UIC John Marshall Journal of Information Technology & Privacy Law

Volume 33 | Issue 3 Article 3

2018

Nothing Personal, It's Just Business: How Google's Course of Business Operates at the Expense of Consumer Privacy, 33 J. Marshall J. Info. Tech. & Privacy L. 187 (2018)

Kayla McKinnon

NOTHING PERSONAL, IT'S JUST BUSINESS: HOW GOOGLE'S COURSE OF BUSINESS OPERATES AT THE EXPENSE OF CONSUMER PRIVACY.

KAYLA MCKINNON*

I. INTRODUCTION

They appear high up on billboards and beneath the street on subway cars. They appear on outdoor benches and inside taxi cabs. They appear on small cards and large spanning digital screens. Just as the thought of them appearing elsewhere seemed impossible, along comes online advertising. Although the concept of online advertising is no new feat for advertising agencies, targeted advertising is the newest tactic employed and it is on the rise. [1]

With a non-targeted advertisement, such as those seen on a billboard or on a promotional card, consumers have the ability to disregard the message if they are not interested in the product or service offered. However, with targeted advertising, advertisements of products or services viewed by consumers follow them even after exiting the website.[2] For example, a student in class enters a search for a pair of boots through Google's search engine and opens the first link that appears on the results page. The student scrolls through the department store's website for a pair of boots and clicks on a pair, but before getting the chance to purchase them, the professor calls on her and she exits the

---

* Kayla McKinnon is from Crown Point, Indiana and received a Bachelor of Arts degree in Psychology from Indiana University in 2015. Kayla is a Juris Doctorate candidate at The John Marshall Law School, expecting to graduate in May 2018. She would like to thank her mother for her endless support and encouragement throughout the entire process of getting this Comment published. She would also like to thank the members of the Journal of Information Technology & Privacy Law for their assistance in editing this Comment.

1. Laura Sydell, *Smart Cookies Put Targeted Online Ads On The Rise*, NATIONAL PUBLIC RADIO, http://www.npr.org/templates/story/story.php?storyId=130349989 (last accessed September 12, 2016).

2. Evan Seligner and Shaun Foster, *How'd My Avatar Get Into That Sneaker Ad?*, SLATE (Jan. 4, 2012 7:10 AM), http://www.slate.com/articles/technology/future_tense/2012/01/behaviorally_targeted_ads_and_the_ethical_dilemmas_behind_building_consumers_into_ads_.html.

website. Later that night, while again using Google's search engine, the student notices an advertisement from the department store with a picture of the exact pair of boots that she had been contemplating purchasing earlier that day. How did the advertisement "know" to present that specific pair of boots on a website that was not the department store's own? This question has been asked by numerous consumers with similar occurrences. The bigger question, however, is where the line on Internet privacy can be drawn.[3]

The Northern District of California, as well as circuit courts throughout the country, have addressed the issue of whether companies like Google and Yahoo can use consumers' personal identification information and auction this information off to advertising agencies that are hungry for a spot on the consumer's webpage.[4] Courts have decided these types of cases; but, the trouble is that—even within the same district [5] —there is no agreement as to whether companies can in fact do this or not, in part, because of the Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"). [6]

This disparity stems originally from what the Wiretap Act [7] defines as electronic *communication*. [8] Today's electronic communication service providers go beyond the communications originally covered at the time of the statute's enactment. Consumers today are on the Internet buying and exchanging products or services, banking, paying credit card bills, ordering Chinese food, watching television series, streaming live sporting events, video chatting with relatives, and engaging in numerous other activities that touch several aspects of the current citi-

---

3. Sydell, *supra* note 1.

4. Darla Cameron, *How Targeted Advertising Works*, THE WASHINGTON POST, August 22, 2013, https://www.washingtonpost.com/apps/g/page/business/how-targeted-advertising-works/412/.

5. The Northern District of California alone has issued the contrasting opinions that are the subject of this comment. *See In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784 (N.D. Ca. Sept. 26, 2013*); In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 U.S. Dist. LEXIS 171124 (N.D. Ca. Dec. 3, 2013); *Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 U.S. Dist. LEXIS 107918 (N.D. Ca. Aug. 12, 2016).

6. The Northern District has come out with opposing interpretations, spaced between less than four months, of the Wiretap Act where the court has narrowly and broadly construed the statute. *See In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *1; *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *1.

7. 18 U.S.C. § 2510 (2012).

8. Under the Wiretap Act, "electronic communication" includes, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system…" 18 U.S.C. § 2510 (2012).

zen's life in the 21st century.[9]

In determining whether to find for the individual consumers or for the Internet moguls, courts have looked to the interpretation of the Wiretap Act, specifically the "ordinary course of business" exception.[10] This exception has both a narrow and broad interpretation. [11] Whether a court narrowly or broadly construes this exception dramatically effects whether or not consumers are able to obtain the remedy they seek under the Wiretap Act. In the Northern District of California, courts have opposing interpretations of the Wiretap Act, [12] leaving consumers without a clear precedent telling them what is to come of their own claims.

This Comment will seek to examine the inconsistencies amongst court interpretations of the Wiretap Act, as well as the coverage of the Wiretap Act, to determine what Congress intended in passing this legislation, and how it coincides with current consumer Internet activity. Part I of this comment will provide background information on targeted advertising and the Wiretap Act, specifically addressing the "ordinary course of business" exception. Part II will delve into contrasting opinions within the Northern District of California and circuit courts throughout the United States. It will also address the Wiretap Act and its fitness to stand alone in defense of consumers—or companies—against the current state of Internet activity. Part III will propose the narrow interpretation of the Wiretap Act, or in the alternative, new legislation to encompass protection of more modern uses of the Internet by consumers.

II. BACKGROUND

Targeted advertising, or online "behavioral advertising," tracks a consumer's activities online—from a search for the top-rated mechanics

---

9. In a study performed by the Pew Internet Project, 33% of people surveyed reported using the Internet to purchased goods; 44% reported they use the Internet for banking and bill paying; 16% reported using the Internet to watch videos; and 79% reported using the Internet to communicate with family and friends. Deborah Fallows, *The Internet and Daily Life,* PEW RESEARCH CENTER (Aug. 11, 2004), http://www.pewinternet.org/2004/08/11/the-internet-and-daily-life/.

10. "The 'first step in interpreting a statute is to determine whether the language at issue has plain and unambiguous meaning.' In so doing, the court 'must begin with ... the assumption that the ordinary meaning of that language accurately express the legislative purpose.'") *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *33.

11. Judge Koh and Judge Grewal both address the opposing interpretation, that being narrow or broad, of the Section 2510 (5)(a)(i) exception of the Wiretap Act throughout each of their respective opinions. *See id*. at *32-37; *Matera*, 2016 U.S. Dist. LEXIS 107918 *25-27.

12. *See generally In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784; *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124.

in the area to browsing a course catalog—in order to tailor advertisements targeted to a consumer's interests. [13] Google does this through "[c]ookies and similar technologies," namely DoubleClick. [14] DoubleClick is a third-party advertising company operated by Google, [15] and a member of the Network Advertising Initiative ("NAI") [16] that serves to generate and direct digital advertising across Google's services. [17] Information is collected and stored via a cookie or similar technology each time a user visits a Google service. [18] Google then links the information to the DoubleClick cookie, [19] allowing advertisers to control how often and how long advertisements are shown. [20] To illustrate, suppose a user searches for a pair of boots through Google's search engine and clicks on a website selling that pair. The user then subscribes to that website and begins receiving e-mails about items for purchase. When the user does this, a DoubleClick cookie is placed on his or her browser, and the more the user searched for those boots and received e-mails from that website, the more targeted advertisements he or she would see across all platforms.[21]

There is more at stake, however, than the potential dissemination of which pair of boots the student is currently eyeing. Other personal

---

13. FEDERAL TRADE COMMISSION, *Online Behavioral Advertising, Moving the Discussion Forward to Possible Self-Regulatory Principles,* https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf (last accessed September 13, 2016).

14. *Google Privacy & Terms,* GOOGLE, https://www.google.com/policies/privacy/ (Aug. 29, 2016).

15. NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/participating-networks (last accessed October 14, 2016).

16. The Network Advertising Initiative (NAI) is a not-for-profit, self-regulatory association founded in 2000, with a total of 100 member companies. NETWORK ADVERTISING INITIATIVE, *supra* note 15.

17. *Id*.

18. "We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites." *Google Privacy & Terms*, GOOGLE, *supra* note 14.

19. *Id*.

20. Joanna Geary, *DoubleClick (Google): What is it and what does it do?* (Apr. 23, 2012), https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring.

21. Sydell, *supra* note 1.

identification information ("PII"), such as a user's age, gender, birth date, zip, and income, have the potential to be exposed to the Internet by targeted advertisements as well. [22] Electronic communication service providers, such as Google, have this information at their disposal after consumers voluntarily offer these details when they register for an account. [23] With this information readily available, the bidding war begins. [24] Advertising networks bid in real-time based on the information they are receiving regarding consumers, and the highest bidder is the advertisement the consumer will see on the next site he or she visits. [25]

According to eMarketer, targeted advertising is anticipated to grow by six percent in the next four years. [26] That statistic may not be surprising as the Internet has become a primary avenue for accessing several aspects of life in the 21st century. [27] However, despite its popularity, "the Internet remains a relatively uncharted frontier in terms of general oversight and control by federal…authorities." [28] Through committees, the House of Representatives launched inquiries into the computer and invasion of privacy as far back as 1966, [29] but unlike the rapidly evolving nature of technology, legislation has lagged.

Congress has emphasized, for example, protection of consumer reporting agencies, [30] education records, [31] and financial records.[32] In 1986, privacy protection extended to new emerging forms of technology, including cellular telephones, private satellite transmissions, paging devices, and electronic mail messages via the computer, through the ECPA. [33] Additionally, the ECPA amended the Wiretap Act of 1968 to include interception of digital and electronic communications, such as the computer. [34]

---

22. *Id*.
23. *Id*.
24. *Id*.
25. *Id*.
26. *Id*.
27. Major R. Ken Pippin, *Consumer Privacy on the Internet: It's "Surfer Beware,"* 47 A.F.L. Rev. 125 (1999).
28. *Id*.
29. Harold C. Relyea, *Personal Privacy Protection: The Legislative Response*, Report No. RL30671, U.S. CONGRESSIONAL RESEARCH SERVICE, Mar. 21, 2001 *available* at https://www.everycrsreport.com/reports/RL30671.html.
30. *Id*. at 5.
31. *Id*. at 11.
32. *Id*. at 12.
33. *Id.*
34. Prior to the amendment in 1986 through the Electronic Communications Privacy Act, the Wiretap Act of 1968 focused on the "interception of conversations using 'hard' telephone lines." With the amendment, the Wiretap Act now covers digital and electronic communication, as well as "hard" telephone conversations. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-22, *available at* https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

The Wiretap Act, as amended by the ECPA, prohibits the intentional interception of "wire, oral, or electronic communications."[35] The Wiretap Act covers "wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers." [36] Under this statute, emails, telephone conversations, and electronically stored data are protected. [37] The Wiretap Act is intended to protect an individual's privacy by providing recourse against another who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." [38] "Intercept" is defined in the Wiretap Act 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." [39] There are exceptions, however, one of which is a primary reason for confusion in the Northern District of California. Section 2510 (5)(a)(i) of the Wiretap Act excludes from the definition of "electronic, mechanical, or other device" 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;
>
> (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." [40]

The first exception is applicable to users or subscribers of electronic communication service providers, while the second exception is reserved for the providers of the electronic communications service. [41] From this language, specifically "ordinary course of business," the Northern District of California and circuit courts throughout the country maintain different interpretations of the level of responsibility of electronic communication service providers in regards to the PII they obtain; thus, resulting in unclear precedent.

Although targeted advertising—in its earliest form—dates back to

---

35. *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *1.
36. 18 U.S.C. § 2510-22 (1986).
37. *Id.*
38. *In re Google, Inc. Privacy Policy Litig.,* 2013 U.S. Dist. LEXIS 171124, at *1.
39. 18 USCS § 2510.
40. 18 USCS § 2510 (5)(a)(i-ii).
41. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *1.

1994, [42] the issue was only recently brought before the court system. Overall, between 2001 and 2016, courts have interpreted the "ordinary course of business" exception narrowly; that is, except for the Northern District of California. [43] In this one district, the exception has been interpreted both narrowly and broadly, exempting interceptions that either facilitated and or are incidental to the operation of the electronic communication service provider, [44] or any and all interceptions done in the course of an electronic communication service provider's ("ECSP") customary and routine practice. [45] Through either interpretation, an interception occurs when there is an "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." [46] With the concentrated amount of technology and Internet companies located in Silicon Valley, it is no surprise why the Northern District of California has such a high volume of cases regarding this issue. Because of this, it is crucial that this district court set the record straight—interpreting the "ordinary course of business" exception of the Wiretap Act narrowly to keep electronic communication service providers at bay and consumers' privacy untouched.

III. ANALYSIS

Google stresses that online-targeted advertising is beneficial to both sides of the browser—both the user and the service provider—as it allows Google to continue providing its services to the public free of charge.[47] Conversely, users have felt no such benefit, and claim targeted advertising is an invasion of privacy.[48] When both sides are presented to the court, under the Wiretap Act, judges first must determine whether this practice is within Google's ordinary course of business. [49]

---

42. Russell Glass, *Data and the Rise of Online Advertising*, LinkedIn, https://www.linkedin.com/pulse/data-rise-online-advertising-russell-glass (last accessed September 12, 2016).

43. By interpreting the "ordinary course of business" exception broadly, Judge Grewal found that targeted advertising by Google to fall within its coverage. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124 at *1.

44. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *30-1.

45. *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *33 (N.D. Ca. December 3, 2013).

46. 18 USCS § 2510(4) (1986).

47. Christopher Batiste-Boykin, Comment, In Re Google Inc.*: ECPA, Consent, and the Ordinary Course of Business in an Automated World,* 20 INTELL. PROP. L. BULL. 21, 34 (2015).

48. *In re Google, Inc. Privacy Policy Litig.,* 2013 U.S. Dist. LEXIS 171124, at *7.

49. "The 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." *In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *27 (N.D. Ca. September 26, 2013). For

A. THE ORDINARY COURSE OF BUSINESS IN SILICON VALLEY

Because of the companies located within the jurisdiction of the Northern District of California—tech giants such as Google, Yahoo, and Facebook—Silicon Valley has become more than fertile ground for technology, but also for lawsuits. Alongside the evolution of technology are privacy concerns, and Google has struggled to toe the line between invasion and necessity with its privacy policy. [50]

As part of Google's Privacy Policy, Google collects information through its search engine, cookies, information provided to affiliated sites by users, and links followed by users. [51] One purpose for doing so is for "the display of customized content and advertising" and assembly of user profiles. [52] *In re Google Inc. v. Gmail Litigation*, users of Google's Gmail service took issue with the above practices and brought suit in the Northern District of California. [53] The users and non-users, as a class consolidated from seven cases, alleged that Google violated the Wiretap Act through the "operation of the Gmail system by intentionally intercepting the content of emails that were in transit to create profiles of Gmail users and to provide targeted advertising." [54] In response, Google vindicated the reading of emails as within the "ordinary course of business" exception, under the Wiretap Act. [55] The outcome of this case was dependent upon a narrow or broad interpretation of the exception. According to Judge Koh, a narrow interpretation was most appropriate and justified for three reasons. [56] First, the court looked to the effect of the modifier "ordinary" on "course of business," and found that the word "ordinary" made it clear that not everything done by Google in the "course of business" would be covered by the exception, in contrast to Google's contention. [57] Secondly, case law revealed that the reasons for the alleged interception must be "legitimate," and "cannot be expanded to mean *anything* that interests a company." (emphasis added)

---

example in *In re Google Inc.*, "the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email." *Id.*

50. Since 2009, Google has updated its privacy policy 23 times, with the latest update published on August 29, 2016. In 2015 alone, the privacy policy was updated four times. *Google Privacy Terms*, *supra* note 14.

51. *In re Google Inc. Gmail Litig.,* 2013 U.S. Dist. LEXIS 172784, at *12.

52. *Id*.

53. The case before the court was brought as a class of consolidated actions from 2008 through 2013 under state and federal anti-wiretapping laws. *Id*. at *6.

54. In addition to claims brought under the Wiretap Act, Plaintiffs alleged violations of California, Pennsylvania, Maryland, and Florida anti-wiretapping statutes. *Id*. at *14.

55. *Id*. at *26.

56. *Id*. at *40 (N.D. Ca. September 26, 2013).

57. *In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *29.

[58] For ECSPs, like Google, the "alleged interception must demonstrate the interception facilitated the communication service or was incidental to the functioning of the provided communication service." [59] Such a demonstration must show "some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good." [60] Here, Google's alleged interception was for the purposes of targeted advertising and creation of user profiles, neither of which established a nexus between the alleged interception and the ability to transmit emails. [61] Lastly, the statutory scheme of the Wiretap Act and legislative history supported a narrow interpretation of the exception, where Congress intended that for an interception to fall within the exception, it must be essential to that service. [62] Moreover, the court found that Congress did not intend unlimited latitude for ECSPs to engage in interception as would serve to benefit their business. [63]

The above reasoning supports a narrow interpretation of the "ordinary course of business" exception, and when applied to the instant case, the court found that Google's contentions were beyond the shield of the exception. [64] Due to Google's collection of information for the purposes of targeted advertising and user profiles, separate and unrelated from that of transmitting emails, [65] the alleged interception was neither essential nor incidental to the Gmail services. [66]

Just four months later, Google was brought before the Northern District of California again in *In re Google, Inc. Privacy Policy Litig.* under similar violations of the Wiretap Act and claimed protection under the same exception; however, this time, Google walked out of the court house doors with a ruling in its favor. [67] Judge Grewal, writing on

---

58. The court cites *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012), in support of a narrow interpretation of the "ordinary course of business" exception after the interception was deemed incidental and related to the delivery of email. *Id.* at *29-30.

59. *Id.* at *30.

60. *Id.* at *40.

61. *Id.*

62. *Id.* at *36-37.

63. The court determined this intent from looking at the first "ordinary course of business" exception, contained in 18 U.S.C. § 2511(2)(a)(i), applying to users or subscribers of ECSPs. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *28-29, 35-36.

64. *Id.* at *40-41.

65. Plaintiffs offer services provided by Google that are related to the service of email include "spam filtering antivirus protections, spell checking, language detection, and sorting." *Id.* at *41.

66. *Id.*

67. The court granted Google's Motion to Dismiss, dismissing Plaintiffs' amended complaint with leave to amend. *In re Google, Inc. Privacy Policy Litig.,* 2013 U.S. Dist. LEXIS 171124, at *2.

behalf of the court, took issue with the narrow interpretation of the "ordinary course of business" exception supported by Judge Koh (in *Gmail Litigation*), after analyzing the statutory text and caselaw. Rather than looking at the term "ordinary," as Judge Koh had done, [68] Judge Grewal turned his attention to the term "business" and the plain meaning it had within the exception. [69] The court determined that with the term "business," Congress intended to include more than just electronic communication services as part of the "ordinary course." [70] Thus, business regarding targeted advertising by Google fell within the exception as part of the ordinary course. [71] Additionally, case law from the Second Circuit further supports the broad interpretation, finding no interception where processing of emails continued after termination of the account.[72]

Judge Grewal also posed the issue of defining what is "necessary," in this case to the delivery of Gmail, with respect to the "ordinary course of business." [73] Questions of where the line could be drawn as to what services are necessary here to transmit email, were unclear to the court.[74] The plaintiffs likewise were unable to draw this line in order to support their argument that Google's activities were "unnecessary and thus fell outside of the 'ordinary course of business.'"[75] With this reasoning and above analysis by Judge Grewal, the court found in favor of Google.[76]

These two opinions from the Northern District of California are illustrations of the difficulty in applying new methods of data collection to the "ordinary course of business" exception.[77] However, early in 2016, the court again addressed the interpretation of the exception in relation to Google's privacy policy.[78]

In *Matera v. Google, Inc.*, the Northern District of California evalu-

---

68. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *29.

69. *In re Google, Inc. Privacy Policy Litig.,* 2013 U.S. Dist. LEXIS 171124, at *33.

70. Those services beyond those provided for electronic communication included "customary and routine business practices." *Id*.

71. *Id*. at *33-34.

72. *Id*. at *34-35 (citing *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005)).

73. *Id*. at *35-36.

74. In determining where to draw the line of necessity, Judge Grewal asked "is it really 'necessary' [to] do more than just comply with email protocols such as POP, IMAP, and MAPI? What about spam-filtering or indexing?" *Id*. at *36.

75. *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *6-37.

76. *See id*. at *36.

77. *See* Batiste-Boykin, *supra* note 47 at 33 (2015).

78. *See Matera*, 2016 U.S. Dist. LEXIS 107918, at * 4, 7. (Plaintiffs originally brought suit on behalf of a class for violations of the Wiretap Act, California's Invasion of Privacy Act, Maryland's Wiretap Act, Florida's Wiretap Act, and Pennsylvania's Wiretapping and Electronic Surveillance Control Act regarding Google's operation of Gmail).

ated the interpretations set forth by Judge Koh [79] and Judge Grewal [80], and reasoned that the statutory text's plain meaning, case law, and statutory scheme supported the narrow interpretation of the "ordinary course of business" exception.[81] In order to satisfy the narrow interpretation, an ECSP must establish "some nexus between the need to engage in the alleged interception and the [provider's] ultimate business, that is, the ability to provide the underlying service or good," as outlined in *In re Google v. Gmail Litigation*. [82]

Here, Judge Koh reiterated her reasoning from *In re Google v. Gmail Litigation*, [83] with the addition of addressing Judge Grewal's opinion in *In re Google v. Privacy Litigation*.[84] In comparing the differing interpretations of the exception, Judge Koh concluded that the narrow interpretation drastically had more support. [85] Unlike the narrow interpretation, a broad interpretation of the exception is not supported by the text's plain meaning as such an interpretation would allow "any electronic service provider like Google to unilaterally adopt any revenue-generating business practice, deem it 'routine,' and exempt itself from the Wiretap Act." [86] This would in turn allow for ECSPs to "self-define" the scope of the exception under the Wiretap Act, running afoul of the plain meaning of the text narrowly exempting interceptions. [87]

Furthermore, the case law used to support Judge Grewal's contention of a broad interpretation more accurately stands for the narrow interpretation. [88] Judge Grewal cited *Kirch v. Embarg Management Co.* [89] and *Hall v. EarthLink Network Inc.* [90] in support of a broad interpreta-

---

79. *In re Google, Inc. Privacy Policy Litig.,* 2013 U.S. Dist. LEXIS 171124, at *1.

80. *Id*.

81. *Matera*, 2016 U.S. Dist. LEXIS 107918, at *44.

82. *Id*. at *27.

83. *See id.* at *21-42. Judge Koh's reasoning outlined the plain meaning of the statute, along with caselaw and legislative history in support of a narrow interpretation of the "ordinary course of business" exception.

84. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *1.

85. *Matera,* 2016 U.S. Dist. LEXIS 107918, at *25-27.

86. *Id*. at *26.

87. Judge Koh cited to *Campbell v. Facebook Inc.*, F.Supp. 3d 836, 844 (N.D. Ca. 2014) for support of the interpretation that Congress did not intend to allow the sort of latitude proposed by the broad interpretation of the "ordinary course of business" exception. *Matera*, 2016 U.S. Dist. LEXIS 107918, at *26.

88. *Id*. at *27-33.

89. "*In Kirch v. Embarq Management Co.,* the Tenth Circuit held that the defendant was protected by the exception when it conducted a test using third-party advertising technology and its customers' communications, because the defendant had 'no more of its users' electronic communications than it had in the ordinary course of its business as an ISP.'" *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *35 (quoting *Kirch v. Embarg Management Co.*, 702 F.3d 1245 (10th Cir. 2012).

90. The Second Circuit held in *Hall v. EarthLink Network Inc.*, 396 F.3d 500 (2d Cir. 2005) that while "[n]othing in processing a closed account's emails facilitates was

tion, where the "ordinary course of business" was not limited to actions necessary for an ESP's services. However, Judge Koh found these cases to stand for the opposite reason.[91] Judge Koh explains that *Kirch* stands for interceptions that are incidental to the interceptor's service as within the "ordinary course of business" exception. [92] Similarly, *Hall* found interceptions exempted if they were incidental to providing the email service at issue as well. [93] With both cases allowing the interception to pass under the exception only if they were "incidental" to providing a service, both more accurately represent the narrow interpretation of the exception, where "not everything that a company may want to do falls within the 'ordinary course of business' exception." [94]

Accordingly, the court found that Plaintiffs reasonably alleged the absence of a nexus between the interception and Google's ability to provide Gmail targeted advertising, and that the interception neither enabled nor assisted the email services, nor was an incidental effect of those services. [95] Instead, the legitimate purpose for the interception was to provide targeted advertising, and the court was not persuaded by the necessity of such advertising for revenue in order to provide Gmail free of charge; especially when it was evidenced that Google was able to provide this service to a portion of users without intercepting emails for the purpose of advertising. [96]

From the opinions of Judge Koh and Judge Grewal, it is apparent that the issue is one of interpretation. [97] Whether the "ordinary course of business" exception is applicable to ECSPs begins with a determination of applying the narrow or broad interpretation, as demonstrated by the above referenced cases. [98] However, companies and consumers of Silicon Valley, and beyond, need a clear standard by which to evaluate their respective claims prior to adjudication—which current precedent

---

necessary to the provision of ECS, suggesting that the processing was performed for other business reasons…such processing was not an 'interception.'" *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, *34-35.

91. *Matera,* 2016 U.S. Dist. LEXIS 107918, at *33.

92. *Id*.

93. *Id*. at *31-32.

94. *Id*. at *35.

95. *Id*. at *43-44.

96. *Id*.

97. In order to determine whether to grant or deny defendant's, Google's, Motion to Dismiss in each case, the court first had to determine if Plaintiffs' had a claim under the Wiretap Act by interpreting whether the "ordinary course of business" exception broadly or narrowly.

98. In each of the above referenced cases, interpretation of the "ordinary course of business" exception was determined after a Motion to Dismiss was filed by defendant, Google. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *1; *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *1; *Matera*, 2016 U.S. Dist. LEXIS 107918, at *1.

has failed to do.

B. GOOGLE'S ORDINARY COURSE OF BUSINESS ACROSS THE COUNTRY

Neither Judge Koh nor Judge Grewal were the first to delve into Google's automatic scanning practices, as the same issues discussed above were brought before the Eastern District of Texas two years prior to being consolidated with *In re Google v. Gmail Litigation*. [99] [100] Just as in *Gmail Litig.*[101], *Privacy Litigation* [102], and *Matera* [103], Plaintiffs in the Eastern District of Texas brought suit against Google for the automatic scanning of emails and using gathered PII for targeted advertising. [104]

In *Dunbar v. Google Inc.*, Google asserted that its advertising practice was "a necessary and fundamental aspect of Google's aim to better serve its Gmail customers, and such ads permit Google to provide its services free of charge to more than 100 million users." [105] Furthermore, Google argued that its device for scanning emails satisfied the requirements of the "ordinary course of business" exception. [106] Plaintiffs, on the other hand, argued that the device utilized by Google for intercepting emails was not necessary for providing email communication services. [107] Similar to the plaintiffs' argument in *In re Google Inc. Gmail Litig.*, [108] Plaintiffs referred to scans for spam, viruses, and spellcheck as related to the transmission of emails; whereas Google's collection of information for advertising was not. [109] Therefore, according to Plaintiffs, Google's device could only fall under the exemption if it was used for the transmission of emails, and that alone, as that would qualify as an ordinary course of business. [110]

---

99. Two years prior to *In re Google Inc. Gmail Litig.*, Google was brought in May of 2011 before the Eastern District of Texas. *Dunbar v. Google, Inc.* (*Gmail Interception*), No. 5:10-CV-194-DF, 2011 U.S. Dis. LEXIS 157932, at *1 (E.D. Tex. May 23, 2011).

100. Google first moved to consolidate six pending actions in the Northern District of California. *In re Google Inc. Gmail Litig.*, 936 F. Supp. 2d 1381, 1381-82 (J.P.M.L. 2013).

101. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *1.

102. *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *1.

103. *Matera,* 2016 U.S. Dist. LEXIS 107918, at *1.

104. Plaintiffs brought suit on behalf of a putative class. *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at *3-6.

105. *Id.* at *3. *See also* Batiste-Boykin, *supra* note 47 at 33 (Google has maintained this argument throughout its entire litigation regarding its practice with targeted advertising).

106. As an ECSP, Google contended that it used "(1) 'any telephone or telegraph instrument, equipment or facility, or any component thereof,' (2) 'in the ordinary course of its business.'" *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at *5 (quoting 18 U.S.C.A. § 2510 (5)(a)).

107. *Id.* at *4.

108. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784 at *41.

109. *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at *4.

110. *Id.*

This case was first brought before Judge Folsom [111] on two motions to dismiss by Google, and thus because he determined that Plaintiffs raised factual issues, he denied the motions. [112] Judge Folsom found issues of fact regarding whether Google used content from Gmail users' emails for purposes other than targeted advertising through Google's device utilized in the ordinary course of business, as well as how necessary the practice of targeted advertising was to Google's operation.[113]

It was not until *Dunbar v. Google Inc.* was transferred to the Northern District of California [114] that the "ordinary course of business" exception would be evaluated as part of *In re Google Inc. Gmail Litig.* [115] As referenced to previously, six cases were consolidated into *In re Google Inc. Gmail Litig.* [116] In addition to the ones in the Northern District of California and the Eastern District of Texas, cases were also filed against Google regarding its targeted advertising and scanning practices in the Southern District of Illinois, [117] the District of Maryland, [118] and the Eastern District of Pennsylvania. [119]

C. APPLICATION OF INTERPRETATIONS VIA GOOGLE'S AUTOMATIC SCANNING

In *Dunbar*, the court analyzed Google's action of using automated systems to intercept e-mails from Gmail accounts to collect information for targeted advertising and user profiles.[120] Beyond e-mail, Google also collects information through other services it offers users, such as

111. District court judge David Folsom wrote the opinion of this case. *Id*. at *1.

112. Google filed a Motion to Dismiss Plaintiffs' Class Action Complaint and a Motion to Dismiss Plaintiffs' First Amended Class Action Complaint. *Id*. at *12.

113. *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at *10-12.

114. In July of 2012, the case was transferred from the Eastern District of Texas to the Northern District of California. *Dunbar v. Google, Inc.,* No. 12-CV-03305-LHK, 2012 U.S. Dist. LEXIS 102313 (N.D. Ca. July 23, 2012).

115. Google moved to consolidate six pending actions from five different districts. *In re Google Inc. Gmail Litig*., 936 F. Supp. 2d 1381 (J.P.M.L. 2013).

116. *In re Google Inc. Gmail Litig*., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 138910, at *5 (N.D. Ca. Sept. 25, 2013).

117. In the Southern District of Illinois, suit was brought on behalf of a minor against Google alleging that the ECSP, inter alia, intercepted and scanned incoming and outgoing emails for the purpose of targeted advertising. Melissa Maalouf, *Lawsuit Against Google for Scanning Minors' Email Without Consent*, ZG ZWILLGEN BLOG (Nov. 16, 2012), http://blog.zwillgen.com/2012/11/16/lawsuit-against-google-for-scanning-minors-emails-without-consent/.

118. *Knowles v. Google, Inc. Filing 1*, JUSTIA DOCKETS & FILINGS, https://docs.justia.com/cases/federal/districtcourts/maryland/mddce/1:2012cv02022/203600/1 (last accessed: Jan. 20, 2017),.

119. *Brinkman v. Google, Inc. Filing 1*, JUSTIA DOCKETS & FILINGS, https://docs.justia.com/cases/federal/districtcourts/california/candce/5:2013cv01607/265083/1 (last accessed Jan. 20, 2017).

120. *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at *9.

Google Maps, Google Accounts, and YouTube. [121] Under Google's privacy policy, Google may combine information collected from any Google service for such purposes as targeted advertising. [122] Therefore, while a user accessing his or her Gmail account may expect one level of privacy and another while he or she is watching her favorite music video on YouTube, Google is collecting information to be used in a different context outside of that service. Considering this, when Google collects information from any of these various avenues for the purposes of targeted advertising, is it within the "ordinary course of business" of that service?

Judge Koh's narrow interpretation of the exception, such as that in *Gmail Litig.* [123], would suggest that the collection of information is an "interception," as defined in the Wiretap Act, and outside the ordinary course of business. [124] In reaching this conclusion, Judge Koh would apply the exception only when an ECSP's interception either (1) facilitated in the transmission of the communication, or (2) was necessary and incidental to the communication.[125] Therefore, according to Judge Koh's analysis, if the alleged interception of emails was not in furtherance of the communication or necessary and/or incidental to the communication, it would fall outside of the exception. [126] Similarly, if information was collected by a user of YouTube and it was not used to either provide the video or collection was not necessary or incidental to searching for the video, it would likely be found as an interception outside of the exception. [127]

Applying the same scenario to Judge Grewal's broad interpretation of the exception, Google would likely qualify under the exception and an interception would not be found. As discussed earlier in *Privacy Policy Litig.*, Judge Grewal broadly interpreted the term "business," and in doing so, would find that business includes advertising in the ordinary course of providing Google's services. [128] Judge Grewal's inclusion of

---

121. "Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google." *Google Privacy & Terms, supra* note 14.

122. *Id*.

123. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *1.

124. 18 USCS § 2510(4) (1986).

125. Batiste-Boykin, *supra* note 47 at 33.

126. *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at *30.

127. Batiste-Boykin, *supra* note 47 at 33.

128. Judge Grewal found legislative intent in choosing the term "business" to cover "customary and routine practices," including those outside of electronic communication

targeted advertising as "business" allows for Google to continue to provide its services for free to the public due to revenue brought in from the advertising. [129]

Additionally, using Judge Koh's criteria, targeted advertising may be found necessary and incidental to the operation or transmission of another service provided. [130] For example, an interception collecting information from a user of Gmail may be necessary and incidental to the operation of YouTube. These arguments, however, fail in application.

Google's business conducted outside of a specific service accessed by a user cannot fit within the "ordinary course" of all services performed by Google. For example, services provided for Gmail cannot be within the "ordinary course of business" for those provided for Google Maps. [131] If this was the case, the purpose behind the Wiretap Act and its exceptions would collapse, allowing for less privacy protection.[132] If any business conducted by an ECSP was found to be part of the course of business, the Wiretap Act would not have any application to those companies and ECSPs could accumulate an unrestricted amount of PII. [133] Even if the interpretation was not stretched to the extent of any business, but only to those "necessary," "incidental," or "facilitating" a service, targeted advertising is not essential such that Google could not operate without it.[134] Its justification for targeted advertising is to provide its services for free to the public,[135] not to merely provide services in general. It was not Congress' intention when enacting the Wiretap Act to provide ECSPs with unlimited latitude to engage in any interception beneficial to its own business models.[136] Targeted advertising

---

services alone. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, *33-34 (N.D. Ca. December 3, 2013).

129. Batiste-Boykin, *supra* note 47 at 33.

130. *Id*.

131. For example, when using Gmail, users can compose electronic messages to send to recipients with text, attachments, images, etc. *What can you do with Gmail?*,G SUITE LEARNING CENTER, https://support.google.com/maps/answer/144349?hl=en (last accessed March 10, 2018). In contrast, to use Google Maps, a user inputs information regarding an address or place and search for directions, information regarding businesses, and travel times. *Google Maps Help*, GOOGLE, https://support.google.com/maps/answer/144349?hl=en (last accessed March 10, 2018).

132. 18 U.S.C. § 2510-22 (1986).

133. *Id*.

134. *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at *3. *See also* Batiste-Boykin, *supra* note 47 at 33.

135. Batiste-Boykin, *supra* note 47 at 33.

136. "[T]he statutory scheme suggests that Congress did not intend to allow electronic communication service providers unlimited leeway to engage in any interception that would benefit their business models." *In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *36.

serves to benefit Google, and Google only. [137] As such, the intent of Congress supports the narrow interpretation of the exception, and the application of the Wiretap Act to the expanding services provided by ECSPs.

D. THE VIEW FROM ANOTHER BENCH

Before there was targeted advertising, a prominent area of coverage for the "ordinary course of business" exception was recorded telephone conversations.[138] In *Arias v. Mutual Cent. Alarm Serv.*, Plaintiffs brought suit against their former employer, Mutual Central Alarm Service, Inc., ("Mutual") for allegedly intercepting their private telephone conversations through a machine furnished by the employer. [139] The Second Circuit interpreted the "ordinary course of business" exception to include the employer's recording of conversations as doing so was substantiated by legitimate business reasons and part of standard practice within the central alarm station industry.[140]

Mutual Central Alarm Service, Inc. installed a Dictaphone [141] machine and connected it to its telephone system where it recorded all incoming and outgoing telephone calls for periods of 24 hours over 30 numbered tapes. [142] While working as employees of Mutual Central Alarm Service, Inc., Plaintiffs alleged that their private telephone conversations were intercepted by their employer and brought suit under the Wiretap Act. [143]

After hearing Plaintiffs' claim, the Southern District of New York determined that the defendant's interception of telephone conversations

---

137. Chad Brooks, *Invasion of Privacy: What Consumers Think of Personalized Online Ads*, BUSINESS NEWS DAILY (May 23, 2017 8:43 AM), https://www.businessnewsdaily.com/4632-online-shoppers-personal-ads.html.

138. *Electronic Communications Privacy Act Primer*, CENTER FOR DEMOCRACY & TECHNOLOGY (May 13, 2015) https://cdt.org/insight/electronic-communications-privacy-act-primer/.

139. *Arias v. Mut. Cent. Alarm Serv.*, 202 F.3d 553, 554, 557 (2d Cir. 2000).

140. "Legitimate business reasons support the continual recording of all incoming and outgoing telephone calls at Mutual. Central station alarm companies [because they] are the repositories of extremely sensitive security information, including information that could facilitate access to their customers' premises." *Id*. at 559.

141. The Dictaphone is a brand name for a dictating machine. *Dictaphone*, dictionary.com, http://www.dictionary.com/browse/dictaphone. A dictating machine was used to record speech for transcription. *Dictating machine,* MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/dictating+machine.

142. *Arias*, 202 F.3d at 554-555.

143. Plaintiffs brought suit under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act. Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), 18 U.S.C. § 2510-22, *available at* https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284 (last accessed on January 20, 2017); *Arias*, 202 F.3d at 555-56.

fell within the ordinary course of business. [144] Plaintiffs then appealed to the Second Circuit contesting that Mutual Central Service, Inc.'s "blanket recording of all incoming and outgoing telephone calls from Mutual's offices [was] not in the ordinary course of business." [145] The court disagreed and affirmed the district court's decision. [146]

In coming to this decision, the Second Circuit found that because companies, like Mutual Central Alarm Services, Inc., house sensitive security information necessary to access their customers' properties, and are the middle point of contact between customers and emergency personnel,

> "'[c]omplete records of calls…are important tools for their operators to ensure that their personnel are not divulging sensitive customer information, that events are reported quickly to emergency services…that customer claims regarding events are verifiable,' and that the police and other authorities may rely on these records in conducting any investigations." [147]

Additionally, it was noted that recording was the standard practice of the central station alarm industry, and in some cases, required. [148] Therefore, Mutual Central Alarm Service Inc.'s practice of recording telephone conversations over 24 hour periods was held to be part of its ordinary course of business, exempting the company from any violation under the Wiretap Act.[149]

Although not explicitly discussed, the Second Circuit's interpretation and application of the "ordinary course of business" exception resembles the narrow interpretation. Unlike *In re Google, Inc. Privacy Litig.*, the Second Circuit did not consider the recorded telephone conversations as part of the ordinary course of business because the calls were part of Mutual Central Alarm Services, Inc.'s customary or routine practice (as with the broad interpretation).[150] Rather, the calls were integral to its security service. [151] Google argued for an exception under the Wiretap Act for its practice of scanning emails to generate targeted advertisements because it allowed for the Gmail service to continue to be offered free of charge.[152] However, unlike Mutual Central Alarm Service, Inc.'s practice, Google's scanning for targeted advertising was not

144. *Arias v. Mut. Cent. Alarm Serv.,* 182 F.R.D. 407, 417 (S.D.N.Y. 1998).
145. *Arias*, 202 F.3d at 554.
146. *Id*.
147. *Id*. at 559.
148. *Id*.
149. In affirming the District Court's holding regarding the "ordinary course of business" exception, the Second Circuit found the grant of summary judgment to Defendant to be proper. *Id*.
150. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *33.
151. *Arias*, 202 F.3d at 559.
152. Batiste-Boykin, *supra* note 47 at 33.

essential to providing the transmission of emails.

The Second Circuit aligned more with Judge Koh of the Northern District California's reasoning, as in *Gmail Litig.*, [153] where both deemed an ordinary course of business as serving a legitimate purpose enabling or assisting the service of the communication provider. [154] Though there is a minimum of 13 years between this case and those involving Google, [155] the interpretation and reasoning is sound. [156] From court to court, bench to bench, the "ordinary course of business" exception is not a catch all provision allowing for a communication provider to qualify any business as such; rather, it is primarily interpreted as a narrow exception and should continue to be interpreted as such. [157]

E. THE WIRETAP ACT NEEDS A REBOOT

Alongside the issue of interpretation is the concern that these privacy cases are brought under the Wiretap Act. For the last 30 years, [158] the Wiretap Act has been on "sleep mode," while the field it regulates is megabytes [159] ahead with the advancement of technology. [160] For example, what started as a search engine—later registered as Google.com—in 1996, [161] has expanded to include products for business, media, geography, home and office, and social platforms just two decades later. [162]

---

153. *Matera*, 2016 U.S. Dist. LEXIS 107918, at *43-44.

154. *Arias*, 202 F.3d at 559.

155. Those cases include the following: *Gmail Interception*, 2011 U.S. Dis. LEXIS 157932, at * 1. *In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *1. *In re Google, Inc. Privacy Policy Litig.,* 2013 U.S. Dist. LEXIS 171124, at *1, and *Matera*, 2016 U.S. Dist. LEXIS 107918, at *1.

156. Two out of three cases in the Northern District of California interpreting the "ordinary course of business" exception have interpreted it narrowly. *See In re Google Inc. Gmail Litig*., No., 2013 U.S. Dist. LEXIS 172784, *1, and *Matera*, 2016 U.S. Dist. LEXIS 107918, at *1.

157. Of the cases cited throughout this comment, there has only been one that has interpreted the "ordinary course of business" exception broadly, allowing for customary and routine business operations of an ECSP to qualify as well for exemption under the Wiretap Act. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *33 (N.D. Ca. December 3, 2013).

158. It has been thirty years since the Wiretap Act was amended by the Electronic Communications Privacy Act in 1986. 18 U.S.C. § 2510-22 (1986).

159. To illustrate, approximately 600 megabytes of data would fit on a CD-ROM disk. *WHAT'S A BYTE? MEGABYTES, GIGABYTES, TERABYTES…WHAT ARE THEY?*, http://www.whatsabyte.com (last accessed Oct. 16, 2016).

160. Pippin, *supra* note 27 at 126.

161. *About Google*, GOOGLE, https://www.google.com/about/company/history/ (last accessed Oct. 13, 2016).

162. A list of Google's services includes (by category):
Web: Web Search, Google Chrome, Toolbar, and Bookmarks.
Mobile: Mobile, Maps for Mobile, and Search for Mobile.

In comparison, the Federal Wiretap Act of 1968 was only amended once in 1986 by the Electronic Communications Privacy Act. [163] During that time between 1968 and 1986, personal computers, digital music, cellphones, and global positioning systems were introduced.[164] Fast forward 18 more years, the World Wide Web, electronic mail, Wi-Fi, and software development kits [165] advanced technology further than previously anticipated by the Wiretap Act. [166]

This rapid evolution of technology has lessened the impact of the Wiretap Act's command—specifically, automated [167] technology. [168] The statute encompasses human interceptions, as suggested by legislative history and the plain language of the Wiretap Act; therefore, automated interceptions of e-mail, for example, make the statute challenging in its application to new technological advances. [169] Since the turn of the 21st century, ECSPs have challenged the statute's application due to innovative technology, with little progress done in the way of establishing an

---

Business: AdWords, G Suite, Google Cloud Platform, Google My Business, AdSense, AdMob, Analystics, and Google Domains.
Media: YouTube, Google Play, Books, Image Search, News, Video Search, Google Photos, Google Cardboard.
Geo: Maps, Earth, and Parnoramio.
Specialized Search: Custom Search, Google Shopping, Finance, Scholar, and Trends.
Home & Office: Gmail, Drive, Docs, Sheets, Slides, Forms, Drawings, Sites, Calendar, Translate, Voice, Google Wallet, Google Cloud Print, Google Keep, Google Store, and Hangouts.
Social: Google+, Blogger, Groups, and Spaces.
Id.

163. 18 U.S.C. § 2510-22 (1986).

164. The year 1970 introduced digital music, followed by cellphones in 1973. Shortly thereafter, personal computers came in 1977 and global positioning systems first appeared in 1978. POPULAR MECHANICS, *The Top 50 Inventions of the Past 50 Years,* http://www.popularmechanics.com/technology/gadgets/a341/2078467/ (Dec. 30, 2005).

165. The World Wide Web was introduced in 1989, electronic mail in 1993, Wi-Fi in 1999, and software development kits came in 2004. Government Computer News (GCN), 25 years: A technology timeline, https://gcn.com/Articles/2007/12/06/25-years--A-technology-timeline.aspx?Page=4 (Dec. 6, 2007).

166. In an effort to dismiss the plaintiffs' complaint, "Google indicated '[t]he processes related to Google's automated scanning are completely automated and involve no human review.'" Because the Wiretap Act, as amended by the Electronic Communications Privacy Act, only addresses human interceptions, Google contended that the automated scanning felt outside of the bounds of the statute. Batiste-Boykin, *supra* note 47 at 33.

167. The verb "automate" is defined as "to run or operate (something, such as a factory or system) by using machines, computers, etc. instead of people to do the work." *Automate*, MERIAM-WEBSTER, http://www.merriam-webster.com/dictionary/automate.

168. Batiste-Boykin, *supra* note 47 at 33.

169. In adopting the ECPA, Congress differentiated between electronic communications and voice telephone services by stating that electronic communications "do not involve humans listening in on voice conversations." Bruce E. Boyden, *CAN A COMPUTER INTERCEPT YOUR EMAIL?*, 34 CARDOZO L. REV. 669, 680 (2012).

effective framework. [170] The ECPA has been amended since 1968, [171] although the effects of the amendment have only been felt by law enforcement [172] and foreign intelligence. [173] While these amendments are noteworthy, they are not sufficient. The Wiretap Act must continually adapt with the field it regulates; thus, the statute must incorporate automated technology to meet the current standard.

F. THE NEXT NECESSARY UPDATE

In re Google v. Privacy Litigation has not been overruled, and therefore, even though *Matera v. Google, Inc.* addresses Judge Grewal's interpretation of the "ordinary course of business" exception, it did not concretely declare the narrow interpretation as the standard to abide by.[174] Furthermore, the Ninth Circuit has yet to rule on the interpretation of the "ordinary course of business" exception, leaving the district courts without clear, binding authority. [175] Thus, while there is guidance on this issue, a user or company may be hesitant as to whether to bring or defend a claim under the Wiretap Act based on the uncertainty of what interpretation will be applied to the potential case. [176] This concern is even more evident when reminded that the above-mentioned cases all revolved around Google's privacy policy and different outcomes resulted. [177]

---

170. "[L]awmakers and industry groups alike have made policy recommendations and proposed new legislation to update the substantive provisions of the ECPA…and establish a more effective framework for the application and enforcement of…[its] provisions, though none have yet been passed." Cohen & Gresser LLP, *Emerging Technologies Push the Boundaries of Privacy Law* (2014) http://www.jdsupra.com/legalnews/emerging-technologies-push-the-boundarie-05965/.

171. 18 U.S.C. § 2510-22 (1986).

172. FEDERAL COMMUNICATIONS COMMISSION, *Communications Assistance for Law Enforcement Act* (June 29, 2016), https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance; *The USA Patriot Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)*, DEPT. OF JUSTICE, https://www.justice.gov/archive/ll/highlights.htm (last accessed Oct. 13, 2016).

173. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436.

174. *Matera*, 2016 U.S. Dist. LEXIS 107918, at * 25-26.

175. *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 842 (N.D. Ca. 2014).

176. " The ECPA is broken. Irreparably. No one understands it, which leads to weird and unpredictable court rulings." Venkat Balasubramani, *Wiretap Claims Against Gmail Scanning Survive Motion to Dismiss—In re: Google Inc. Gmail Litigation,* TECHNOLOGY & MARKETING LAW BLOG (Sept. 30, 2013), http://blog.ericgoldman.org/archives/2013/09/wiretap_claims_1.htm.

177. Between the years 2013 and 2016, three suits have been brought against Google concerning its privacy policy and automated practices, and of those three, Google has received one ruling in its favor; whereas the plaintiffs of these suits have received two favorable decisions. *See In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, at

Thus far, the interpretation of the "ordinary course of business" exception has been prevalent in the Northern District of California, but how will the issue be presented in another district? Judges in courts across the country may be swayed by the interpretations of either Judge Koh or Judge Grewal, resulting in three potential harms. The first of these harms is the unclear precedent set by contrasting interpretations,[178] potentially discouraging consumers from bringing similar claims, while encouraging ECSPs to continue unlawful practices. Second, there is potential for venue shopping by plaintiffs. [179] If certain courts are interpreting the exception in a more favorable way than another court, the plaintiff may be more inclined to bring suit in the former over the latter.[180] And doing so would only extend the duration of the harms, furthering the cycle of uncertainty. Lastly, there is a potential for the misuse of judicial resources regarding the courts' time in trying the same issue, as the Northern District has done not once,[181] not twice,[182] but on three separate occasions.[183] While there is case law interpreting the "ordinary course of business" exception, there is not nearly enough to form a prevailing interpretation or set a standard on how to apply it.

Because of such potential harms, the need for a standardized interpretation, the narrow interpretation, set forth by Congress is that much stronger. If the narrow interpretation was the standard for the "ordinary course of business" exception, a clear precedent could be set, consumers could feel confident bringing their claims, venue shopping would

---

*45 (denying Google's motion to dismiss); *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *52 (granting Google's motion to dismiss); *Matera*, 2016 U.S. Dist. LEXIS 107918, at *44-45 (denying Google's motion to dismiss).

178. Specifically, these contrasting opinions are those from the Northern District of California, where precedent set by claims brought under the Section 2510 (5)(a)(i) of the Wiretap Act is unclear. *See In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *1 (holding that the narrow interpretation of the exception reflected the plain meaning, statutory interpretation, and legislative history of the Wiretap Act as amended by the ECPA); *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *1 (holding that the broad interpretation reflected Congress' deliberate decision in choosing the general term "business").

179. Ali Brieland, *Supreme Court limits 'venue shopping' for patent cases*, THE HILL (May 22, 2017 12:19 PM), http://thehill.com/regulation/court-battles/334548-supreme-court-limits-venue-shopping-for-patent-cases.

180. Such was the case with companies involved in patent suits, where venue was justified where the company conducted its business. Instead, the Supreme Court ruled that "[c]ompanies now will be required to bring lawsuits to where the targeted company is incorporated…The ruling will have broad implications for patent lawsuits, which are frequently moved to certain districts that have a track records of being favorable to patent infringement claims." *Id*.

181. *In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *1.

182. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *1.

183. *Matera*, 2016 U.S. Dist. LEXIS 107918, at *1.

be eliminated, and judicial resources could be used more efficiently. Furthermore, if there was a standardized interpretation, the scope of ECSPs legal interceptions could be lessened, preserving a level of privacy for consumers. With the broad interpretation of the "ordinary course of business" exception, an ECSP's "ordinary," "customary," or "routine" practices could fall under the umbrella of the exception. Without the narrow interpretation as the standard interpretation, ECSPs could in time argue that it has become "custom" or "routine" to intercept communications for targeted advertising purposes. This in turn could result in a larger collection of PII, leaving little privacy remaining with consumers.

Although it was enacted in 1968 [184], the Wiretap Act has the potential to affect consumers and businesses more now and in the future than ever before. The first step to ensuring its effectiveness is amending the Wiretap Act to include automated technology, so that practices, such as Google's scanning of user e-mails, can be challenged under the statute. Doing so would ensure that consumers with privacy concerns could bring claims challenging the current methods of today's ECSPs. Secondly, the narrow interpretation of the "ordinary course of business" exception must be the standard in evaluating an ECSP's practices. Setting such a standard would more closely align with the plain meaning and legislative history of the statute. This would also clear the docket from hearing this repetitive issue, ultimately conserving judicial resources. Lastly, the Wiretap Act must be continuously kept up to date with technology that is current. Doing so will benefit consumers, as well as ECSPs like Google because with these measures, consumers can be rest assured that their privacy concerns are recognized and protected. Additionally, if the Wiretap Act is continuously updated with the most recent technology, a technology gap, such as that between the enactment of the Wiretap Act and the introduction of the Internet, can be avoided.

IV. CONCLUSION

There were more than one billion search queries per day through Google in 2012. [185] That same year, Google had 153,441,000 visitors per month searching on its site. Using that same measurement, Yahoo! had 130,121,00 and YouTube had 106,692,000 visitors. [186] These millions of users have converted the Internet into a storage area from the collection

184. The Federal Wiretap Act was first enacted in 1968, and amended by the Electronic Communications Act in 1986.18 U.S.C. § 2510-22 (1986).

185. GO-GULF, *HOW PEOPLE SPEND THEIR TIME ONLINE,* BLOG (Feb. 2, 2012) http://www.go-gulf.com/blog/online-time/.

186. *Id*.

of data retrieved from these sites and others. [187] Facebook alone stored, accessed, and analyzed at least 30 petabytes [188] of data generated by users in 2013. [189] From the years 2008 through 2013, there was a 9-fold increase in digital information created and shared. [190]

This storage area has been created in part due to ECSPs taking advantage of the gaps and misinterpretations of the Wiretap Act. Due to the outdated nature of the statute and the conflicting interpretations by the court, ECSPs can engage in practices, namely targeted advertising, to their own benefit—losing sight of concern for user privacy.

The broad interpretation proposed by Judge Grewal in *Privacy Policy Litig*. prolongs a routine neglect of user privacy, finding ECSP's practices of collecting information for the purposes of targeted advertising as within the "ordinary course of business." [191] This interpretation swallows the Wiretap Act's exception in whole, allowing for an ECSP to justify any conduct as part of the ordinary course of business by claiming that it serves an end goal or purpose. [192] In contrast, a narrow interpretation of the exception, advocated by Judge Koh in *Gmail Litig.*, serves both sides of the browser—user and ECSP.[193] It does this by holding the ECSP to a narrow lane in which to operate by allowing interceptions only necessary for the facilitation of a service or for a purpose incidental to the operation of that service. [194] In doing so, the ECSPs still conduct their business in accordance with the limiting purpose of the statute, while also serving the privacy concerns of users by limiting information collection regarding their interaction with the

---

187. Pippin, *supra* note 27 at 126.

188. The size of one petabyte has the capacity to store 20 million 4-door filing cabinets or 500 billion pages of printed text. WHAT'S A BYTE?, *supra* note 159.

189. Vala Afshar, *50 Powerful Statistics About Tech Mega Trends Affecting Every Business* (Sept. 23, 2013) http://www.slideshare.net/ValaAfshar/6297-top50megatrends-v3/46-APPSIndustry_to_reach_tippingpoint_in.

190. *Id*.

191. According to Judge Grewal's broad interpretation of Section 2510 (5)(a)(i) of the Wiretap Act, exempted practices include services outside those necessary for providing electronic communications itself, such as targeted advertising. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *32-33.

192. A broad interpretation of Section 2510 (5)(a)(i) of the Wiretap Act "permits an electronic communication service provider like Google to unilaterally adopt any revenue-generating business practice, deem it 'routine,' and exempt itself from the Wiretap Act." *Matera*, 2016 U.S. Dist. LEXIS 107918, at *25-26.

193. The narrow interpretation of "the ordinary course of business' exception protects an electronic communication service provider's interception of email where there is 'some nexus between the need to engage in the alleged interception and the [provider's] ultimate business, that is, the ability to provide the underlying service or good.'" *Matera*, 2016 U.S. Dist. LEXIS 107918, at *27. By placing this limitation on interceptions, the user's privacy concerns are addressed and the ECSP can continue to operate and intercept information within reasonable bounds.

194. *In re Google Inc. Gmail Litig.,* 2013 U.S. Dist. LEXIS 172784, at *40-41.

ECSP.

Holding ECSPs to this narrow interpretation will place the most immediate effect on this field; however, it does not stop here. In order to fully oversee this field, further amendments to the Wiretap Act are necessary. For this statute to have an impact today, it must include automated technology since ECSPs like Google are moving to full automation. [195] This is evidenced by the fact that Google has been brought before the Northern District of California, not once, [196] not twice, [197] but three times [198] within the last three years. The debate over employment of automated technology could be cleared, or narrowed in scope, if the Wiretap Act specifically addressed the practices employed by ECSPs like Google.[199]

Targeted advertising finds us on the streets and in our homes. Advertising is displayed on billboards above us, and on subway cars below us. Advertisements zoom by us on a bus and wait for us on a park bench. The courts and Congress have interpreted the Wiretap Act so that targeted advertising can follow us through the depths of the Internet. Users choose which websites to visit, who to chat with, and what to do online. This decision-making power should remain with the users when it comes to what advertisements are preferred to be seen and where. The users bringing claims have expressed this privacy concern. [200] It is now time for ESCPs, the courts (specifically the Northern District of California), and Congress to listen, amend, and maintain the Wiretap Act.

---

195. Batiste-Boykin, *supra* note 47 at 33.

196. *In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784 (N.D. Ca. September 26, 2013).

197. *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *1.

198. *Matera*., 2016 U.S. Dist. LEXIS 107918, at *1.

199. Such practices that need to be addressed by the Wiretap Act include automated technology, which was the subject of the litigation concerning Google's practice of scanning emails. *See In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *55-56; *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *45-47.

200. These concerns have been focused around Google's practices of pulling personal identification information across all platforms, including YouTube, from users and using that information to provide targeted advertising. The discomfort with Google's practices is evidenced by the numerous lawsuits brought against the company, including those referred to here in this comment. *See In re Google Inc. Gmail Litig*., 2013 U.S. Dist. LEXIS 172784, at *6-9; *In re Google, Inc. Privacy Policy Litig*., 2013 U.S. Dist. LEXIS 171124, at *3-8; *Matera*, 2016 U.S. Dist. LEXIS 107918, at *4-5.