In Re Google Inc.: ECPA, Consent, and the Ordinary Course of Business in an Automated World

CHRISTOPHER BATISTE-BOYKIN *

INTRODUCTION

Question: How do you fit a square peg into a round hole?
Answer: You either hack off the edges of the square or you make the hole bigger.

The common saying above reflects how courts have addressed the automated scanning of email content in different factual contexts. At least one federal court has suggested that, under certain circumstances, electronic communications service ("ECS") providers may be able to scan the content of email to provide targeted advertisements. Another federal court in the same district signaled that ECS providers may be liable under Electronic Communications Privacy Act ("ECPA")\(^1\) when they engage in this practice.

Either way, users of ECS providers, like Google, should be wary because online communications are becoming a rich resource for companies to mine for data. As advances in technology occur, the information that ECS providers gather from online communications will inform advertisers of users’ tastes, preferences, beliefs, associations, interests, schedules, locations, ages, and incomes. It may also reveal users’ medical information, sexual behavior, travel history, future destinations, and much more.

According to Ray Kurzweil, Google’s director of engineering, by 2029, “computers will be more intelligent than we are and will be able to understand what we say, learn from experience, make jokes, tell stories and even flirt.”\(^2\) Google’s CEO, Eric Schmidt, has even indicated that Google

---

* Chris Batiste-Boykin is a 4th year dual JD and MBA candidate expected to graduate in May 2016. Chris also holds a B.A. in Political Science and a minor in African American Studies from the University of California at Berkeley, conferred in May 2007. Born in Los Angeles, CA, and raised in San Jose, CA, Chris has witnessed the profound affect technology has had on jurisprudence and seeks to resolve tough legal issues that arise at the intersection of law and technology. Equally inspired by many University of San Francisco School of Law professors, Chris would like to give a special thanks to Susan Freiwald for her unbounded knowledge, guidance, and assistance in developing this article. Chris would also like to thank his family for their support and USF’s Intellectual Property Law Bulletin Staff for their hard work and dedication to publishing this comment.

“‘know[s] where you are. We know where you’ve been. We can more or
less know what you’re thinking about.’”\(^3\)

In May 2013, plaintiffs, representing an uncertified class, filed suit in
the Northern District of California and alleged that Google violated ECPA
by intercepting and reading the content of their email in an effort to create
targeted advertisements and user profiles.\(^4\) Google denied violating ECPA
and claimed that its practices fell within two exceptions to ECPA liability:
the consent exception and the ordinary course of business exception.\(^5\)

On September 26, 2013, Judge Lucy Koh for the Northern District of
California, issued an order granting in part and denying in part Google’s
Motion to Dismiss against the plaintiffs.\(^6\) Judge Koh determined that Gmail
users and non-Gmail users neither expressly nor impliedly consented to
Google scanning the content of their email to provide targeted
advertisements or to create alleged user profiles.\(^7\) Judge Koh determined
that the ordinary course of business exception did not apply to Google’s
practice of scanning email content to provide targeted advertisements.
Judge Koh explained that the exception should be read narrowly and that
ECPA’s text, statutory scheme, and legislative history indicated that only
interceptions that facilitate or are incidental to the ECS at issue are exempt
from ECPA liability.\(^8\)

Prior to Judge Koh’s order, another group of plaintiffs had challenged
Google’s data collection practices in the same federal district. In 2012, a
group of plaintiffs alleged, among other things, violations of ECPA for
intercepting content from one Google product and combining the content
with information gathered from another product, stored on Google’s
servers.\(^9\) In re Google, Inc. Privacy Policy Litigation centered on Google’s
ability to gather information from a user’s Gmail account or Google+
account and use that information in its search engine to personalize search
results or provide targeted advertisements while the user is surfing the
Internet.\(^10\)


\(^3\) Nick Saint, Google CEO: “We Know Where You Are. We Know Where You’ve Been. We
Can More or Less Know What You’re Thinking About.” BUSINESS INSIDER (Oct. 4, 2010, 9:47 AM),
http://www.businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-
we-can-more-or-less-know-what-youre-thinking-about-2010-10.

\(^4\) See Plaintiffs’ Consolidated Individual and Class Action Complaint at 1–2, In re Google
Inc. Gmail Litigation, No. 5:13-md-02430-LHK (N.D. Cal. May 16, 2013), ECF No. 73 [hereinafter
Plaintiffs’ Complaint] (The remainder of this paper will refer to this litigation as Gmail Litigation).

\(^5\) See Defendant Google Inc.’s Motion to Dismiss Plaintiffs’ Consolidated Individual and
Class Action Complaint; Memorandum of Points and Authorities in Support thereof at 6–20, In re
Mot. to Dismiss].

\(^6\) See Order Granting in Part and Denying in Part Defendant’s Motion to Dismiss, In re
[hereinafter Koh Order].

\(^7\) Id. at 23.

\(^8\) Id. at 9–11.

\(^9\) See Order Granting Defendant’s Motion to Dismiss with Leave to Amend at 6, In re
6738343 [hereinafter Privacy Policy Lit.].

\(^10\) Id. at 2.
Google’s Motion to Dismiss in the above case and found that ECPA excludes from the definition of a device any equipment used by an ECS provider in the ordinary course of business. Judge Grewal determined that ECPA’s ordinary course of business exception should be read according to its plain language. Therefore, Google did not violate ECPA because no device, as defined by the statute, was used to intercept electronic communications.

Judge Koh’s decision in Gmail Litigation received a mixed response. Privacy advocates applauded the decision, arguing that email is private correspondence and should not be subject to monitoring by a multi-billion dollar corporation. Other commentators questioned how the automated scanning of emails to provide targeted advertisements could be an illegal interception, when scanning email to provide spam and anti-virus detection is not. Privacy advocates and ECS providers watched the progress of the litigation closely, since automated scanning hung in the balance.

Part I of this paper will describe Google’s automated email scanning practices and the Gmail platform. Part II argues that the consent Google claims to gain for the automated scanning of email is inconsistent with the traditional precepts of contract law. Part II agrees with Judge Koh’s determination that Google did not obtain consent from users or non-users to scan the content of their email. It advocates for Congress to adopt a two-party consent standard to better align ECPA with its purpose. Part III assesses the ordinary course of business exception and concludes that Google’s business practice fits within the meaning of the exception. Part III therefore disagrees with Judge Koh’s analysis and agrees with Judge Grewal’s determination that ECPA’s plain language supports finding no liability for Google. It goes on to suggest that an industry-based organization be tasked to assess whether a business practice is a known industry standard to resolve any ambiguity within the ordinary course of business exception. Part IV contends that, in most circumstances, the automated scanning of email should be an illegal interception under ECPA, even though no humans are necessarily involved. The paper concludes by cautioning that statutorily protected values, like privacy in electronic communications, should not be overlooked in favor of technological advancement.

I. GOOGLE’S AUTOMATED SCANNING OF EMAIL CONTENT

In its Motion to Dismiss, Google indicated that “[t]he processes

11 Id. at 6.
12 Id.
13 See, e.g., Martha Mendoza, Google says it has the right to scan your email, CTV NEWS (Sept. 5, 2013, 6:15 AM), http://www.ctvnews.ca/sci-tech/google-says-it-has-a-right-to-scan-your-email-1.1441131.
related to Google's automated scanning are completely automated and involve no human review." This implies that Google's automated scanning does not threaten privacy or violate ECPA since no person controls the process or reviews the results of the email scan. An automated process is defined as a "technique, method, or system of operating or controlling a process by highly automatic means, as by electronic devices, reducing human intervention to a minimum." Automated processes are not unfamiliar to society, especially among devices such as heating and cooling systems, lighting settings and certain computer functions, which do not require human intervention to operate. Automated processes can be considered efficient and reliable since they may eliminate unacceptable uses or outcomes that may be produced by a device under direct human supervision or control.

Since Gmail's launch, Google and other email service providers have automatically scanned the text of incoming email messages to filter out spam and email viruses from users' inboxes. Google also scans the contents of email messages in order to display advertisements and allegedly, to create user profiles. According to the plaintiffs' complaint, when a Gmail user receives an incoming email message, Google transmits the message, reads and acquires the content of the message, then selects matching advertisements to attach to the message. Plaintiffs' contended that this process occurs separately from Google's spam and filtering processes.

Like other email service providers with scan and filter features, Google offers Gmail as a service beyond the transmission of email. Gmail is a service platform that Google offers for free. In March 2008, Google revamped Gmail and included features such as: a "faster interface, group chat from the browser, streamlined contact manager, colored message labels, improved keyboard shortcuts, bookmarkable messages and searches" and a new RSS feed. Subsequently, in June 2008, Google introduced Google Labs, which allowed Gmail users to test experimental features before their official release.

19 See Plaintiffs' Complaint at 6–14, In re Google Inc. Gmail Litigation, No. 5:13-md-02430-LHK (N.D. Cal. May 16, 2013), ECF No. 73.
20 See id.
21 See id. at 2.
23 Robby Stein, 3 Gmail Labs Features that Will Spice Up Your Inbox, OFFICIAL GMAIL BLOG (June 16, 2008), http://gmailblog.blogspot.com/2008/06/3-gmail-labs-features-that-will-spice.html.
By 2010, Google began transitioning Gmail’s email platform to a platform for developers as well.\(^24\) Gmail integrated Google Voice in August 2010, which allowed users to make voice calls in Gmail’s chat service.\(^25\) In December 2011, Gmail integrated social networking with Gmail through Google+, where users share content and communicate through videoconferencing and traditional messaging.\(^26\) Google integrated Google Drive with Gmail in April 2012. Google Drive is a collaborative environment where users can share documents, PDFs, videos, photos, and most types of files.\(^27\)

II. ECPA’S CONSENT EXCEPTION

Google does not establish consent from Gmail or non-Gmail users to satisfy ECPA’s consent exception, but may qualify for another exception. The named plaintiffs in Gmail Litigation represented a class of Gmail and non-Gmail users. Gmail users claimed that Google continuously intercepted, read, and acquired content from emails that were in transit to provide targeted advertisements and create profiles of Gmail users.\(^28\) Non-Gmail users did not receive targeted advertisements, but claimed that Google unlawfully intercepted and used the contents of their email messages in violation of ECPA.\(^29\) All plaintiffs claimed that Google did not establish consent.\(^30\)

A. LACK OF CONSENT

As ECPA stands now, Google only needs to expressly indicate that it scans Gmail users’ email content to provide targeted advertisements in its terms of service and privacy policy. When users accept the terms of service or privacy policy, Google gains consent from them. ECPA carves out an exception to an illegal interception of an electronic communication when the consent of one party to the communication is obtained.\(^31\) Thus, consent

\(^{24}\) See Marshall Kirkpatrick, Gmail’s New API: Email as Enterprise Platform, READWRITE (May 18, 2010), http://readwrite.com/2010/05/18/gmail-as-platform-for-enterprise-


\(^{28}\) See Plaintiffs’ Complaint at 6–14, In re Google Inc. Gmail Litigation, No. 5:13-md-02430-LHK (N.D. Cal. May 16, 2013), ECF No. 73.

\(^{29}\) Id. at 3–5.

\(^{30}\) Id.

\(^{31}\) Electronic Communications Privacy Act § 2511(2)(d) (“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.”) (emphasis added).
becomes a crucial consideration for any ECS provider to engage in activity that could be considered a violation of ECPA. Consent was not gained because Google never clearly indicated to any user that it would intercept and read email communications to provide targeted advertisements and to create user profiles, in its terms of service or privacy policy.\textsuperscript{32}

B. GOOGLE CLAIMS GMAIL USERS CONSENT TO AUTOMATED SCANNING

Google claimed that it is able to scan email content because email senders and recipients give consent, either expressly or impliedly.\textsuperscript{33} Google obtains express consent when Gmail users accept Google’s terms of service and its privacy policy, which occurs when users sign up for Google’s services.\textsuperscript{34} In its Motion to Dismiss, Google stated, “Gmail [p]laintiffs concede that by signing up for, or using, their Gmail or Google Apps accounts . . . they are contractually bound to Google’s terms.”\textsuperscript{35} As such, acceptance of Google’s terms of service and privacy policy indicates contractual consent.\textsuperscript{36} Courts consistently determine that these contracts, often characterized as click-wrap agreements, are “a valid way to manifest assent.”\textsuperscript{37} Courts tend to engage in an assent (or consent) analysis only to determine whether an “I Agree” button was clicked.\textsuperscript{38}

Google also argued that non-Google users impliedly consent to the automated scanning of email content when they send email to Gmail users because “all users of email must necessarily expect that their emails will be subject to automated processing.”\textsuperscript{39} Non-Gmail users are not contractually bound by Google’s terms of service or privacy policy.\textsuperscript{40} However, Google contended that non-Gmail users expect automatic processing of email by a recipient’s service provider in the course of the delivery of email and that users have no legitimate expectation of privacy in information voluntarily given to third parties.\textsuperscript{41} Google relied on the argument that the processing of email is so widely understood and accepted that the act of sending an email constitutes implied consent, as a matter of law.\textsuperscript{42}

\textsuperscript{32} See Plaintiffs’ Complaint, supra note 28, at 18–19.
\textsuperscript{34} See id.
\textsuperscript{35} Id. at 14.
\textsuperscript{36} Id.
\textsuperscript{37} Nathan J. Davis, Presumed Assent: The Judicial Acceptance of Clickwrap, 22 BERKELEY TECH. L.J. 577, 579 (2007). See also Ed Bayley, The Clicks that Bind: Ways Users “Agree” to Online Terms of Service, ELECTRONIC FRONTIER FOUNDATION (Nov. 16, 2009), https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service (adding that the creation of a legal contract by clicking the “I Agree” button turns on reasonable notice and an opportunity to review).
\textsuperscript{38} See Davis, supra note 37.
\textsuperscript{40} Id.
\textsuperscript{41} Id.
\textsuperscript{42} See id. at 20.
C. JUDGE KOH'S ORDER

Judge Koh correctly determined that Google did not obtain users' and non-users' consent to the automated scanning of email content because Google's terms of service and privacy policy did not explicitly notify plaintiffs that it would intercept users' emails to provide targeted advertisements or to create user profiles. Google claimed that Gmail users were aware of the practice because its privacy policies stated that Google may use information to "[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services." Google's privacy policies also stated that it "also use[s] this information to offer you tailored content—like giving you more relevant search results and ads." Google had attempted to gain consent by walking a thin line between explicit disclosure of its practice of email scanning and vague reference to using user information to advertise and develop new services.

Rightfully, Judge Koh determined that Gmail users' acceptance of Google's terms of service and privacy policy did not establish explicit consent. Judge Koh found that disclosures hinting at Google's practice of scanning email content were vague and unclear, and thus did not establish consent. Judge Koh explained that, "a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements."

Additionally, Judge Koh rejected Google's contention that non-Gmail users impliedly consented to the practice of email scanning since Google was unable to show any case that stood for the proposition that by sending an email to an intended recipient, the sender consented to the interception of that email by a third party. In her opinion, accepting Google's implied consent argument "would eviscerate the rule against interception."

Ultimately, the court determined that because of a lack of notice, neither Gmail users nor non-Gmail users expressly or impliedly consented to Google's interception of their emails.

D. GOOGLE'S PAST PRIVACY POLICIES

Google claims to aggressively protect user privacy while pursuing its own business interests. Google also claims that it seeks to provide clear,
easy to understand terms of service and privacy policies to help consumers make informed decisions about using its services. Google announced that its goal is to be transparent when it comes to user privacy. But Google does not achieve this by consistently failing to explicitly inform users that Gmail employs automated software to scan the content of email to place targeted advertisements and/or create user profiles.

Google’s privacy policies have been under scrutiny in the past. In 2007, Google adjusted the language in its privacy policy about the retention of user search information from “as long as it is useful,” to keeping the information for “at least 18 months and no longer than 24 months.” Google changed the language to comply with European guidelines related to data retention practices. In the recent past, Privacy International, a privacy rights organization in the U.K. named Google “the worst” company when it comes to policies that protect user privacy. Incidents of vague, unclear, or ambiguous language in Google’s privacy policies suggests that contrary to Google’s claim of transparency, Google will only disclose information of its practices if the disclosure does not disturb its business interest.

E. CONSENT IS NON-NEGOTIABLE

Judge Koh’s determination that Google does not establish consent through its terms of service and privacy policy does not adequately redress the loss of privacy through the use of email scanning because the only users who can obtain redress from the practice may be the plaintiffs in the Gmail Litigation case. If Google engages in a controversial or illegal practice, it can simply amend its terms of service and/or privacy policy to expressly indicate the practice to settle the controversy. In fact, Google did amend its terms of service and privacy policy after the litigation started. The ability for ECS providers to amend their terms and service and privacy

54 Shannon, supra note 51.
55 See Shannon, supra note 51.
56 Waters, supra note 53.
57 Shannon, supra note 51.
58 See Nate Anderson, After Criticism, Google Confirms that It Doesn’t Own Your Spreadsheets, ARS TECHNICA (Nov. 26, 2007, 8:02 PM), http://arstechnica.com/uncategorized/2007/11/after-criticism-google-confirms-that-it-doesnt-own-your-fantasy-football-spreadsheets/.
policies does not protect consumers from illegal interceptions of email communications, rather it simply informs consumers that the practice occurs.

Still, one should interpret Judge Koh’s Order as a signal to ECS providers that the privacy of personal information transmitted through email is a growing concern of consumers and the courts. How can ECPA protect privacy if ECS providers can use terms of service agreements and privacy policies to obtain user consent to access personal information? The ability to obtain consent without meaningful bargaining, or a meeting of the minds, eviscerates ECPA’s aim to protect the privacy of electronic communications. Still, many Gmail users are unwilling to forego Google’s widely used, free service in order to protect their personal information.

F. GOOGLE CANNOT OBTAIN CONSENT WITH VAGUE TERMS

The Gmail Litigation case brings to the forefront the normative question of whether the terms of service and/or the privacy policies of an ECS provider can truly establish users’ consent. Even with the explicit disclosure of practices, ECS providers cannot obtain consent from their users merely through the terms of service and privacy policies as required by traditional precepts of contract law.

Contract theorist, Professor Margaret Radin, has stated that: “[t]he traditional picture of contract is the time-honored meeting of the minds. The traditional picture imagines two autonomous wills coming together to express their autonomy by binding themselves reciprocally to a bargain of exchange.” A meeting of the minds is not obtained upon the acceptance of controversial terms of service and/or privacy policies by users of a high-demand service, like Gmail. A meeting of the minds is not met because users do not have a meaningful opportunity to bargain or negotiate Google’s terms in order to use its services.

In many cases, consent by consumers is fictional. Consent is a fiction when the terms of service or privacy policy do not disclose material information including: (1) the type of data being collected, monitored, recorded, or transmitted, (2) how the data is collected, (3) how the data may be used, and (4) whether the data may be used by a third party. Google’s terms of service and privacy policy at the time of the litigation did not meet this standard. If ECS providers want to scan the content of users’ email, then they should gain express consent from both parties of a communication to achieve ECPA’s goal of protecting electronic communications from unwanted intrusions on privacy.

ECPA should be amended to require consent from both parties to the

63 Id.
communication, when engaging in monitoring that does not fall within any other exception of ECPA to ensure non-fictional consent. This approach models the consent requirements in California, Washington, and Massachusetts.\(^{64}\)

If obtaining the consent of both parties in order to monitor email communications is unreasonable, then ECS providers should gain consent of its users through an opt-in option that expressly informs users what changes will be applied to a new, updated service, including email monitoring. For instance, if Google wants to scan emails to provide targeted advertisements and create user profiles, then permitting users to opt in after a clear explanation of the practice would indicate explicit consent, made on an informed basis, where a meeting of the minds is clear. However, in light of this proposed approach, another hurdle to protect privacy of email communication still exists.

III. THE “ORDINARY COURSE OF BUSINESS” EXCEPTION UNDER ECPA

Even if Google is unable to establish consent from its users, ECPA’s ordinary course of business exception applies to Google’s email scanning practice since the practice does not involve humans listening to private communications. All interceptions under ECPA require the use of device.\(^{65}\) Excluded from the definition of a device is, “any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business.”\(^{66}\) The provision indicates that an ECS provider using equipment while engaged in the ordinary course of its business does not intercept a communication because it does not use a “device” as defined by the statute.\(^{67}\) This exception is particularly useful in the context of Internet communications since the transmission of email requires the use of equipment that accesses the content of email to route the message.\(^{68}\)

The commercial Internet had barely emerged when Congress enacted ECPA,\(^{69}\) yet legislators were aware of email use at the time.\(^{70}\) The ordinary course of business exception highlights the intent of legislators to allow limited access to the content of electronic communications to maintain an ECS. Specifically, Congress recognized that “[t]he provider of electronic

---


\(^{65}\) Electronic Communications Privacy Act § 2510(4) (stating “‘intercept’ means 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”) (emphasis added).

\(^{66}\) Electronic Communications Privacy Act § 2510(5)(a).

\(^{67}\) See Bruce E. Boyden, Can a Computer Intercept Your Email?, 34 CARDOZO L. REV. 669, 678 (2013).


communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain.”

A. THE “ORDINARY COURSE OF BUSINESS” EXCEPTION AS JUDGE KOH INTERPRETED IT

Judge Koh indicated that a business model, like that of Gmail, does not fall within the ordinary course of business exception because the exception should be read narrowly. Under her reading, the ordinary course of business exception applies only when an ECS “provider’s interception facilitates the transmission of the communication at issue” or is necessary and incidental to that communication.

Judge Koh found that Google intercepted email content to allegedly “create user profiles and to provide targeted advertising” and not solely to transmit email. Judge Koh determined that the phrase “ordinary course of business” should be split, to enable the term “ordinary” to give effect to and limit the phrase “course of business.” Judge Koh found that the term “ordinary” does not allow everything done in the course business to fall within the exception. The purpose of this distinction was to match the phrase “ordinary course of business” to another provision in ECPA, the necessary incident provision.

This separate provision of ECPA, which is not included in ECPA’s definition of a device, provides another exception to an illegal interception and states that:

It shall not be unlawful under this chapter for an . . . agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic 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).

Judge Koh suggested that this provision indicates legislators’ intent to limit the ordinary course of business exception to interceptions that are incidental to the function of an electronic communications service. Judge Koh’s interpretation suggests that the second clause of the above provision, indicating that, “a provider of wire communication service . . . shall not utilize service observing or random monitoring except for mechanical or

73 Id. at 8.
74 Id.
75 Id.
76 Id.
77 Electronic Communications Privacy Act § 2511(2)(a)(i).
78 See Koh Order, supra note 72.
service quality controls,’”79 applies to ECS providers, like Google.

However, in its Senate Report, Congress distinguished between wire communication providers and ECS providers.80 “In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service.”81 (emphasis added). The Senate Report goes on to state that ECS providers may have to monitor communications in order to properly route, terminate, or otherwise manage the individual messages. Although such “monitoring functions . . . may be necessary to the provision of an electronic communication service, [they] do not involve humans listening in” and are not prohibited.82 It appears that Congress gave ECS providers more leeway to monitor electronic communications, beyond mechanical and/or service quality controls checks, including that which is necessary to operate their services. Certainly, the ability to generate advertising revenue through targeted advertisements is necessary to the provision of Gmail given that increased revenue allows Google to offer increased storage and a range of applications, as a free platform.

B. CRITIQUES OF JUDGE KOH’S DECISION

A question arises as to whether Judge Koh read ECPA’s “ordinary course of business” exception and the necessary incident provision fairly.83 Judge Koh acknowledged that there must be “some link between the alleged interceptions at issue and its ability to operate the communication system.”84 There is a strong link between the revenue gained from targeted advertisements and the ability to provide a free email platform and to improve that platform,85 especially in light of the stated purpose of ECPA, to “minimiz[e] intrusions on the privacy of system users” and to protect “the business needs of electronic communications system providers” (emphasis added).86

Judge Koh’s interpretations of these provisions are not unfounded. However, a narrow reading is inconsistent with the balance Congress sought to strike in protecting the privacy of electronic communications and

79 Electronic Communications Privacy Act § 2511(2)(a)(i).
81 Id.
82 Id.
85 SeeDefs. Mot. to Dismiss at 15, In re Google Inc. Gmail Litigation, No. 5:13-md-02430-LHK (N.D. Cal. June 13, 2013) (noting Google’s privacy policy suggests the information gathered from users is used to “[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services.” The clarity of Google’s privacy policy is discussed above in Part II, but this language attempts to model itself after the Electronic Communications Privacy Act § 2511(2)(a)(i)).
promoting the advancement of technology.\textsuperscript{87} It inappropriately expands the protection of electronic communications provided under ECPA. Judge Koh seems to view Gmail as simply a tool for the transmission of email—which is shortsighted. Instead, Gmail is an app-enabled platform that allows email, instant messaging, social networking through Google+, video conferencing, Google Docs, calendars, and more.\textsuperscript{88}

C. THE “ORDINARY COURSE OF BUSINESS” EXCEPTION AS JUDGE GREWAL INTERPRETED IT

Judge Koh and Judge Grewal vastly differ in their interpretation of the “ordinary course of business exception” under ECPA. Judge Grewal’s approach in Privacy Policy Lit. centered on Google’s ability to collect information from its services to provide targeted advertisements, yet Judge Grewal granted Google’s motion to dismiss.\textsuperscript{89} In contrast to Judge Koh, Judge Grewal accused the plaintiffs of utterly failing “to cite any authority that” rejects the inexplicably plain language of ECPA, which “excludes from the definition of a ‘device,’ a provider’s own equipment used in the ordinary course of business.”\textsuperscript{90} Ultimately, Judge Grewal found that plaintiffs did not identify a concrete harm arising from Google’s practice of gathering information from one Google service and using the information to provide targeted advertisements in another Google service.\textsuperscript{91}

The divergence in interpretations of the “ordinary course of business” exception in Judge Koh’s and Judge Grewal’s opinions reflect the inconsistent application of the exception. The difference settling each motion to dismiss demonstrates the difficulty courts have in determining whether new forms of data collection fall within the exception.\textsuperscript{92} Judge Grewal’s decision is consistent with the exception’s plain language and also comports with Congress’ intent to protect privacy while balancing the business needs of ECS providers.

\textsuperscript{87} See id. (relying on Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983), which stated that “[t]he phrase ‘in the ordinary course of business’ cannot be expanded to mean anything that interests a company.” On the other hand, Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553, 559 (2d Cir. 2000) found that,”[l]egitimate business reasons support the continual recording of all incoming and outgoing telephone calls.” The court in Arias found that the defendant did not violate the Wiretap Act even though it recorded telephone calls because “[t]he common understanding of ‘ordinary course of business’ are amply satisfied.”) (emphasis added). See also Berry v. Funk, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (finding that actions are in the ordinary course of business if they are “justified by a valid business purpose, or . . . shown to be undertaken normally.”) (quoting Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994)).


\textsuperscript{89} See Privacy Policy Lit. at 6, In re Google, Inc. Privacy Policy Litigation, No. C12-01382 PSG (N.D. Cal. Dec. 28, 2012), 2012 WL 6738343 (Judge Grewal’s discussion of Google’s data collection practices only briefly addressed ECPA’s ordinary course of business exception. Judge Grewal did not discuss users’ consent, and thus his decision only comments on the ordinary course of business exception’s plain language.).

\textsuperscript{90} Id.

\textsuperscript{91} See id.

\textsuperscript{92} See id.
The scanning of email content to provide targeted advertisements is part of Google’s ordinary business practice since it enables Google to sell ads at higher rates and assures advertisers that users have an interest in their product. In Gmail Litigation, Google asserted that Gmail’s advertising-based business model generates revenue, enabling Google to provide Gmail for free to the public. Gmail’s free platform has supported the practice of targeted advertising since as early as 2004. In fact, advertising plays such a central role in Google’s overall operations that in 2009, advertising made up 97 percent of all of Google’s revenues. Further, Gmail offers services beyond the transmission of email, and the use of targeted advertising supports these services. In this sense, the use of targeted advertisements could be considered necessary and incidental to the function of the platform. To construe otherwise would stagnate Gmail as a service only offering email. Other prominent email service providers engage in the practice of scanning email content to deliver targeted advertisements, including Yahoo. For that reason, the use of automated equipment to scan email to provide targeted advertisements can also be understood as an industry standard.

ECS providers like Google need to monitor the content of communications to scan for viruses or spam. This type of monitoring is an acceptable practice because the information gathered is not disclosed and occurs strictly for the transmission of relevant email. The scanning of electronic communications for viruses or spam should be considered a known industry standard because it is well-known to consumers and industry insiders. Further, if a known industry standard becomes prevalent and widely accepted then that practice should fall under the ordinary course of business exception. Judges should consult an industry standard group to determine whether a practice is known in the industry. A neutral organization that can confirm industry standards will eliminate inconsistent applications of the exception. Congress could call an agency or organization to update courts on known industry standards that may fall within the ordinary course of business exception at the time of an alleged interception.

IV. GOOGLE’S AUTOMATED SCANNING SHOULD BE ILLEGAL EVEN IF

95 See Saul Hansell, The Internet Ad You Are About to See Has Already Read Your E-mail, N.Y. TIMES (June 21, 2004), http://www.nytimes.com/2004/06/21/business/media-business-advertising-internet-ad-you-are-about-see-has-already-read-your-e.html.
98 See id. at 3.
Even though Google does not gain consent to scan email content, the practice does fall within ECPA’s ordinary course of business exception. Yet users lose privacy even if Google gains their consent by acceptance of terms of service or privacy policies that explicitly disclose the practice or if the practice falls within an ECPA exception. Underlying Google’s defense of email scanning is the notion that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” The third party rule, as articulated in Smith v. Maryland, supports the notion that Gmail users and people who email Gmail users “have no legitimate expectation of privacy” in the content of their emails. As of June 2012, there were 425 million active monthly users of Gmail. Given the number of people who use Gmail, and the number of people who email Gmail users, the proposition suggests that email users have to accept privacy intrusions in order to use free email services.

The idea that the contents of your emails are subject to the third party rule stretches the doctrine of Smith v. Maryland. In Smith, the court determined that there was no legitimate expectation of the privacy in the phone numbers one dials. Subsequent courts have discussed the reach of the third party doctrine and have noted that the Court in Smith distinguished pen registers (a device used to record numbers dialed on a phone line) from more intrusive surveillance techniques on the basis that pen registers did not acquire the contents of communications.

In the digital age, people who use email have an expectation of privacy in the content of their correspondence. Most of us use email to communicate private ideas to close friends and lovers; we communicate with our employers; we discuss medical and legal issues, as well as, a host of other personal matters. The contents of these emails are more personal than a phone call or even a face-to-face conversation.


100 Maryland, 442 U.S. at 743-44.


102 Sean Ludwig, Gmail Finally Blows Past Hotmail to Become the World’s Largest Email Service, VENTUREBEAT (June 28, 2012, 5:05 PM), http://venturebeat.com/2012/06/28/gmail-hotmail-yahoo-email-users/.

103 See Simpson, supra note 101.

104 Maryland, 442 U.S. at 745.

105 See United States v. Forrester, 512 F.3d 500, 513 (9th Cir. 2007) (finding email and internet users have no expectation of privacy in the to/from information of their email messages or IP addresses of the websites they visit since the information is provided to and used by internet service providers for the purposes of directing the routing of information, thus email to/from addresses and IP addresses are considered addressing information).

106 Steven R. Morrison, What the Cops Can’t Do, Internet Service Providers Can: Preserving Privacy in Email Contents, 16 VA. J.L. & TECH. 253, 255 (2011); see also United States v. Warshack, 631 F.3d 266, 274, 286–87 (6th Cir. 2010) (indicating that defendant “Warshack enjoyed a reasonable expectation of privacy in his emails,” and “the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.”).
of other issues.\textsuperscript{107} The widespread use of a popular email service should not come at the cost of privacy in our most intimate conversations.

ECPA does not adequately address the intrusion of privacy by automated scanning of email and courts have struggled to apply “the outdated statute to modern communications.”\textsuperscript{108} Still, the loss of privacy needs to be addressed, given society’s reasonable expectation of privacy of email content and the intention of Congress to enact legislation to prevent unlawful interceptions of electronic communications.

A. ECPA: A POOR FIT

As ECPA currently stands, the automated scanning of email content does not involve humans listening and is not clearly prohibited, yet ECPA is undercut by the emergence of technology that can read and interpret email content without human intervention. In its Motion to Dismiss, Google argues that it “applies automated systems for the delivery of email . . . . These systems are also used to display advertisements targeted to email content . . . . The processes related to Google’s automated scanning are completely automated and involve no human review.”\textsuperscript{109} Google suggests that ECPA is not violated during the process of email scanning since no human intercepts the email or reviews its contents. Further, at least one legal scholar, Bruce Boyden, agrees with Google, stating that “the legal status of automated processing, if it is done without advance consent, is unclear.”\textsuperscript{110} He argues that, “automated processing that leaves no record of the contents of a communication does not violate the ECPA, because it does not ‘intercept’ that communication within the meaning of the Act.”\textsuperscript{111}

The legal status of automated scanning without advance consent is unclear because ECPA’s prohibition on the interception of electronic communications does not fit squarely when the interception is completely automated. The legislative history and the plain language of ECPA suggest that the statute prohibits only human interceptions of electronic communications.\textsuperscript{112} Since no human intercepts email content, ECPA is difficult to apply and should be amended to clarify whether an automated process that captures email content is an interception within the meaning of the statute. The widespread use of automated processes by ECS providers, and the ability to capture and comprehend a wealth of personal information is analogous to a human doing the same thing. ECPA was enacted to prohibit this type of data collection without express consent.

\textsuperscript{107} Morrison, supra note 106, at 255.
\textsuperscript{110} Bruce E. Boyden, Can a Computer Intercept Your Email?, 34 CARDozo L. REV. 669 (2013).
\textsuperscript{111} Id.
\textsuperscript{112} See id. at 676.
The question of whether ECPA prohibits automated interceptions of communications should depend on what is done with the collected information. For instance, if the interception is only for transmission and routing of email then an exemption to ECPA liability arises. If the interception is for other purposes including providing targeted advertisements or user profiles, then the interception should be prohibited since the practice includes reading and comprehending email content to display targeted advertisements. If ECPA was drafted to protect private conversations and email has become a primary mode of private communication, then the content of email communication should be protected. Therefore, ECPA’s language should be updated to indicate that illegal interceptions may occur whether or not a human ever reviews the information collected to resolve any ambiguity in the legal status of automated scanning without advance consent, if no other exception applies.

V. CONCLUSION

The purpose of ECPA is to “protect[] the privacy of information in any electronic form, . . . adapting the law to the technology of the present and future, rather than the past.” ECPA’s legislative purpose indicates that the statute must address and adapt to changing technology. ECPA needs comprehensive revision to do this. The automated scanning of email content will likely increase and become more intrusive as computer technology develops. Automated processes pose a high risk of harm to individuals because private information may be improperly used or disclosed. These risks require that automated email scanning be regulated.

The problem with trying to fit a square peg in a round hole is the incongruent fit. Similarly, Judge Koh’s dissection of ECPA’s ordinary course of business exception attempts to allow plaintiffs to pursue a cause of action for a privacy violation, but does not fit ECPA’s plain language and legislative history. Accordingly, her decision does not fit within ECPA’s restrictions and is inconsistent with at least one other judge’s interpretation of the ordinary course of business exception. An industry group or organization appointed by Congress could inform courts on known industry standards to determine whether a practice is within the ordinary course of business to protect consumers from unlawful

113 Id. ("If some sort of record is created that preserves or conveys the 'substance, purport, or meaning' of the communication for human review, then the act of creating that record is an interception under the Act.").
114 See Plaintiffs’ Complaint at 1–2, In re Google Inc. Gmail Litigation, No. 5:13-md-02430-LHK (N.D. Cal. May 16, 2013), ECF No. 73.
interceptions of private email communications and avoid differing interpretations of the statute’s exceptions. Plaintiffs should be able to pursue and recover relief for any legitimate violation of privacy in electronic communications, much like they can when they are victims of unlawful wiretaps. The balance that Congress seeks between protecting privacy and allowing technological development is lost when different courts apply different standards to the same statute.

Further, ECPA should require that ECS providers obtain the consent of both parties to a communication, possibly through opting-in to a practice, whenever ECS providers want to update their services that will implicate the privacy of communications. These steps will reinforce private communications by disallowing technological advancement to supersede statutorily protected values, which are informed by the concerns of legislators, voters, and consumers. Privacy should not be sacrificed to technological advancement when both can be maintained.