alcoa Global Fasteners Inc.*, 2009 WL 2058541, at *5-6 (C.D. Cal. June 16, 2009) (certifying order that turned on interpretation of federal statute that was an issue "of first impression in the Ninth Circuit" because "[i]t would be

[7] The fact that a single state-law claim under CIPA § 631 might remain should not bar certification. The Court's ruling on Plaintiffs' § 631 claim itself presents a controlling question of law for which there is substantial ground for a difference of opinion. As the Court noted, "there is no binding authority with respect to whether section 631 applies to email," and thus the Court determined that it "must predict what the California Supreme Court would do if confronted with the issue." (Order at 36.) If the Court grants the instant motion, the entire Order would be certified and the Court of Appeals "'may review the entire order, either to consider a question different than the one certified as controlling or to decide the case despite the lack of any identified controlling question.'" *Rivera v. NIBCO, Inc.*, 364 F.3d 1057, 1063 (9th Cir. 2004) (quoting *Yamaha Motor Corp., U.S.A. v. Calhoun*, 516 U.S. 199, 205 (1996)). Because the Court's ruling on the applicability of § 631 to email is part of the same Order in which the Court decided the "ordinary course of its business" issue, if the Ninth Circuit were to consider and reverse both holdings, the action would be terminated in its entirety, without regard to the issue of consent.

preferable … to address the issue now, rather than to require the parties … to expend significant time and resources").

Finally, this question may have widespread effects on a broad swath of internet industries, and thus presents an issue of important precedential value for other cases. *See Klinghoffer*, 921 F.2d at 24 ("the impact that an appeal will have on other cases is a factor" in determining whether a question is controlling). As Internet-based businesses continue to grow in unexpected ways beyond what anyone could have ever predicted when ECPA was passed in 1986, these important questions will only arise more frequently. *Cf. Am. Geophysical Union v. Texaco Inc.*, 802 F. Supp. 1, 30 (S.D.N.Y. 1992) (Leval, J.) ("[t]he shared interests of large research corporations and the publishing community would be importantly served by an immediate appeal, clarifying these questions"). The interests of Internet-based businesses, ECS providers, and the general public thus would be served by receiving immediate appellate clarification on this issue. Further, there is every indication that the number of lawsuits on this issue will increase—not only does this class action incorporate six separate complaints gathered from across the Nation, but just *one week* after the Court issued the Order another class action was filed in this District against Yahoo alleging claims materially identical to those here. *See Kevranian v. Yahoo!, Inc.*, No. 5:13-cv-04547-HRL, ECF No. 1 (N.D. Cal. Oct. 2, 2013).[8] Expeditious resolution of this issue will thus conserve judicial resources for this Court in this case, and for courts in similar cases.

B. Substantial Ground for Difference of Opinion Exists as to the Proper Construction of the "Ordinary Course of Its Business" Exception

"Courts traditionally will find that a substantial ground for difference of opinion exists where 'the circuits are in dispute on the question and the court of appeals of the circuit has not spoken on the point, if complicated questions arise under foreign law, or if novel and difficult questions of first impression are presented.'" *Couch v. Telescope Inc.*, 611 F.3d 629, 633 (9th Cir. 2010) (quoting 3 FEDERAL PROCEDURE, LAWYERS EDITION § 3:212 (2010)) (footnotes omitted);

[8] In addition, the Order has been submitted to courts in other Wiretap Act cases. *See, e.g., In re Google Inc. Privacy Policy Litig.*, No. 12-cv-1382 PSG, ECF No. 65, Ex. A (N.D. Cal. Oct. 3, 2013); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, No. 12-md-2358(SLR), ECF No. 119, Ex. A (D. Del. Oct. 2, 2013).

see also VIA Techs., Inc. v. SonicBlue Claims LLC, 2011 WL 2437452, at *1 (N.D. Cal. June 17, 2011) ("Substantial grounds for a difference of opinion … arise when an issue involves one or more difficult and pivotal questions of law not settled by controlling authority."). As the Ninth Circuit recently explained:

> Our interlocutory appellate jurisdiction does not turn on a prior court's having reached a conclusion adverse to that from which appellants seek relief. A substantial ground for difference of opinion exists where reasonable jurists might disagree on an issue's resolution, not merely where they have already disagreed. Stated another way, when novel legal issues are presented, on which fair-minded jurists might reach contradictory conclusions, a novel issue may be certified for interlocutory appeal without first awaiting development of contradictory precedent.

Reese, 643 F.3d at 688 (footnote omitted).[9]

Applying these principles here, substantial ground exists for disagreement with the Court's conclusion that the "ordinary course of its business" exception is available *only* where the interception facilitated the "transmission of email" (Order at 13). To the contrary, the plain text of the statute suggests that the exception applies where the interception assists the overall business of which email service is part. This is a novel issue, and fair-minded people may disagree on the interpretation and persuasive value of the statutory text, analogous case law and legislative history. Moreover, there is no controlling authority—*no other court* of which we are aware has construed § 2510(5)(a) as the Court did here. *See VIA Techs.*, 2011 WL 2437425, at *2 (certifying order where "court was unable to locate any definitive authority that answered *the exact question* raised by the … defense") (emphasis added).

First, the statutory text of § 2510(5)(a)(ii) alone would allow a fair-minded jurist to disagree with the Court. The text exempts from the definition of "intercept" any use of a device

---

[9] The applicable standard is not whether the Court is confident in its ruling, but rather whether others may reasonably disagree. As one court recently explained in certifying an order:

> On the issue …, I am convinced that the Decision reflects the better and more considered view of the law. However, if a district court had to believe that her decision was likely to be reversed before certifying a question under 28 U.S.C. § 1292(b), there would be no such certifications. Probability of reversal is not the standard. The standard is whether there is "substantial ground for disagreement."

Dev. Specialists, Inc. v. Akin Gump Strauss Hauer & Feld LLP, 2012 WL 2952929, at *8 (S.D.N.Y. July 18, 2012).

by an ECS provider "in the ordinary course of *its business*"—not "in the ordinary course of *transmitting the electronic communication*." The word "business" is a broad term that, on its face, encompasses conduct broader than the mere technological instrumentality of transmitting emails. The modification of this phrase with the word "ordinary" demonstrates that Congress intended to protect an ECS provider's customary, routine business practices.

The significance of the plain text cannot be overstated. The "first step in interpreting a statute is to determine whether the language at issue has a plain and unambiguous meaning." *Wilson v. C.I.R.*, 705 F.3d 980, 987-88 (9th Cir. 2013) (citation omitted). In so doing, the Court "must begin with … the assumption that the ordinary meaning of that language accurately express the legislative purpose." *de Osorio v. Mayorkas*, 695 F.3d 1003, 1019 (9th Cir. 2012) (citing Gross *v. FBL Fin. Servs. Inc.*, 557 U.S. 167, 175 (2009)). "If the statutory language is unambiguous and the statutory scheme is coherent and consistent, judicial inquiry must cease." *Services Emps. Int'l Union v. Nat'l Union of Healthcare Workers*, 718 F.3d 1036, 1045 (9th Cir. 2013) (quoting *Miranda v. Anchondo*, 684 F.3d 844, 849 (9th Cir. 2012)). In this case, a fair-minded jurist could disagree with the Court and determine, *based on the statutory text alone*, that Google's automated scanning of emails to create targeted advertising and alleged user profiles—all of which indisputably are conducted routinely, and which act to improve and underwrite Google's free services to users—requires reversal. While there may be gray areas in other contexts as to whether the interception is in the course of the ECS provider's "business" as opposed to *non*-business, no such textual uncertainty exists here.[10]

Second, the statutory scheme and legislative history of ECPA permit a conclusion other than that reached by the Court. For example, in describing the statutory structure of ECPA, the Court cites to and quotes 18 U.S.C. § 2511(2)(a)(i), which states:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic

[10] The Court's acknowledgment that "not everything that a company may want to do falls within the 'ordinary course of business' exception" (Order at 14) is true—and supports Google. For example, the requirement that use of the device be for valid and routine business purposes acts as a backstop to any abuse.

> communication, to intercept, disclose, or use that communication in the normal 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.

(Emphasis added.) The Court cites this passage for the proposition that the statute "explicitly limits the use of service observing or random monitoring by electronic communication service providers to mechanical and service quality control checks." (Order at 17.) This, however, is factually incorrect—the statute limits such service observing or random monitoring ***only as to wire communication services, not to electronic communication services***. The statute does not impose any limits on ECS providers regarding service observing or random monitoring. The explicit exclusion of ECS providers from this limiting language supports a broad, not narrow, reading of § 2510(5)(a)(ii). Certainly a reasonable jurist could disagree with the Court's conclusion.

The legislative history of ECPA explains why § 2511(2)(a)(i) applies only to wire communication service providers and not to ECS providers:

> In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain. *These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited.* In contrast, the traditional limits on service "observing" and random "monitoring" do refer to human aural interceptions and are retained with respect to voice or "wire" communications.

(Wong Decl., Ex. BB at 20 (emphasis added).) Based on this legislative history, a reasonable jurist could adopt a broad reading of § 2510(5)(a)(ii)—Congress simply was not concerned about the type of scanning presented here that does not "involve humans listening in on voice conversations." *Id.*

It is important to bear in mind that, in 1986, Congress could not have had an inkling of the vast presence that online activity would have in everyday lives in 2013. The word "Internet" does not appear once in ECPA's legislative history. *See also Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 504 (2d Cir. 2005) ("To understand Congress' intent it is important to note that Internet technology has advanced significantly since Congress enacted ECPA in 1986."). While the

legislative history above states that ECS providers "may" have to monitor transmissions to properly "route, terminate, and otherwise manage" emails, there is no indication that Congress intended to *limit* ECS monitoring only to such tasks—otherwise, Congress would have expressly imposed a statutory limit on ECS providers, as it did for wire communications service providers. Thus, reasonable grounds exist for construing Congress's failure to limit to ECS providers as supporting a broad reading of § 2510(5)(a)(ii).

Third, the case law upon which the Court relies reasonably could be viewed as supporting Google's motion to dismiss. Indeed, the Court cites to *no* controlling authority in support of its interpretation of § 2510(5)(a)(ii), instead relying solely on decisions outside this Circuit, none of which is directly on point and none of which interprets the statute as narrowly as this Court, creating tension between the holdings of this Court and those of the Second and Tenth Circuits. In *Hall*, for example, the Second Circuit relied on the "ordinary course of its business" exception to affirm the dismissal of an ECPA claim brought against an ISP where the plaintiff alleged that the ISP continued processing his emails after he terminated his account. *See* 396 F.3d at 504-05. The processing of emails to a closed account did not facilitate and was not instrumental to the ECS, nor was it incidental to the functioning of the ECS, yet the Second Circuit held that such processing was not an "interception." *Id.* While this Court distinguished *Hall* on the ground that Earthlink "continued to receive and store emails after an account was cancelled" and that Earthlink "did not have the ability to bounce e-mail back to senders after the termination of the account" (Order at 16), neither of these distinctions explains why it was *instrumental*, as part of Earthlink's provision of the business of email services, to continue processing emails to closed accounts. A reasonable jurist could conclude that *Hall* supports the conclusion that a business reason (*e.g.*, storing email in case a former customer asks for it) could fall within the scope of § 2510(5)(a)(ii), even if it was not incidental to the provision of the email system itself.

Similarly, in *Kirch v. Embarq Management Co.*, 702 F.3d 1245, 1250 (10th Cir. 2012), the Tenth Circuit held that Embarq, in allowing NebuAd to run a technology test related to advertising, was protected by the exception because Embarq had "no more of its users' electronic communications than it had in the ordinary course of its business as an ISP." Thus, *Kirch* looked

from a historical standpoint at defendant's ongoing, *entire* business, not just at the particular interceptions at issue. This Court distinguished *Kirch* on the grounds that "Embarq itself did not review any of the raw data that NebuAd collected." (Order at 15.) *Kirch*, however, made no finding that if Embarq *had* collected and reviewed such data as an ordinary, ongoing part of its business, such a review would be an "interception." To the contrary, the district court in that case noted that the "ordinary course of its business" defense "appears to have merit, as plaintiffs have admitted that *Embarq conducted the NebuAd test to further legitimate business purposes and that behavioral advertising is a widespread business and is commonplace on the Internet*." *Kirch*, 2011 WL 3651359, at *9 n.42 (D. Kan. Aug. 19, 2011) (emphasis added).[11] Thus, *Kirch* supports the application of § 2510(5)(a)(ii) where the ESC is furthering its "legitimate business purposes"—including advertising—and is not limited to only those acts that are technically necessary to perform email transmission. Both *Hall* and *Kirch*—the only two cases cited by the Court addressing § 2510(5)(a)(ii)—found that the exception *did* apply, and neither held that only acts "instrumental" to the technological process of sending an email qualify. The Order thus is in tension with the Second and Tenth Circuits, and guidance from the Ninth Circuit is needed to resolve any confusion or inconsistency.

The Court also cites to a number of decisions construing the "ordinary course of its business" exception to § 2510(5)(a)(i) in the context of an employer monitoring employees' telephone and pager calls. (*See* Order at 18-19, citing *Adams v. City of Battle Creek*, 250 F.3d 980 (6th Cir. 2001); *Arias v. Mutual Central Alarm Serv., Inc.*, 202 F.3d 553 (2d Cir. 2000); *United States v. Murdock*, 63 F.3d 1391 (6th Cir. 1995); *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983); *James v. Newspaper Agency Corp.*, 591 F.2d 579 (10th Cir. 1979).) While the Court characterizes these cases as holding that "there must be some nexus between the need to engage in

[11] The Court suggests that "Google is more akin to NebuAd, which intercepted data for the purpose of providing targeted advertising." (Order at 15.) This ignores, however, that: (1) unlike the one-time NebuAd test on Embarq, Google's scanning is an ordinary and routine part of its business; and (2) Google's targeted advertising is a component of its own integrated services—unlike NebuAd and Embarq, which were two companies with separate business goals, Google's business includes *both* the provision of email and targeted advertising, necessarily intertwined.

the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying good or service" (Order at 19), none of these cases required such a narrow connection, to the contrary, they suggest the opposite. *Adams*, for example, holds that application of the exception requires that the use be merely "for a *legitimate* business purpose." 250 F.3d at 984.[12] And *Berry*, 146 F.3d at 1009, noted that "if covert monitoring is to take place it must itself be justified by a valid business purpose, or, perhaps, at least must be shown to be undertaken normally" (quotation marks and internal citation omitted). In any event, Google's automated scanning serves not merely "legitimate" and "valid" business purposes, but is fundamental to allowing Gmail to continue to operate. Indeed, effective targeted advertising, achieved through the challenged automated scanning, *funds* Gmail and permits it to continue as a free service—a quintessential "nexus." Substantial ground thus exists for interpreting this line of cases as supporting Google's argument that its routine practice of automated scanning is for valid, legitimate business purposes and thus falls within the protection afforded by the statute.

Fourth, a reasonable jurist may be persuaded that, under the Court's test, absurd results will necessarily follow. For example, the Court's construction of § 2510(5)(a)(ii) arguably would manufacture never-ending ECPA cases for the provision of services that are claimed not to be "instrumental" to the facilitation or functioning of an ECS, but nonetheless are expected by all users. Using the Court's analysis, one could conclude that email spell-checking, spam filtering, and search indexing are not "instrumental" to the technical transmission of emails, but the presence of such features cannot realistically be perceived as giving rise to ECPA violations—they, like targeted advertising, are part of the ordinary business of providing an effective email service, expected by consumers.[13]

---

[12] *See also, e.g.*, *Arias*, 202 F.3d at 559 ("[l]egitimate business reasons"); *Watkins*, 704 F.2d at 582 ("if the intercepted call was a business call, then [employer's] monitoring of it was in the ordinary course of business").

[13] The Court discounts any danger to such generally accepted email services on the ground that they may fall within a narrow definition of "ordinary course of its business" or may be protectable by attaining user consent. (*See* Order at 20 n.4.) But the Order indisputably creates uncertainty about whether and when such services are protected under ECPA, underscoring the need for the Ninth Circuit's guidance.

Further, the Order is in fundamental tension with a recent opinion from this District that dismissed ECPA claims as applied to Gmail services. *See In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012). There, Judge Grewal noted that the "plain language of [ECPA] … excludes from the definition of a 'device' *a provider's own equipment* used in the ordinary course of business." *Id.* at *6 (emphasis added); *see also id.* at *5 (use of a "device" under ECPA "cannot include Google's own systems"). Here, Google's automated scanning technologies are Google's own "devices." Given the disconnect between Judge Grewal's decision and the Order, both the instant parties and future parties would be best served by receiving guidance from the Ninth Circuit to provide clarity on these issues.

Finally, the Court offered an alternative ground for finding that the "ordinary course of its business" exception is inapplicable: namely, that Plaintiffs sufficiently allege that Google has violated its own internal policies and is therefore acting outside the ordinary course of business. (Order at 20-22.) For this argument, the Court cites only *Berry*, where the D.C. Circuit found that the State Department Operations Center's internal guidelines "clearly indicate the norm of behavior [phone monitors] were to follow." 146 F.3d at 1010. Substantial ground exists, however, for rejecting the Court's position because it *notices to third-party customers* in the TOS and Privacy Policy are not "internal policies" akin to the internal guidelines distributed to call monitors at the State Department. To the contrary, Google's automated scanning is its standard norm of behavior. To state a claim of a violation of an "internal policy," Plaintiffs must offer allegations as to "internal policies" that Google adopted and how it violated those internal standards. Plaintiffs have not done so. And even if Google's TOS and Privacy Policy could somehow be construed as internal policies, Google did not violate such policies, as Plaintiffs consented to the activities at issue. *See infra*, Point II.[14]

[14] To the extent that substantial ground for difference of opinion exists as to the examples Google lists of information it may collect from users (Order at 21), Google addresses this argument in the discussion of consent. *See infra*, Point II. Any suggestion that Google violated its own internal polices because it purportedly did not provide notice of such collection improperly conflates the two inquiries. *See Amati v. City of Woodstock*, 176 F.3d 952, 955 (7th Cir. 2001) (Posner, J.).

C. Certification of the "Ordinary Course of Its Business" Question May Materially Advance the Termination of the Litigation

Immediate appeal of the Order "may materially advance the ultimate termination of the litigation." 28 U.S.C. § 1292(b). This factor does not "require[] that the interlocutory appeal have a final, dispositive effect on the litigation, only that it 'may materially advance' the litigation." *See Reese*, 643 F.3d at 688. Whether certification will materially advance the termination of the litigation "is closely related to the question of whether an issue of law is 'controlling' 'in that the [district court] should consider the effect of a reversal … on the management of the case." *Lakeland Village Homeowners Ass'n v. Great Am. Ins. Group*, 727 F. Supp. 2d 887, 896 (E.D. Cal. 2010) (quotation marks and citation omitted).

If the Ninth Circuit agrees that the Order too narrowly construes § 2510(5)(a)(ii) and reverses the Order, this action might well be entirely terminated. Particularly in a class action, interlocutory appeal saves judicial and party resources that might be wasted on class-certification motions, expert discovery, and fact discovery, all of which might well be unnecessary should the Ninth Circuit reverse. *See, e.g.*, *Helman*, 2009 WL 2058541, at *6 (particularly in "complex" cases, "[i]t would be preferable for the Court of Appeals to address the issue now, rather than to require the parties and to expend significant time and resources, which might ultimately be wasted").[15]

II. THE COURT SHOULD CERTIFY THE QUESTION OF THE PROPER SCOPE OF THE "PRIOR CONSENT" EXCEPTION UNDER 18 U.S.C. § 2511(2)(d)

Liability under ECPA is also foreclosed where a party to the communication consents to an interception:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

[15] For the reasons noted above, *see supra* fn. 7, if the Court determines that the "ordinary course of business" exception warrants interlocutory appellate review, the Court need not even proceed to the second issue presented, as the entire Order would be certified.

18 U.S.C. § 2511(2)(d).

On the issue of consent, this Court concluded (Order at 24) that the TOS did not sufficiently inform users that it would "intercept emails for the purposes of creating user profiles or providing targeted advertising" and (*id.* at 26) that the Privacy Policies "do not specifically mention the content of users' emails to each other or to or from non-users" and thus "are not broad enough to encompass such interceptions." The Court also found that non-Gmail users did not impliedly consent to Google's automated scanning of emails sent, because accepting that theory "would eviscerate the rule against interception." (Order at 27.)

The Court's ruling on the application of the consent exception in § 2511(2)(d) involves a controlling question of law on which there is substantial ground for difference of opinion, and as to which an immediate appeal may materially advance the ultimate termination of the litigation.

A. Whether Plaintiffs Consented to Automated Scanning Pursuant to § 2511(2)(d) Is a Controlling Question of Law

The Court's interpretation of Google's TOS and Privacy Policy to determine whether they establish consent under § 2511(2)(d) is a question of law reviewed *de novo* on appeal. *See, e.g.*, *MHC Fin. Ltd. P'ship v. City of San Rafael*, 714 F.3d 1118, 1131 (9th Cir. 2013) ("A district court's interpretation and meaning of contract provisions is reviewed de novo."); *Doe I v. Wal-Mart Stores, Inc.*, 572 F.3d 677, 681 (9th Cir. 2009) ("Contract interpretation is a question of law that we review *de novo*."); *Lively*, 456 F.3d at 938 (interpretation and construction of federal statute reviewed *de novo*). As the Court based its ruling both on its interpretation of contractual terms and on its construction of a provision of ECPA, this issue presents a question of law.

For reasons similar to those discussed above, *see supra* Point I.A., the issue is "controlling" because "resolution of the issue on appeal could materially affect the outcome of litigation in the district court." *In re Cement Antitrust*, 673 F.2d at 1026. While it is not necessary for a reversal to completely terminate an action to be controlling, circumstances where reversal *will* terminate the action are, by definition, "controlling." *See Klinghoffer*, 921 F.2d at 24. If the Ninth Circuit reverses the Order on *de novo* review and finds that *all* Plaintiffs—Gmail users and non-Gmail users alike—necessarily consented to Google's automated scanning, the entire case

would be terminated. Even if the Ninth Circuit reverses only as to consent of Gmail users but not to consent of non-Gmail users, the scope of the action would be significantly narrowed, removing a large, discrete segment of class-action plaintiffs from the case.

Finally, much like the "ordinary course of its business" exception, the "prior consent" question presents an issue of great importance to future litigation and to Internet-based business and Internet users. *Id.* Whether (1) Google's TOS and Privacy Policy are sufficient to provide notice here; and (2) websites are required to list every conceivable purpose of every conceivable use of a user's information in its terms of service, are both issues likely to arise in the future that could direct the course of how such provisions are written. Businesses and users alike could only be served by receiving clarity on this important issue. *See, e.g.*, *Am. Geophysical Union*, 802 F. Supp. at 30.

B. Substantial Ground for Difference of Opinion Exists as to Whether Plaintiffs Consented to Automated Scanning Pursuant to § 2511(2)(d)

While the Court ruled that Gmail users' acquiescence to Google's TOS and Privacy Policies does not establish explicit or implied consent, a fair-minded jurist reviewing Google's policies could reach a contrary conclusion, satisfying the second § 1292(b) factor.

Google's TOS and Privacy Policy (which is incorporated into the TOS), read together, put Gmail users on express notice that Google may use information gathered from their use of Google's integrated services—which include Gmail—to improve and develop its services, which include targeted advertising and the alleged user profiles.[16] On an appropriate construction of § 2511(2)(d), a reasonable jurist considering the text of these policies could find that Gmail users expressly consented to automated scanning of emails in connection with Google's provision of its services. *See, e.g.*, *Kirch*, 2011 WL 3651359, at *7-9 (consent based on terms of service); *Deering v. CenturyTel, Inc.*, 2011 WL 1842859, at *1-3 (D. Mont. May 16, 2011) (granting

[16] In addition, through March 2012, Google had a Gmail-specific Legal Notice, which informed Gmail users that Google "will not use any of *your content* for any purpose except to provide you with the Service." (Compl. ¶ 121) (emphasis added). Because "your content" logically means "the content of your emails," this notice, when read in connection with Google's TOS and Privacy Policy, further notified Google users their "content" may be used to provide them with Google's services.

motion to dismiss ECPA claim based on consent to privacy policy); *Mortensen v. Bresnan Commc'n, L.L.C.*, 2010 WL 5140454, at *5 (D. Mont. Dec. 13, 2010) (similar). Thus, substantial ground exists for disagreement with the Court.

First, while the Court acknowledged that Section 8 of the TOS notified users that "content may be intercepted" (Order at 24), the Court nonetheless held that Gmail users did not consent to such automated scanning of their emails *for the specific purposes* for which Plaintiffs now complain. (*See, e.g.*, Order at 23 ("the Court finds that it cannot conclude that any party … has consented to Google's reading of email *for the purposes of creating user profiles or providing targeted advertising*") (emphasis added); 24 (TOS suggests that content may be intercepted "for a different purpose" but "[t]his does not suggest to the user that Google would intercept emails *for the purposes of creating user profiles or providing targeted advertising*.") (emphasis added); *id.* ("to the extent that section 8 of the Terms of Service establishes consent, it does so *only for the purpose* of interceptions to eliminate objectionable content") (emphasis added).) Substantial ground exists for disagreement with this construction of "consent."

The text of § 2511(2)(d) provides no indication that "consent" is purpose-specific, nor does the Court cite to any authority that the exception is so narrowly construed.[17] Rather, the statute states that it is *the interception itself* to which a party provides consent. *See* 18 U.S.C. § 2511(2)(d) (it is not unlawful "to intercept a[n] … electronic communication where … one of the parties to the communication has given prior consent *to such interception*") (emphasis added). Indeed, the statute lists specific purposes that are *not* protected by the exception: "the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.* The plain text of the statute thus provides that, once a party consents

[17] *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983)—which the Court cites to for this point—is inapposite. (Order at 24.) In *Watkins*, the plaintiff consented to the monitoring of her sales calls, but did not consent to the monitoring of her personal calls. *Id.* at 581. The plaintiff did not argue, nor did the 11th Circuit hold, that a *legitimately monitored sales call* could not be consented to if the company used the monitoring of that business call for a different purpose. *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003), which the Court also cites, makes this point. There, plaintiffs "insisted there be no collection of personal data," *id.* at 20, and thus the initial interception was not consented to.

to an interception, "such interception" may be used by the recipient if it is not "for the purpose of committing any criminal or tortious act"—otherwise, the subsequent language addressing prohibited purposes would be superfluous. Thus, under ECPA, a relevant consent is to the *act* of interception, not to any *purpose* of that interception unless the purpose is to commit a criminal or tortious act. Other decisions are in accord that, once a party to a communication consents to the interception itself, the purpose for such interception is immaterial. *See, e.g.*, *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1162-63 (W.D. Wash. 2001), *abrogated on other grounds by Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004) (act of interception protected by § 2511(d)(2), as long as interception was not for a criminal or tortious purpose).[18]

Giving this statutory text its plain meaning, a fair-minded jurist could conclude that, because Plaintiffs do not allege that Google's automated scanning of emails was for the purpose of committing a criminal or tortious act, Plaintiffs consented to the automated scanning of emails regardless of the purpose for interception—and certainly consented to Google using the intercepted material for the purpose of facilitating use of integrated Google services. Where statutory language is clear, "judicial inquiry must cease." *Services Emps. Int'l Union*, 718 F.3d at 1045. And if there were any doubt, it is resolved by clear precedent that "'consent' must be construed broadly under the Wiretap Act." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 514 n.23 (S.D.N.Y. 2001). The fact that remedies may lie under *other* legal provisions for certain misuses of procured information have no bearing on this basic point.

The same basis provides reasonable grounds to conclude that *both Gmail and non-Gmail* users impliedly consented to the automated scanning of emails sent to or from Gmail users. Plaintiffs concede that the automated processing of emails—including Google's scanning of content of emails for spam and virus detection—is widely known. (*See, e.g.*, ECF No. 53 at 2 (not contesting public awareness that email content is scanned "to filter out spam or detect computer

---

[18] *See also* Orin Kerr, *Is Gmail Illegal?* at http://www.volokh.com/2013/10/04/is-gmail-illegal/ (Oct. 4, 2013) ("In the case of Gmail's policies, Gmail users were put on notice as to the interception. Whether they knew about what would happen after the interception occurred is immaterial to the consent.").

viruses" (modifications omitted).) Further, every reputable provider of email services offers such features. Thus, when Gmail and non-Gmail users impliedly consented to the content of their emails being scanned by Google for spam or virus detection, the use of such scanning for other non-tortious or non-criminal purposes did not give rise to an ECPA violation.[19] Such a reading avoids the need for the Court to look to the TOS or Privacy Policies to determine express consent, as implied consent is already present. At a minimum, a fair-minded jurist could reasonably understand the text of § 2511(2)(d) to require such an outcome.

Second, the Court's apparent requirement that Google list every purpose for which material is collected with specificity is impracticable to satisfy without rendering the policy far less accessible to users, due to increased length, complexity, and excessive detail. Google's TOS and Privacy Policy are written in such a way to make it *more* likely that users will read and understand the terms—they use general terms and provide a few examples in easy-to-understand language. If Google and other technology companies were suddenly forced to describe and explain in detail every purpose for which every piece of data is used, terms of service and privacy policies would be lengthy and incomprehensible. The level of specificity the Order requires would also require companies to revise their terms of service and privacy policies every time they add or revise features to existing products or alter how they use data to implement existing features—an impracticable task given the speed and frequency at which Google and other technology companies innovate.

The same applies to the Court's suggestion that users did not consent to automated scanning of their email because email is not specifically listed among Google's list of examples of in its TOS and Privacy Policies of which information it collects. Google (like most companies) provides broad, general language notifying users that it collects information relating to users' interactions with its services. (*See, e.g.*, Rothman Decl, Ex. E at § 17.1 ("advertisements may be targeted to the content of information stored on the Service, queries made through the Service or

[19] For this reason, substantial ground exists for difference of opinion on the remaining state-law claims, as both parties consent to the acts of interception at issue.

other information"); *id.* § 8.3 ("Google reserves the right … to pre-screen, review, flag, [or] filter … any or all Content from *any Service*.") (emphasis added); Ex. J ("We also use the information we collect from *all of our services* to provide, maintain, protect and improve them, to develop new ones…. We use this information to offer you tailored content…." (emphasis added).) It would be commercially impracticable and unduly burdensome for websites to specifically list every possible way that information might be collected when general, easily understood terms (such as "services") much more clearly inform users of the website's overall practices. And to avoid any confusion on that point, in employing language of examples, Google indicates such lists are not exclusive by using words such as "include" or "in addition to." (*See* ECF No. 56, App. A.); *see United States v. Gertz*, 249 F.2d 662, 666 (9th Cir. 1957) ("The word 'includes' is usually a term of enlargement, and not of limitation").

Third, the Court separately criticized Section 17 of Google's TOS because it states that "advertisements *may* be targeted to the content of information," and not *will* be targeted. (Order at 25.) A fair-minded jurist, however, could find that the Court misconstrued the word "may." In the TOS, the word "may" means that Google *has permission to* target advertisements to content. *See* BLACK'S LAW DICTIONARY 1068 (9th ed. 2009) (first definition of "may" is "[t]o be permitted to"); *BlueEarth Biofuels, LLC v. Hawaiian Elec. Co.*, 2011 WL 2116989, at *20 (D. Haw. May 25, 2011) (citing BLACK'S). Any other construction of "may" would encourage a tortured reading of the TOS—why would Google inform users that advertisements "might" be targeted, if not to notify users of the likelihood that it would occur?[20] As such, courts generally accept that using the word "may" provides sufficient notice of events. *See, e.g.*, *Deering*, 2011 WL 1842859 at *1-2 (notice valid where TOS disclosed that certain information "may" be collected).

---

[20] The Court's only authority for this point is *Berry*. (Order at 25.) In *Berry*, however, the Court ruled that knowing about the "capacity" to monitor telephone calls was not sufficient evidence of notice that monitoring would happen. 146 F.3d at 1011. That is, capacity does not automatically equal possible action. This Court's interpretation of "may," however, demonstrates a likelihood, not merely an ability, to target ads. *See United States v. VandeBrake*, 679 F.3d 1030, 1048 n.17 (8th Cir. 2012) (where "may" used to express possibility, "'may' … expresses likelihood whereas 'might' expresses a stronger sense of doubt"). Further, the Court's construction contradicts almost every employee monitoring case, where employees are informed of the *possibility* of monitoring.

C. Certification of the "Prior Consent" Question May Materially Advance the Termination of the Litigation

For the same reasons discussed above, *see supra* Point I.C., immediate appeal "may materially advance the ultimate termination of the litigation." 28 U.S.C. § 1292(b). If the Ninth Circuit finds that Plaintiffs consented to Google's automated scanning and reverses the Order, the action may be terminated in its entirety. And because the case is at such an early stage, resolution of such a threshold issue at the outset will save the parties and the Court significant time and resources by avoiding potentially unnecessary discovery and motion practice.

CONCLUSION

The Court should certify the Order for interlocutory appellate review pursuant to 28 U.S.C. § 1292(b).

DATED: October 9, 2013

COOLEY LLP
MICHAEL G. RHODES (116126)
WHITTY SOMVICHIAN (194463)
KYLE C. WONG (224021)

QUINN EMANUEL URQUHART & SULLIVAN, LLP
KATHLEEN M. SULLIVAN (242261)

/s/ Kathleen M. Sullivan
Kathleen M. Sullivan
Attorneys for Defendant GOOGLE INC.