Case Western Reserve Law Review

Volume 70 | Issue 2 Article 13

2019

Bringing an End to the Wiretap Act as Data Privacy Legislation

Helen Jazzar

— Note —

BRINGING AN END TO THE WIRETAP ACT AS DATA PRIVACY LEGISLATION

CONTENTS

INTRODUCTION

The things that other people do not know about us are the things that make us human. Despite all of the benefits technology brings society, many digital users are left wondering how safe their personal information is when social media websites, search engines, Internet service providers, and other electronic communications service providers ("ECSPs") collect and sell their data for commercial gain.

With outdated legislation ill-suited to deal with modern technological advances, digital users have resorted to filing suit against ECSPs under a 1986 law, the Electronic Communications Privacy Act ("ECPA"), which forms Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act").[1] Digital users allege that ECSPs are guilty of wiretapping when ECSPs "intercept"[2] information

1. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012).

2. 18 U.S.C. § 2511(1)(a) (2012) (providing criminal and civil sanctions for "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire,

contained in electronic communications sent via ECSPs' platforms for the purpose of creating online-targeted advertisements.[3]

Courts should not interpret the Wiretap Act to include conduct it was never intended to encompass.[4] Leaving ECSPs amenable to suit under the Wiretap Act for conducting customary digital marketing practices stretches the text and purpose of the statute too far. Instead of applying the Wiretap Act to digital marketing practices, Congress should create a new federal data privacy law that governs the digital marketing industry as a whole.

This Note explains that ECSPs are not guilty of wiretapping when they use a digital user's information to create targeted advertisements because ECSPs are not "intercepting" an "electronic communication" under the Wiretap Act. This Note proposes that Congress adopt a new federal data privacy law that provides digital users the ability to retain control over how their personal information is shared.

Part I analyzes the legislative history of the Wiretap Act and relevant court decisions interpreting its language. Part II looks to the text and structure of the Wiretap Act, highlighting the statute's in–applicability to digital marketing practices. Lastly, by comparing the European Union General Data Protection Regulation[5] and the California Consumer Privacy Act of 2018,[6] Part III proposes attributes that new federal data privacy legislation should possess.

---

oral, or electronic communication"); *see also id.* §§ 2511(4)–(5) (describing civil and criminal liability for a violation of subsection (1)).

3. *See, e.g.*, *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5366963, at *7 (N.D. Cal. Sept. 26, 2013) ("Plaintiffs contend that Google violated the Wiretap Act in its 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 advertisements.").

4. Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 2, 5 (2018) ("Despite this admitted lack of transparency, the U.S. government does not adequately regulate service providers in any comprehensive way."); Crystal Schreiber, Note, *Google's Targeted Advertising: An Analysis of Privacy Protections in an Internet Age*, 24 TRANSNAT'L L. & CONTEMP. PROBS. 269, 286 (2014) ("The current U.S. federal laws provide too little protection for [I]nternet users. The pace at which technology and economic incentives have developed the marketplace has drastically exceeded the pace of protective legislation.").

5. Directive 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

6. California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2018) [hereinafter CCPA].

I. HISTORY OF THE WIRETAP ACT AND RELEVANT CASE LAW

The Wiretap Act was last amended at a time when the World Wide Web did not exist, let alone Google and Facebook.[7] Not only were these tech giants unknown, but Americans also had a completely different relationship with technology because they did not spend most of their time online.[8] As Americans changed the way they spent their time and money, businesses had to change the way they accommodated their clients. Accordingly, post cards were supplanted by emails and billboards were supplanted by online digital advertisements.[9]

In the modern era, ECSPs commonly track digital users' personal information.[10] Some ECSPs, such as Google, obtain personal information by scanning messages, while others, such as Embarq, obtain personal information by installing special technology on its servers that tracks a digital user's online behavior. After gathering personal information through unsettling digital marketing practices, ECSPs are in the driver's seat. Google, for example, engages in keyword bidding, a lucrative process that involves running an auction with third-party

7. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *see The Birth of the Web*, EUR. ORG. FOR NUCLEAR RESEARCH, https://home.cern/topics/birth-web [https://perma.cc/W8UB-WKLZ] (last visited Oct. 8, 2019).

8. In 1996, the small percentage of Americans with Internet access spent an average of only 3.5 hours per week online. WILLIAM J. GIBBS, CONTEMPORARY RESEARCH METHODS AND DATA ANALYTICS IN THE NEWS INDUSTRY 1 (2015). Fast-forward to 2018, and the average American spent about 23.6 hours per week online. Jamie Condliffe, *The Average American Spends 24 Hours a Week Online*, MIT TECH. REV. (Jan. 23, 2018), https://www.technologyreview.com/the-download/610045/the-average-american-spends-24-hours-a-week-online/ [https://perma.cc/MZ7G-PE68].

9. Forbes Communications Council, *Does Print Still Have a Place in the Future of Advertising? 10 Experts Weigh In*, FORBES (Mar. 2, 2018, 8:00 AM), https://www.forbes.com/sites/forbescommunicationscouncil/2018/03/02/does-print-still-have-a-place-in-the-future-of-advertising-10-experts-weigh-in/ [https://perma.cc/GG46-6ZCF] ("Since the dawn of the [I]nternet, people have heralded the death of print media. It's true that news has gone primarily online; most major media companies have made business model shifts in recent years to accommodate consumer preference for digital content.").

10. Laura Sydell, *Smart Cookies Put Targeted Online Ads on the Rise,* NPR (Oct. 5, 2010, 11:46 AM), http://www.npr.org/templates/story/story.php?storyId=130349989 [https://perma.cc/5953-LZWB].

companies for ad placement.[11] The highest bidding company has its advertisement appear on a digital user's webpage.[12]

To understand why the Wiretap Act does not apply to ECSPs' digital marketing practices, it is important to examine the statute's history and subsequent cases interpreting its language.

A. History

Although early American law proscribed eavesdropping,[13] the crime was seldom enforced until the creation of telephones and telegraphs.[14] Correspondingly, in 1918, Congress enacted the first federal wiretap statute as a temporary measure to prevent the disclosure of government secrets during World War I.[15] Shortly thereafter, Congress enacted the Radio Act of 1927, a law that effectively proscribed intercepting and divulging private radio messages.[16]

After *Olmstead v. United States*,[17] Congress passed the Communications Act of 1934,[18] expanding the Radio Act's interception proscription to include "radio" or "wire" communications. As the proscription broadened, states were left balancing their citizens' Fourth Amendment rights against the preservation of wiretapping as a law enforcement tool.[19] Consequently, some states established statutory systems authorizing law enforcement officials to wiretap or electronically eavesdrop on individuals, provided they first obtained a warrant or court order.[20]

Against this backdrop, Congress enacted the Wiretap Act in 1968,[21] establishing procedures for law enforcement authorities to follow when

11. *Id.*

12. *Id.*

13. GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., ORDER CODE 98-326, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 2 (2013).

14. *Id.*

15. Law of Oct. 29, 1918, ch. 197, 40 Stat. 1017 (1918).

16. Radio Act of 1927, ch. 169, 44 Stat. 1162 (1927).

17. 277 U.S. 438 (1928). There, the Court held that no Fourth Amendment violation occurred when the government introduced at trial evidence it obtained through wiretapping. *Id.* at 466.

18. Ch. 652, § 605, 48 Stat. 1064, 1103–04 (codified at 47 U.S.C. § 605 (2012)).

19. STEVENS & DOYLE, *supra* note 13, at 5.

20. *Id.*

21. Pub. L. No. 90-351, 82 Stat. 197 (June 11, 1968) (codified as amended at 18 U.S.C. §§ 2510–2520 (2012)).

conducting a wiretap. The Act was enacted "[t]o prevent crime and to insure the greater safety of the people."[22]

In 1986, Congress recast the Wiretap Act and granted law enforcement access to "electronic communications."[23] Congress's goal was not only to "strike a balance between the interests of privacy and law enforcement," but also to "avoid unnecessarily crippling infant industries in the fields of advanced communications technology."[24] Fittingly, Congress added a liability exemption for ECSPs:[25] the "ordinary course of business" exception exempts an ECSP from liability for interceptions that occur "in the ordinary course of its business."[26]

In creating the ordinary-course-of-business exception, Congress recognized that the "provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain."[27] The ordinary-course-of-business exception also represented Congress's goal of striking a balance between protecting individuals' privacy and "ensuring that the telecommunications industry was not hindered in the rapid development and deployment of the new services and technologies that continue to benefit and revolutionize society."[28]

The words "ordinary course of its business" were not defined in the ECPA. The judiciary has widely debated the definition and scope of the ordinary-course-of-business exception ever since.

B. Relevant Case Law

Following the enactment of the Wiretap Act, employees commonly sued employers for eavesdropping on their communications at work. Generally, employers would argue that the ordinary-course-of-business exception applied, thus exempting them from liability.[29] From these

22. *Id.*

23. STEVENS & DOYLE, *supra* note 13, at 6 (citing 18 U.S.C. §§ 2510–2521 (2012)).

24. *Id.* (citing H.R. REP. NO. 99-647, at 18–19 (1984); S. REP. NO. 99-541, at 5 (1986)).

25. 18 U.S.C. § 2510(5)(a)(i)–(ii) (2012).

26. Interceptions that are conducted in the ordinary course of an ECSP's business are excluded from the definition of "device." *See* 18 U.S.C. § 2510(5) (2012) (defining an "electronic, mechanical, or other device" as "any device . . . other than . . . 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").

27. S. REP. NO. 99-541, at 20 (1986).

28. H.R. REP. NO. 103-827, at 13 (1994).

29. *See* Adams v. City of Battle Creek, 250 F.3d 980, 983 (6th Cir. 2001); Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553, 558 (2d Cir. 2000);

cases, a general rule emerged: if "the exemption is claimed as a practice in the ordinary course of business, the interception must be for a legitimate business reason, it must be routinely conducted, and at least in some circuits employees must be notified at [sic] that their conversations are being monitored."[30]

As the Wiretap Act began to evolve into data privacy legislation, ECSPs, like employers accused of wiretapping, relied on the ordinary-course-of-business exception to protect themselves from liability. For example, in *Hall v. EarthLink Network Inc.*,[31] the United States Court of Appeals for the Second Circuit was faced with an Internet service provider sued under the Wiretap Act for continuing to receive messages sent to the plaintiff's email address after he terminated his email account.[32] The court found that the ordinary-course-of-business exception applied because it was Earthlink's "practice at the time to continue to receive and store emails on the server's mail file after any account was cancelled," and because Earthlink did not have "the ability to bounce e-mail[s] back to senders after the termination of an account."[33]

The Wiretap Act fully evolved into data privacy legislation, however, in *Kirch v. Embarq Management Co.*[34] There, the United States Court of Appeals for the Tenth Circuit wrestled with an unprecedented fact pattern involving a third-party company that used digital users' information to create online-targeted advertisements.

The defendant, Embarq Management Company, was an Internet service provider.[35] Embarq entered into an agreement with NebuAd, Inc., an online advertising company, "to conduct a technology test for directing online advertising to the users most likely to be interested in the ads."[36] The technology test involved NebuAd installing a system on Embarq's network so that traffic passing through that system would be sent to NebuAd's servers.[37] NebuAd then used the information to track what websites Embarq users visited. After acquiring the information,

---

Berry v. Funk, 146 F.3d 1003, 1008 (D.C. Cir. 1998); Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994); Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992).

30. STEVENS & DOYLE, *supra* note 13, at 10.

31. 396 F.3d 500 (2d Cir. 2005).

32. *Id.* at 502.

33. *Id.* at 505.

34. 702 F.3d 1245 (10th Cir. 2012).

35. *Id.* at 1245.

36. *Id.* at 1245–46.

37. *Id.* at 1247.

NebuAd delivered online advertisements that would likely interest users who visited those websites.[38]

Embarq users sued, alleging that during NebuAd's technology test, Embarq intercepted their communications and routed them to NebuAd.[39] The court held that Embarq was not liable "[b]ecause this access was only in the ordinary course of providing Internet services as an ISP."[40] Moreover, the court recognized that Embarq, an intermediary between Embarq's users and NebuAd, could not be liable under the Wiretap Act as an "aider and abettor."[41]

Relying on *Hall*, the court reasoned that just as Earthlink acquired Hall's emails in its ordinary course of business, Embarq's ordinary course of business as an Internet service provider necessitated that it have access to data transmitted over its Internet-providing equipment.[42]

The United States Court of Appeals for the Tenth Circuit never explicitly answered the question of whether NebuAd was liable under the Wiretap Act as a third-party advertising company for using the plaintiffs' data to create online-targeted advertisements.[43] This unanswered question would soon generate litigation in Silicon Valley.

In the United States District Court for the Northern District of California, unnerving digital marketing practices have caused digital users to sue ECSPs under the Wiretap Act.[44] Despite the clear factual differences between those cases and the appellate decisions in *Kirch* and *Hall*,[45] some Northern District of California courts have nevertheless

38. *Id.*

39. *Id.* at 1248 (quoting Kirch v. Embarq Mgmt., No. 10–2047–JAR, 2011 WL 3651359, at *6 (D. Kan. Aug. 19, 2011)).

40. *Id.* at 1246.

41. *Id.*

42. *Id.* at 1250–51.

43. *Id.* at 1249 ("Like the district court, we need not address whether NebuAd intercepted any of the Kirches' electronic communications."). Following the trial court's decision, the case between the Kirches and NebuAd was settled. *See* Valentine v. NebuAd, Inc., No. C 08-05113 TEH (LB), 2011 WL 13244509, at *1 (N.D. Cal. Nov. 21, 2011).

44. *E.g.*, *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013); *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013).

45. As one judge in the Northern District of California has observed:

> While *Hall* and *Kirch* present useful discussions of the "ordinary course of business" exceptions, the court ultimately finds that the factual differences preclude any meaningful application of those courts' reasoning to this case. In *Hall*, there was no "interception" analogous to the alleged interception in this case—instead, the complained-about conduct was nothing more than the receipt of emails itself, which would be "ordinary" even under the narrowest

relied on those decisions when deciding whether the ordinary-course-of-business exception applies to an ECSP's digital marketing practices.[46] The scope of the exception as applied to digital marketing practices has resulted in diverging views among various judges in the district.[47]

The following sections analyze both broad and narrow interpretations of the ordinary-course-of-business exception.[48] The last interpretation is one that this Note defines as a "functional interpretation." Lastly, this Note explains that these varying interpretations create more problems than they solve by creating conflicting standards for compliance. Digital users' privacy rights should not depend on which judge is assigned their case.

1. Judge Koh: Narrow

Under Judge Koh's interpretation of the ordinary-course-of-business exception, the exception applies only if an ECSP can prove that its digital marketing practice either facilitates, is incidental to, or is necessary to the transmission of the underlying communication.

To illustrate, in *In re Google Inc. Gmail Litigation*,[49] Judge Koh held that the ordinary-course-of-business exception did not apply to Google because Google's digital marketing practice of scanning emails to create targeted advertisements was not "instrumental," "incidental," or "necessary" to Google sending an email.[50]

> view of the word. And while *Kirch* involved analysis of users' web activity to aid in targeting advertising (similar to the allegations in the present case), the court's dismissal of the Wiretap Act claim was based primarily on the fact that any unlawful interception was performed by a third party, rather than by the defendant. Notably, the *Kirch* court did not explain whether its decision would have been the same if the defendant itself had analyzed the web traffic to deliver targeted advertising, and the court never expressly held that targeted-ad-analysis was within the ordinary course of Embarq's business as an [I]nternet service provider.

Campbell v. Facebook Inc., 77 F. Supp. 3d 836, 843 (N.D. Cal. 2014).

46. *See infra* Parts I.B.1–2.

47. *See Campbell*, 77 F. Supp. 3d at 843 (noting that "the *Google* court rejected a 'narrow read' of the exception that would be 'limited to only action taken to deliver the electronic communication;'" whereas "the *Gmail* court cautioned that an overly broad interpretation of the exception would read the word 'ordinary' out of the statute").

48. *See generally* Kayla McKinnon, Comment, *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, 189–99 (2018) (discussing how the ordinary-course-of-business exception has both a narrow and a broad interpretation).

49. No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013).

50. *Id.* at *9, *11.

The court held that *Kirch* cut in favor of a narrow reading of the ordinary-course-of-business exception, and that *Kirch* stood only for the limited proposition that "interceptions incidental to the provision of the alleged interceptor's [I]nternet service fall within the 'ordinary course of business' exception."[51] Relying on *Hall*, the court found that, unlike Earthlink—which presented testimony that it routinely continued to receive and store emails after an account was cancelled and that it did not have the ability to bounce-back emails to senders after an account was terminated—Google's alleged interceptions were not a necessary part of its ability to provide email services.[52]

In light of the statutory text's plain meaning, as well as the overall statutory scheme and its legislative history, the court held that the ordinary-course-of-business exception is "narrow and designed only to protect electronic communication service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to provision of the electronic communication service at issue."[53]

Moreover, the court found that for a practice to fall within the ordinary-course-of-business exception, the alleged interception must have "some nexus" to the ECSP's ultimate business; that is, its ability to provide the underlying service or good.[54] Narrowly interpreting the ordinary-course-of-business exception remains the majority approach within the Northern District of California.[55]

2. Judge Grewal: Broad

Three months following *In re Google Inc. Gmail Litigation*, Judge Grewal rejected Judge Koh's narrow interpretation of the ordinary-course-of-business exception. In *In re Google, Inc. Privacy Policy Litigation*,[56] Judge Grewal held that the exception applied if ECSPs can prove that their digital marketing practice is furthering a legitimate business purpose and is not limited to acts that are necessary to process

51. *Id.* at *8.

52. *Id.* at *9.

53. *Id.* at *11.

54. *Id.* at *11. Additionally, key to the court's finding was that Google violated its own internal policies. *Id.* at *11–12.

55. *See* Matera v. Google Inc., No. 15-CV-04062-LHK, 2016 WL 8200619, at *14 (N.D. Cal. Aug. 12, 2016) (finding that the alleged practice requires "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") (quoting *In re Google Inc. Gmail,* 2013 WL 5423918, at *11 (alteration in original)).

56. No. C-12-01382-PSG, 2013 WL 6248499, at *10–11 (N.D. Cal. Dec. 3, 2013).

the underlying communication.[57] Judge Grewal reasoned that because advertising is a legitimate business purpose, the ordinary-course-of-business exception applied, exempting Google from liability under the Wiretap Act.[58]

The plaintiffs in *In re Google, Inc. Privacy Policy Litigation* alleged that Google's practice of tracking a user's personal identification information constituted a wiretap.[59] The plaintiffs argued that the ordinary-course-of-business exception did not apply because it was not *necessary* for the delivery of Gmail that Google gather information about a person across all of Google's platforms to create personalized Google search results and advertisements.[60]

The court interpreted *Kirch* to apply the ordinary-course-of-business exception "where the provider is furthering its 'legitimate business purposes'—including advertising—and is not limited to only those acts that are technically necessary to processing email."[61] Judge Grewal further noted that other courts have "agreed that the 'ordinary course of business' exception is not limited to actions necessary to providing the electronic communication services" because "[n]othing in processing a closed account's emails facilitates [or] was necessary" to sending emails.[62]

Faced with the same text, history, and case law as Judge Koh, Judge Grewal stated that "[r]ather than narrowing the exemption to only the provision of electronic communications services itself, or some such narrower scope, Congress specifically chose the broader term 'business' that covers more farranging [sic] activity."[63] The court reasoned that pairing "business" with "ordinary course" "suggest[s] an interest in protecting a provider's customary and routine business practices."[64] Therefore, because targeted advertising was part of Google's customary and routine business practice, the ordinary-course-

57. *Id.* at *11.

58. *Id.*

59. *Id.* at *2–3.

60. *Id.* at *10–11.

61. *Id.* at *11.

62. *Id.*

63. *Id.* at *10.

64. *Id.*; *see also* Kirch v. Embarq Mgt., 10-2047-JAR, 2011 WL 3651359 at *9 n.42 (D. Kan. Aug. 19, 2011) ("The Court notes that [the ordinary-course-of-business] defense also appears to have merit, as plaintiffs have admitted that Embarq conducted the NebuAd test to further legitimate business purposes and that behavioral advertising is a widespread business and is commonplace on the Internet.").

of-business exception applied and the Wiretap Act claim against Google was dismissed.[65]

3. Chief Judge Hamilton: Functional

Chief Judge Hamilton adopted a functional approach in *Campbell v. Facebook Inc.*[66] In *Campbell*, the chief judge recognized that, while Judge Grewal's approach "emphasized the need to give meaning to the term 'business,' [Judge Koh's approach] cautioned that an overly broad interpretation of the exception would read the word 'ordinary' out of the statute."[67]

Chief Judge Hamilton held, as Judge Koh did, that there must be "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."[68] She also held, as Judge Grewal did, that the exception must cover more than "necessary" activities.[69] Chief Judge Hamilton also focused on the word "its" in the phrase "ordinary course of its business," determining that a court must consider the details of an ECSP's business "and must not rely on a generic, one-size-fits-all approach that would apply the exception uniformly across all electronic communication service providers."[70] Under this functional approach, the fact that ECSPs generate revenue from a digital marketing practice, without more, does not mean that such conduct falls within the ordinary course of that ECSP's business.[71]

The plaintiffs in *Campbell* alleged that Facebook violated the Wiretap Act by using "likes" to compile user profiles and then using those profiles to deliver targeted advertising to its users.[72] But because the court did not find "any facts alleged in the complaint or facts presented by Facebook that indicate a nexus between Facebook's alleged scanning of users' private messages for advertising purposes and

65. *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *11.

66. 77 F. Supp. 3d 836 (N.D. Cal. 2014).

67. *Id.* at 843.

68. *Id.* at 844 (quoting *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013)).

69. *Id.*

70. *Id.*

71. *Id.* ("An electronic communications service provider cannot simply adopt any revenue-generating practice and deem it 'ordinary' by its own subjective standard.").

72. *Id.* at 838–39.

its ability to provide its service,"[73] the ordinary-course-of-business exception did not apply, and Facebook's motion to dismiss was denied.[74]

Two years after *Campbell*, Google was sued again under the Wiretap Act, this time by digital users who did not use Google's services, but corresponded by email to individuals who did use Gmail services in *Matera v. Google Inc.*[75] The plaintiffs alleged that, "due to the ubiquity of Gmail, [they] ha[ve] sent emails to and received emails from Gmail users, which Google allegedly ha[d] intercepted, scanned, and analyzed."[76] Google responded by moving to certify the following question to the United States Court of Appeals for the Ninth Circuit: "Whether Google's automated scanning of emails in providing Google services falls within the 'ordinary course of its business' exception to the Wiretap Act."[77] Ultimately, the court refused to certify the question for interlocutory appeal.[78]

In *Matera*, Judge Koh relied on the narrow approach she used in *In re Google Inc. Gmail Litigation* to deny Google's motion to dismiss because Google's alleged interception of emails to provide targeted advertising, which in turn generated the revenue necessary for Google to provide Gmail, did not provide a "sufficient nexus" between the alleged interception and Gmail's service.[79]

The common issue with each approach to the ordinary-course-of-business exception is the lack of clarity each interpretation provides. First, Judge Koh does not explain what practices are instrumental to sending a message.[80] Also, it remains unclear what business practices provide a sufficient nexus between an ECSP's need to engage in the alleged interception and the ECSP's ability to provide its underlying service or good. Second, Judge Grewal does not explain how to decide whether a business practice is "legitimate." Judge Grewal also reads "ordinary" out of the statute.[81] Third, Chief Judge Hamilton leaves

73. *Id.* at 844.

74. *Id.* at 850.

75. No. 15-CV-04062-LHK, 2016 WL 8200619 (N.D. Cal. Aug. 12, 2016).

76. *Id.* at *2.

77. *Id.* at *15 (citation omitted).

78. *Id.* at *16.

79. *Matera*, 2016 WL 8200619, at *14.

80. *See In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *11 (N.D. Cal. Dec. 3, 2013) ("For example, in delivering Gmail is it really 'necessary' [to] do more than just the comply with email protocols such as POP, IMAP and MAPI? What about spam-filtering or indexing? None of these activities have anything specifically to do with transmitting email.").

81. *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013) ("The presence of the modifier 'ordinary'

courts with little to no guidance on how to decide whether a business practice is ordinary. For example, is a certain practice ordinary because ECSPs have been engaging in that practice for decades? Or, is a practice ordinary because an ECSP's *industry* has been engaging in that practice for decades?

As a result of the ambiguity surrounding the ordinary-course-of-business exception, ECSPs are unaware of the protocol they need to follow to ensure they comply with federal law. More importantly, digital users have no way of knowing what information ECSPs collect from them, to whom ECSPs are selling their information, or how to opt out of an ECSP's data collection—short of filing a federal lawsuit.[82]

Although Google and Facebook relied on the ordinary-course-of-business exception, the Wiretap Act's text suggests that the Act does not apply to digital marketing practices at all.

II. STATUTORY TEXT

The Wiretap Act provides for both civil and criminal penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[83] The Wiretap Act defines "intercept" as the "aural or other acquisition of the contents

must mean that not everything Google does in the course of its business would fall within the exception."); *see also* McKinnon, *supra* note 48, at 210 ("The broad interpretation proposed by Judge Grewal in *Privacy Policy Litig.* prolongs a routine neglect of user privacy . . . . 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.").

82. Even if digital users sue ECSPs under the Wiretap Act, there is a clear information asymmetry between digital users and ECSPs. Since ECSPs generally keep their digital marketing practices private, digital users may not meet pleading requirements under the Wiretap Act because they may not know the specific digital marketing practices ECSPs use. *See, e.g.*, Smith v. Google LLC, No. 18-CV-06459-SVK, 2019 WL 542110, at *3 (N.D. Cal. Jan. 18, 2019) (finding plaintiff's allegation insufficient to state a claim for relief under the Wiretap Act on the basis that "Google intercepted wire, oral, and electronic communications by invading the privacy of my phone calls, [I]nternet searches, and emails and are alleged to have redirected them unlawfully and/or improperly to unintended end users and/or endpoints." (quoting Second Amended Complaint at 2, *id.* (No. 5:18CV06459))).

83. 18 U.S.C. § 2511(1)(a) (2012). Additionally, the United States Court of Appeals for the Ninth Circuit has held that for there to be an interception in violation of the Wiretap Act, the communication must be acquired during transmission, not while the communication is in electronic storage. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2001).

of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[84]

By emphasizing important distinctions between an electronic communication and online behavior, and between device and software, this Note illustrates how the Wiretap Act's text is inapplicable to digital marketing practices entirely. Additionally, this Note argues that the penalties imposed under the Wiretap Act may lead ECSPs to charge subscription fees, may not adequately deter ECSPs from violating the Wiretap Act, and may actually encourage ECSPs to spread a digital user's information.

A. Electronic Communication

Under the Wiretap Act, "electronic communication" is defined as "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 that affects interstate or foreign commerce."[85] This definition is stretched too far when it includes a transfer that does not involve a human on the receiving end of the communication.

The notion that a human has to be on the receiving end of an electronic communication is strongly supported by the statutory scheme. It is significant that the Wiretap Act excludes from the definition of electronic communication any communication made through a "tone-only paging device" or from a "tracking device" because both a two-tone pager and a tracking device involve a "transfer" between two devices that does not involve a human on its receiving end.[86] Similarly, when a digital user's online behavior is tracked by an ECSP for digital marketing purposes, the digital user is transferring information to a computer, not a human.

The Wiretap Act generally "protects *the parties* to a communication against the unlawful interception, use, and disclosure of that communication by persons who are not parties to the communication."[87] The Wiretap Act also allows an "aggrieved person" to move to suppress the contents of an unlawfully intercepted communication.[88] An "aggrieved person" is any "person who *was a party* to any intercepted wire, oral, or electronic communication or a person against whom the

84. 18 U.S.C. § 2510(4) (2012).

85. *Id.* § 2510(12).

86. *Id.* § 2510(12)(B)–(C).

87. United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009) (citing 18 U.S.C. §§ 2511–2512 (2012)) (emphasis in original).

88. *Id.* (citing 18 U.S.C. § 2518(10)).

interception was directed."[89] The plain language of the Wiretap Act suggests that in order for there to be an "electronic communication," there must be at least two "parties," or individuals, involved.

Despite the statutory scheme and the text of the Wiretap Act, courts have interpreted "electronic communication" to include a data transfer between a human and a computer. For example, in *Kirch*, the plaintiffs alleged that their Internet service provider aided a third-party advertising company in intercepting "Internet traffic."[90] The third-party advertising company obtained three pieces of information from digital users: (1) the digital user's webpage address, (2) the last URL she visited before the request, and (3) an encrypted advertising-network cookie.[91]

Internet traffic is similar to the Call Data Content ("CDC") at issue in *United States v. Reed*.[92] In *Reed*, two men who were indicted for distributing and manufacturing Phencyclidine argued that the wiretap evidence that the government acquired in the course of its investigation should have been suppressed because the government failed to seal the CDC information during its wiretap.[93] The district court ruled that since CDC was not a communication under the Wiretap Act, the evidence acquired by the government would not be suppressed.[94] The United States Court of Appeals for the Ninth Circuit affirmed, holding that CDC was not an electronic communication because "it [wa]s not communicated to or from *the parties* to the telephone call."[95] Rather, the CDC amounted to data that were incidental to the use of a communication device, and, therefore, it contained "no 'content' or information that the parties intended to communicate."[96] The same goes for the "Internet traffic" obtained by the third-party advertising company in *Kirch* because the alleged communication was data incidental to the digital user's use of a computer and was not

89. *Id.* (citing 18 U.S.C § 2510(11)) (emphasis in original).

90. Kirch v. Embarq Mgmt., 702 F.3d 1245, 1247 (10th Cir. 2012).

91. *Id.* at 1247–48.

92. 575 F.3d 900 (9th Cir. 2009). CDC includes information regarding the origination, length, and time of a phone call. *See id.* at 914.

93. *Id.* at 905, 914. The Wiretap Act's sealing requirement states that "[t]he recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, . . . such recordings shall be made available to the judge issuing such order and sealed under his directions." *Id.* at 915 (quoting 18 U.S.C. § 2518(8) (2012)).

94. *Id.*

95. *Id.* at 916 (emphasis added).

96. *Id.*

information the digital user intended to communicate to another human.

At least one legal commentator has taken this argument a step further, suggesting that a human must be on the receiving end of an *interception* for that person to have a viable claim under the Wiretap Act.[97] Under this view, Google's email-scanning practices would not constitute an interception under the Wiretap Act because the practice is "completely automated and involve[s] no human review."[98]

In sum, the Wiretap Act should not apply unless at least two humans are involved in a communication, namely the person orchestrating the communication (the sender) and the person receiving the communication (the receiver).

B. Device

For an interception to occur under the Wiretap Act, the intercepted communication's contents must be acquired "through the use of any electronic, mechanical, or other device" that "can be used to intercept a wire, oral, or electronic communication."[99] Since software, as opposed to a device, captures or redirects the contents of a communication, ECSPs are technically not "intercepting" an electronic communication under the Act.

Instead of identifying the device that acquires the content of a communication,[100] courts have mistakenly analyzed the device that

97. Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 CARDOZO L. REV. 669, 717 (2012) ("The Act has always required at least the prospect of human review, and not only because it was initially drafted in 1968. Rather, it is because, as the drafters of the ECPA in 1986 understood, computer monitoring is qualitatively different from human monitoring. It is the threat of human use of personal information that reduces privacy, and not simply that one's information may be used in some way."); *see also* Christopher Batiste-Boykin, In re Google Inc.*: ECPA, Consent, and the Ordinary Course of Business in an Automated World*, 20 INTELL. PROP. L. BULL. 21, 36 (2015) ("The legislative history and the plain language of ECPA suggest that the statute prohibits only human interceptions of electronic communications.").

98. Memorandum in Support of Defendant's Motion to Dismiss Plaintiffs' Consolidated Individual & Class Action Complaint at 4, *In re* Google Inc. Gmail Litig., No. 5:13-MD-02430-LHK, 2013 WL 5366963 (N.D. Cal. June 13, 2013), ECF No. 44.

99. 18 U.S.C. § 2510(4)–(5) (2012).

100. Although the term "acquisition" is not defined in the statute, the Ninth Circuit has adopted its "ordinary meaning": "the act of acquiring, or coming into possession of." United States v. Smith, 155 F.3d 1051, 1055 n.7 (9th Cir. 1998). The Ninth Circuit has elsewhere held that acquisition occurs "when the contents of a wire communication are captured or redirected in any way." Noel v. Hall, 568 F.3d 743, 749 (9th Cir. 2009) (quoting United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992)).

stores the underlying communication. For example, in *Kirch*, the plaintiffs alleged that "the Internet traffic that passed through *the UTA* was sent to the NebuAd servers in its system."[101] The court's analysis in *Kirch* does not turn on whether a server is a "device" because the server did not acquire the plaintiffs' Internet communications; the Ultra-Transparent Technology ("UTA") is the device because it captured and redirected the communications to a third-party's server.[102]

Like NebuAd's use of the UTA system in *Kirch*, Google uses "various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs."[103] Google also conceded "that incoming and outgoing emails [were] analyzed by automated software"[104] before stopping that practice in 2017.[105]

To understand why deep-packet inspection technology, cookies, pixel tags, browser web storage or application data caches, databases, and server logs (all intangible items) are excluded from the Wiretap Act, it is important to identify what Congress understood "device" to mean at the time the ECPA was adopted in 1986.

The enactment of the Computer Fraud and Abuse Act of 1984[106] ("CFAA") supports the notion that Congress was aware of the distinction between "device" and "software," but intentionally chose to exclude software from the Wiretap Act. The CFAA was enacted primarily to address the growing problem of computer hacking.

101. Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1247 (10th Cir. 2012) (emphasis added).

102. An Ultra-Transparent Technology is a type of deep packet inspection technology. HANDBOOK ON ETHICS AND MARKETING 397 (Alexander Nill ed. 2015); *see also* Andrea N. Person, *Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May Be Limiting the Online Experience*, 62 FED. COMM. L.J. 435, 438 (2010) ("Deep Packet Inspection technology provides Internet service providers (ISPs) with the ability to collect all Internet communications made by a consumer. Depending on how the technology is deployed, it may 'monitor[], analyze[], and potentially manipulate[] Internet traffic.'" (alteration in original)).

103. *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=en#infocollect [https://perma.cc/M8GD-2AUJ] (last updated Jan. 22, 2019).

104. Samuel Gibbs, *Gmail Does Scan All Emails, New Terms Clarify*, THE GUARDIAN (Apr. 15, 2014, 8:24 AM), https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify [https://perma.cc/D3AL-MUXN].

105. Kaya Yurieff, *Google Still Lets Third-Party Apps Scan Your Gmail Data*, CNN (Sept. 20, 2018, 5:32 PM), https://money.cnn.com/2018/09/20/technology/google-gmail-scanning/index.html [https://perma.cc/N4ZU-3P2V].

106. 18 U.S.C. § 1030 (2012).

Congress recognized that by "intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system."[107]

The CFAA defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device . . . but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."[108] Further, the CFAA states that "[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, *computer software*, or firmware."[109] By distinguishing software and device in the CFAA in 1984, but excluding any mention of software in the ECPA in 1986, Congress understood device to exclude software.

Similarly, the California legislature distinguished "Unique Iden–tifier" from the definition of "device" in the California Consumer Privacy Act of 2018.[110] The California Consumer Privacy Act of 2018 defines "device" as "any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device."[111] "Unique identifier," however, is defined as "a persistent identifier that can be used to recognize a consumer . . . including, but not limited to . . . cookies, beacons, pixel tags, mobile ad identifiers, or similar technology."[112]

Because software is distinct from a device, ECSPs such as Facebook are not intentionally intercepting the contents of a communication when their automated software scans a digital user's message. Therefore, a mere allegation that an ECSP "uses a software application called a 'web crawler' to scan any URLs that are contained in messages and to send server requests to that web page"[113] does not prove that an interception occurred under the Wiretap Act because a tangible "device" is not acquiring the content of the electronic communication, software is.[114]

C. Penalties

Anyone who has been damaged by the interception or disclosure of their communications under the Wiretap Act is entitled to: "(1) any

107. United States v. Nosal, 676 F.3d 854, 858 (6th Cir. 2012) (alteration in original) (quoting S. REP. NO. 99–432, at 9 (1986)).

108. 18 U.S.C. § 1030(e)(1) (2012).

109. *Id.* § 1030(g) (emphasis added).

110. CCPA §§ 1798.100–.199 (2018).

111. CCPA § 1798.140(j).

112. *Id.* § 1798.140(x).

113. Campbell v. Facebook, Inc., 77 F. Supp. 3d 836, 840 (N.D. Cal. 2014).

114. *See id.*

preliminary, equitable, or declaratory relief that may be appropriate; (2) statutory and punitive damages; and (3) reasonable attorney's fees."

As this Note explains below, providing injunctive relief to digital users under the Wiretap Act may lead ECSPs to begin charging subscription fees for their services, may not adequately deter ECSPs from violating a digital user's privacy, and may incentivize ECSPs to spread a digital user's information to be exempt from liability under the Wiretap Act.

Providing injunctive relief to digital users under the Wiretap Act may result in ECSPs losing advertising revenue. To offset their losses, ECSPs may begin charging digital users a subscription fee to use their services.

ECSPs such as Google receive their primary source of revenue from digital advertisements.[115] Around eighty-six percent of Google's total revenue in the second quarter of 2018 was derived from advertising revenue.[116] Google generates its revenue and operates free-of-charge because it processes, collects, and sells its digital users' data. But if enough digital users are granted injunctions that enjoin ECSPs such as Google from obtaining personal information from its users, then ECSPs may need to find other ways to compensate for their loss of advertisement revenue.

One way Google could compensate for the loss of advertisement revenue is to begin charging all digital users an annual subscription fee to use its services.[117] According to nmpiHome, this annual subscription fee could be forty-five dollars or more.[118] The nmpiHome authors envision that the subscription would "include a full privacy agreement whereby no data about the user is collected. This could ease privacy concerns, but could also place consumers at a disadvantage as this data is currently used by Google to improve the user [experience]."[119]

For some users, the social-media experience is more valuable than protecting their personal information, suggesting that some digital users

115. For the second quarter ending on June 30, 2018, Google reported its advertisement revenue to be $28.087 billion, up 23.9% from $22.672 billion a year earlier. Zak Stambor, *Google's Ad Revenue Jumps 24% in Q2*, DIGITAL COM. 360 (July 23, 2018), https://www.digitalcommerce360.com/2018/07/23/googles-ad-revenue-jumps-24-in-q2/ [https://perma.cc/3VX9-GBBF].

116. *See Alphabet Announces Second Quarter 2018 Results*, GOOGLE (July 23, 2018), https://abc.xyz/investor/pdf/2018Q2_alphabet_earnings_release.pdf [https://perma.cc/TX7Z-BSV].

117. *What if You Had to Pay for Google?*, NMPI BLOG (June 13, 2017), https://nmpidigital.com/what-if-you-had-to-pay-for-google/?no_redirect [https://perma.cc/227J-7E2Q].

118. *Id.*

119. *Id.*

may not value their privacy enough to pay a subscription fee for online services. For example, "[d]espite the parade of negative publicity surrounding the Cambridge Analytica revelations in mid-March 2018, Facebook added 70 million users between the end of 2017 and March 31, 2018."[120] According to some economists, "[t]his implies the value users derive from the social network more than offsets the privacy concerns."[121] But without laws that expressly permit ECSPs to charge the digital users that seek injunctive relief or opt out of data collection a subscription fee, the other digital users who are unbothered by ECSPs collecting their personal information in exchange for free services may wind up paying for an ECSP's service if enough other digital users object to sharing their personal information.[122]

The Wiretap Act also requires subsequent offenders to be fined five hundred dollars.[123] In contrast, the European Union's General Data Protection Regulation imposes on data controllers fines of at least four percent of annual global turnover or €20,000,000.[124] Low fines, such as those provided in the Wiretap Act, may not encourage ECSPs to comply with federal law.

---

120. Jay R. Corrigan et al., *How Much is Social Media Worth? Estimating the Value of Facebook by Paying Users to Stop Using it,* PLOS ONE (Dec. 19, 2018), at 8, https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0207101&type=printable [https://perma.cc/8XQY-3WNA]. Cambridge Analytica allegedly secretly harvested more than 50 million Facebook users' personal information to build a system that could target US voters with personalized political advertisements based on their psychological profiles. Patrick Greenfield, *The Cambridge Analytica Files: The Story So Far*, THE GUARDIAN (Mar. 25, 2018, 7:53 PM), https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far [https://perma.cc/GK3W-9ZJ4].

121. Corrigan et al., *supra* note 120.

122. In a recent study, Pew Research analyzed Americans' opinions on privacy- and information-sharing by asking individuals how comfortable they would be with free access to a social media site that used their activity on that site to deliver targeted advertisements. LEE RAINIE & MAEVE DUGGAN, PEW RES. CTR., PRIVACY AND INFORMATION SHARING 2–3 (Jan. 14, 2016), http://www.pewresearch.org/wp-content/uploads/sites/9/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [https://perma.cc/MT7G-FNJ5]. Specifically, one of the focus group participants stated, "[t]o be honest, I don't really care. That is especially the case when I voluntarily use a service in return for giving up some information. For example, I use Gmail for free, but I know that Google will capture some information in return. I'm fine with that." *Id.* at 6; *see also* United States v. Jones, 565 U.S. 400, 427 (2012) (Sotomayor, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.").

123. 18 U.S.C. § 2511(5)(a)(ii)(B) (2012).

124. GDPR, *supra* note 5, at 83.

The logical outgrowth from ECSPs' potential liability for wiretapping has been for ECSPs to outsource digital marketing practices to third parties.[125] For instance, Google could avoid liability under the Wiretap Act as an "aider and abettor" if it acts like the defendant in *Kirch* and provides digital users' information to a third party.[126] But if protecting a digital user's personal information is the ultimate goal, it seems counterintuitive that distributing a digital user's personal information to more organizations exempts an ECSP from liability under the Wiretap Act.

III. PROPOSAL FOR FEDERAL LEGISLATION

Digital users are not without hope.[127] In 2016, the European Union enacted the General Data Protection Regulation ("GDPR"), a privacy law that has been coined as "one of the strongest and most comprehensive attempts globally to regulate the collection and use of personal data by both governments and the private sector."[128] Two years later, the State of California adopted the California Consumer Privacy Act of 2018 ("CCPA"), a privacy law "creating one of the most significant regulations overseeing the data-collection practices of technology companies in the United States."[129] In this Part, this Note proposes certain attributes that a new federal data privacy law should

125. Yurieff, *supra* note 105 ("Gmail, which has over 1.4 billion users globally, lets third-party developers integrate services into its email platform, such as trip planners and custom relationship management systems.").

126. Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1246 (10th Cir. 2012).

127. Congress is currently contemplating what the United States' first federal data-privacy law should look like in light of other data-privacy legislation, such as the CCPA and the GDPR. *See* Rhys Dipshan, *House Hearing on Federal Privacy Law Takes Aim at GDPR, CCPA*, LAW.COM: LEGALTECH NEWS (Feb. 26, 2019, 2:24 PM), https://www.law.com/legaltechnews/2019/02/26/house-hearing-on-federal-privacy-law-takes-aim-at-gdpr-ccpa/ [https://perma.cc/6H6K-JCPN] ("A U.S. House of Repre–sentatives hearing on consumer privacy largely dismissed the EU's General Data Protection Regulation and the California Consumer Privacy Act as the basis for future federal privacy legislation. But there was consensus that the status quo is unsustainable, with some arguing that the nationwide adoption of certain GDPR and CCPA principles is necessary in the U.S.").

128. *The EU General Data Protection Regulation*, HUMAN RIGHTS WATCH (June 6, 2018, 5:00 AM), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [https://perma.cc/JX2F-ZRNY].

129. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/5TM4-U2BH].

possess based on the strengths and weaknesses of both the GDPR and the CCPA.

A. European Union General Data Protection Regulation

The GDPR provides "data subjects"[130] in the European Union ("EU") with several rights, including: the "right to be informed" (prescribing when information must be given to data subjects and what they must be informed of);[131] the "right of access" (allowing data subjects to have full visibility of the data an organization holds about them);[132] the "right to rectification" (granting data subjects the ability to have inaccurate personal data rectified, or completed if it is incomplete);[133] the "right to erasure" (allowing individuals to request the deletion of their personal information);[134] the "right to restrict processing" (providing data subjects with the ability to limit the way that an organization uses their data);[135] the "right to data portability" (allowing subjects to receive their data processed on the basis of contract or consent in a structured, commonly used, and machine-readable format and to transmit that data to another controller without hindrance);[136] and the "right to object" (granting data subjects the ability to object to any type of processing of personal data).[137]

The GDPR applies to all data controllers and data processors that hold EU citizens' personal data.[138] Accordingly, the GDPR applies specifically to organizations that may not have a presence in the EU, but still offer goods and services to, or monitor the behavior of, persons in the EU.[139] Data subjects must "opt in" to data collection, meaning

130. GDPR, *supra* note 5, at 33 (A data subject is "an identified or identifiable natural person.").

131. *Id.* at 11–12.

132. *Id.* at 43.

133. *Id.*

134. *Id.* at 43–44.

135. *Id.* at 44–45.

136. *Id.* at 45.

137. *Id.* at 45–46; *see also* Sarah Hospelhorn, *California Consumer Privacy Act (CCPA) vs. GDPR*, VARONIS, https://www.varonis.com/blog/ccpa-vs-gdpr/ [https://perma.cc/84TQ-A6M4] (last updated Nov. 5, 2018).

138. *See generally* GDPR, *supra* note 5.

139. DATAGUIDANCE & FUTURE OF PRIVACY FORUM, COMPARING PRIVACY LAWS: GDPR V. CCPA 8 (2018), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [https://perma.cc/SL84-AM54], *available at* Gabriela Zanfir-Fortuna & Michelle Bae, *CCPA, Face to Face with the GDPR: An In Depth Comparative Analysis*, FUTURE OF PRIVACY F. (Nov. 28, 2018), https://fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/ [https://perma.cc/WE2R-

that each website a data subject visits must obtain consent from the data subject prior to collecting the data subject's data.[140]

Individuals may seek damages for injuries caused by security-measures violations or data breaches.[141] Organizations in breach may be fined up to four percent of annual global turnover or €20,000,000.[142]

B. California Consumer Privacy Act of 2018

The CCPA provides consumers[143] with four main rights: access, deletion, opt-out, and non-discrimination. The rights to "access"[144] and "deletion"[145] are similar to those guaranteed under the GDPR. Unlike the GDPR, however, the CCPA has both a "right to opt out" (allowing consumers to opt out from selling of their personal information) and a "right of non-discrimination" (protecting consumers from being discriminated against for exercising their privacy rights).[146]

Only California businesses of a substantial size that collect consumer personal data are subject to the CCPA.[147] Compared to how data subjects in the EU have a right to opt in and object to *data collection*, consumers in California can only opt out of *the sale of personal data*, not the collection of data or any other use that does not

2P67]. Indeed, the GDPR commenced an enforcement notice against a Canadian data controller, AggregateIQ, in September 2018. Jonathan Chadwick, *AggregateIQ Hit with First GDRP* [sic] *Enforcement Notice*, COMPUTER BUS. REV. ONLINE (Sept. 21, 2018), https://www.cbronline.com/news/gdpr-enforcement [https://perma.cc/V7SP-CX62].

140. GDPR, *supra* note 5, at 6 ("Silence, pre-ticked boxes or inactivity should not constitute consent.").

141. *Id.* at 80–82.

142. *Id.* at 83.

143. CCPA, *supra* note 6, § 1798.140(g) ("'Consumer' means a natural person who is a California resident . . . .").

144. *Id.* § 1798.110.

145. *Id.* § 1798.105(a).

146. *Id.* § 1798.125(a)(1)(A)–(C) ("A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer."). This provision can be interpreted to mean that businesses cannot charge the *specific* consumers that opt out of data collection a subscription fee without charging *all* consumers a subscription fee.

147. *Id.* § 1798.140(c). Only California businesses that earn $25,000,000 or more in revenue, or that annually buy, receive, sell or share personal information of 50,000 or more consumers, households or devices for commercial purposes, or that derive 50% or more of its annual revenue from selling consumer personal information is subject to the CCPA. *Id.*

fall under the definition of "selling."[148] Personal information obtained through automated means, such as the email-scanning practices at issue in *In re Google, Inc. Gmail Litigation* and *In re Google, Inc. Privacy Policy Litigation*, are regulated under the CCPA because "selling" encompasses disseminating a digital user's information to a third party.[149]

Although businesses cannot discriminate against consumers for their privacy choices, businesses may provide a consumer with "financial incentives," including compensation, for allowing the business to collect, sell, or not delete a consumer's personal information.[150] The CCPA also requires that businesses include a "Do Not Sell My Personal Information" link on their home webpage.[151] Further, there is a specific requirement that consumers must receive an explicit notice when a third party intends to sell personal information as part of a merger.[152]

The GDPR specifies that organizations that do not have a physical presence in the EU may be subject to the GDPR.[153] It is unclear whether the CCPA applies to a business established outside of California that collects or sells California consumers' personal information while

148. DATAGUIDANCE & FUTURE OF PRIVACY FORUM, *supra* note 139, at 30. "Selling" includes "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . personal information . . . for monetary or other valuable consideration." CCPA, *supra* note 6, § 1798.140(t)(1).

149. *See* CCPA, *supra* note 6, § 1798.140(t)(1); *see also id.* § 1798.140(q) ("'Processing' means any operation or set of operations that are performed on personal data or on sets of personal data, *whether or not by automated means*." (emphasis added)).

150. *Id.* § 1798.125(b)(1).

151. *Id.* § 1798.135(a)(1).

152. *Id.* § 1798.130(a)(2).

153. GDPR, *supra* note 5, at 22–23. Under the GDPR, a company is subject to the GDPR if it processes personal data of an individual residing in the EU when the data are accessed. *Id.*

conducting business.[154] Businesses in breach of the CCPA can be fined up to $7,500 per violation.[155]

The state attorney general has the exclusive power to enforce the CCPA, except in data-breach cases where the attorney general declines to prosecute within thirty days of being notified of a consumer's intent to bring suit.[156]

C. Analysis

Although both the GDPR and the CCPA "aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share consumer data,"[157] they both pose various issues. The GDPR's opt-in requirement, for example, relies on the premise that digital users actually read the consent and disclosures webpage before waiving their privacy rights by clicking an "accept" button.[158] Adhesion contracts on webpages may not be the best way to

154. DATAGUIDANCE & FUTURE OF PRIVACY FORUM, *supra* note 139, at 8. In general, when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms. *See* Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 455–56 (2007) (citing Smith v. United States, 507 U.S. 197, 204 (1993)). This *Pennoyer*-esque presumption may be outdated, as illustrated by a recent decision issued by the United States Supreme Court. In *South Dakota v. Wayfair, Inc.*, the Court held that online retailers without a physical presence in a state—but with sufficient contacts in that state—could be required to collect use taxes from its in-state customers. 138 S. Ct. 2080, 2099 (2018). The Court reasoned that "[b]etween targeted advertising and instant access to most consumers via any [I]nternet-enabled device, 'a business may be present in a State in a meaningful way without' that presence 'being physical in the traditional sense of the term.'" *Id.* at 2095 (quoting *Direct Marketing Assn. v. Brohl*, 135 S. Ct. 1124, 1135 (2015)). *Wayfair* suggests that businesses that collect data of California residents online may be subject to the CCPA, even if they do not have a "traditional" physical presence in California. Should an out-of-state business be required to obey another state's tax and data privacy laws? *See* Jonathan L. Entin, *Another Superseded* Quill*: The End of the Physical-Presence Rule for Requiring Out-of-State Businesses to Collect Use Taxes*, 36 J. TAX'N INV. 15, 23 (2018) ("The Supreme Court's *Wayfair* decision leaves many uncertainties. . . . Most of those uncertainties relate to how the Court will define the scope of state authority to compel out-of-state-business to collect use taxes . . . .").

155. CCPA, *supra* note 6, § 1798.155(b).

156. *Id.*

157. Zanfir-Fortuna & Bae, *supra* note 139.

158. *But cf. 15 Unexpected Consequences of GDPR*, FORBES (Aug. 15, 2018, 9:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#54a41c594ad7 [https://perma.cc/K3D8-SG56] ("Another unintended impact is 'check the box' fatigue where opt-in consent language is presented so frequently on websites and

obtain informed consent. A digital user's online experience is hindered when they are persistently being asked for consent every time they visit a new website. Although the CCPA's opt-out requirement allows for a less intrusive user experience, the requirement only applies to the selling of data, not the collection of it. As a result, digital users are not given adequate control over how their personal information is used under the CCPA.

The CCPA's $7,500 per violation fine may also be minuscule in comparison to the GDPR's potential fine. Along with weak penalties that may not deter businesses from breaching a digital user's privacy, the CCPA applies only to very specific businesses, which may result in businesses restructuring themselves in a way that exempts them from liability under the CCPA. For example, a company may structure its finances so that it does not generate $25,000,000 in revenue. A company may also outsource data-mining practices to international third-party companies that may not be subjected to the CCPA.[159] Lastly, neither the CCPA nor the GDPR explicitly permit businesses to charge an additional fee only to consumers who want to use a business's products and services but who do not want their information monetized. As a result, businesses subject to the CCPA and the GDPR may have no choice but to begin charging subscription fees to *all* digital users because *some* value their privacy more than others.

D. Proposal

New legislation should be focused on providing digital users the ability to retain control over how their personal information is shared. American digital users should be granted the right to access their personal information that was collected, processed, or sold by an organization. Organizations should be given at least ten business days to comply with an American digital user's request for personal information by sending those users a hard copy of the personal information via first-class mail or sending the American digital user a PDF by email.

American digital users should also be granted the right to delete personal data that organizations have collected from them. Upon a request to an organization that their data be deleted, American digital users should receive a confirmation via first-class mail or email that their data has been deleted.

Increased privacy may come at a cost. Just as American digital users should have the ability to opt out of the collecting, processing, and selling of their personal information, ECSPs should be permitted to charge a subscription fee to those users. Such a system would allow

apps that consumers don't read the consents and just check the box, waiving their privacy rights.").

159. *See* DATAGUIDANCE & FUTURE OF PRIVACY FORUM, *supra* note 139, at 8–9.

American digital users who are comfortable exchanging their data in return for a free service to continue to do so, while still protecting users who place a higher premium on their personal information.

Instead of cluttering webpages with adhesion contracts or "Do Not Sell My Personal Information" buttons, Congress should create a federal data privacy website where American digital users register an account and set their default privacy preferences.[160] After registering for an account, those users should be given a list of all websites that collect, process, or sell information about them. After reviewing that list, users should be able to opt out of the data-collection practices of some or all of the sites. Information gathered from that central webpage about each American digital user's privacy preferences should then be sent to the ECSPs that are subject to the new federal legislation to ensure they comply with each user's preferences.

American digital users who are not comfortable providing information to the federal data privacy website should still be given the chance to opt out of the collection, process, and sale of their personal information directly from the ECSP. Accordingly, although there does not need to be a "Do Not Sell My Personal Information" button on the top of every homepage, ECSPs subject to the new federal legislation should still provide American digital users the ability to opt out in a privacy settings tab on their main webpage.

The new federal legislation should be implemented by a federal agency. An existing agency, such as the Federal Trade Commission, could enforce the legislation.[161] The Federal Trade Commission currently "oversees consumer protection and enforces antitrust laws, but has limited ability to police data privacy."[162] The Federal Trade Commission should have the ability to enforce the new data privacy

160. Since the webpage would be collecting information of American digital users, the national website should be exempt from the new federal legislation. *See* Consumer Data Protection Act, SIL18B29, § 6 (a)(1)(A) 115th Cong. (2018) (proposing that the Federal Trade Commission implement and maintain a ''Do Not Track'' data sharing opt out website that allows consumers to opt out of data sharing, view their opt out status, and change their opt out status).

161. An existing agency such as the Federal Trade Commission can be tasked with enforcement. Alternatively, a new agency, consisting of professionals who are familiar with data analytics, technology, and software development, may be created to enforce the new federal data privacy legislation.

162. Daniel R. Stoller & Ben Brody, *New FTC Powers Weighed in Senate Data Privacy Hearing*, BLOOMBERG LAW (Feb. 27, 2019, 2:28 PM), https://www.bloomberglaw.com/document/XC7HDUR8000000?bna_news_filter=privacy-and-data-security&jcsearch=BNA%2520000001692f6cd275a76bbf7e443f0002#jcite [https://perma.cc/KTC8-L357].

legislation in conjunction with the states' attorneys general,[163] similar to its enforcement powers under the Children's Online Privacy Protection Act.[164]

Although the new federal legislation should be comprehensive and detailed, technology progresses at an exponentially faster rate than the law. Congress cannot possibly foresee every potential way data might be processed or collected in the future. Accordingly, the new legislation should provide the enforcing agency with limited rulemaking authority, specifically in the area of determining what actions constitute "collecting" or "processing" an American consumer's data.

The enforcing agency should be tasked with ensuring organizations comply with the new federal legislation. To do so, it should have the power to conduct investigations, manage the new federal data privacy website, offer compliance advice to organizations (perhaps via an anonymous hotline),[165] and outline compliance protocols in an annually updated manual.[166] The new federal legislation should also require

163. *See id.*

164. 15 U.S.C. § 6505 (2012).

165. American organizations should be given the necessary tools to comply with the new federal legislation. Based on a Crowd Research Report, EU organizations' main GDPR-compliance challenges are "a lack of expert staff (cited by 43 percent), lack of budget (40 percent), and a limited understanding of GDPR regulations (31 percent)." Bob Violino, *GDPR Compliance: For Many Companies, it Might be Time to Panic*, ZDNET (May 24, 2018, 9:31 AM), https://www.zdnet.com/article/gdpr-compliance-for-many-companies-it-might-be-time-to-panic/ [https://perma.cc/NKK8-X39E].

166. Compliance with federal law may be easier for large companies with divisions dedicated to compliance. For mid-size and small companies who do not have adequate resources, the agency can serve as a resource to ensure that they can comply with federal law and stay in business. *See* Ivana Kottasová, *These Companies are Getting Killed by GDPR*, CNN (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html [https://perma.cc/4LUM-N7VE] ("The cost of complying with the [GDPR] has already forced an online game producer, a small social network and a mobile marketing firm to close key businesses or shut down entirely. . . . Complying with the new regulations isn't cheap, and experts say the world's biggest companies are spending tens of millions of dollars to prepare. Smaller companies that do not have the same resources are struggling."); *see also* Lisa V. Zivkovic, *The Alignment Between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject*, 28 TRANSNAT'L L. & CONTEMP. PROBS. 189, 210–11 (2018) ("The discretion left to the supervisory authorities to ensure compliance is arguably substantial. In other words, given the potential for liability, the cost to comply, and the uncertainty regarding requirements for actual compliance, American multinational companies are arguably more likely to sever their business models and localize their data rather

organizations to submit to the enforcing agency semi-annual reports outlining what data-collection practices the company is using and where each American digital user's data are going.

This proposed federal legislation should preempt state data privacy laws.[167] Under the principles of federalism, the new federal legislation should trump state privacy laws such as the CCPA.[168] The new federal legislation also should not use restrictive language to define who is subject to the statute because companies who do not meet a revenue threshold, for instance, are still capable of invading a digital user's privacy. Instead of following the CCPA's definition of "business,"[169] the new federal legislation should refer to organizations in more general terms, such as "data controllers" and "data processors."[170] The new federal legislation should have a provision explicitly stating that the statute applies to data processors and data controllers who are not physically located in the United States but collect information from American digital users. As a result, organizations subject to the new federal legislation would be discouraged from outsourcing their data-mining practices abroad to foreign companies.

Penalties under the new federal legislation should deter organizations from breaching a digital user's privacy. The federal legislation should follow the GDPR and require breaching organizations to pay either four percent of annual turnover or $20,000,000 for an offense. American digital users should be notified directly from the

than risk not only losing business in the EU but also suffering the important economic penalties for non-compliance.").

167. As noted by the Federal Trade Commission's former Chairman, Jon Leibowitz, "'[y]ou don't want a cacophony or a crazy quilt patchwork of [fifty] different state laws . . . [i]t'll make consumers numb to notifications' about companies' data privacy policies." Gopal Ratnam, *Senate Commerce Chairman Eyes Data Privacy Bill This Year*, ROLL CALL (Feb. 28, 2019, 1:43 PM), https://www.rollcall.com/news/congress/senate-commerce-chairman-eyes-data-privacy-bill-year [https://perma.cc/XRP6-TCDT].

168. *See* McCulloch v. The State of Maryland et al., 17 U.S. (4 Wheat.) 316, 360–61 (1819) (stating that "the States are prohibited from passing any acts which shall be repugnant to a law of the United States."). A comprehensive federal data privacy law may also avoid the significant constitutional concerns inherent in a state-by-state patchwork approach to data privacy. *See* Mallory Ursul, *The States' Role in Data Privacy: California Consumer Privacy Act Versus Dormant Commerce Clause*, 52 SUFFOLK U. L. REV. 577, 602 (2019) (stating that "if circumstances change where more states begin to regulate data privacy and create regulatory conflict, the CCPA may be held unconstitutional under the Dormant Commerce Clause.").

169. CCPA, *supra* note 6, § 1798.140(c)(1).

170. *See* GDPR, *supra* note 5, at 33 (broadly defining both "controller" and "processor").

enforcing agency if their personal information was involved in a data breach. The enforcing agency and the states' attorneys general should have the exclusive authority to prosecute organizations who violate the new federal legislation. If either decline to prosecute an organization, American digital users affected by a serious breach should be permitted to file a grievance with the enforcing agency and exhaust all administrative remedies before filing a civil suit against an ECSP in federal court.

CONCLUSION

Federal data privacy legislation has appeared on the horizon and will likely be formally introduced to Congress in the coming year.[171] For example, Senator Ron Wyden's bill, the Consumer Data Protection Act of 2018,[172] creates a set of minimum cybersecurity and privacy standards, a national Do Not Track system that allows consumers to stop third-party data companies from tracking them on the web, and establishes a consumer's right to know what personal data is being collected about her and how it is being used.[173] Senator Brian Schatz's bill, the Data Care Act of 2018,[174] proposes a "duty to care" regulatory approach that would require tech companies to provide a "reasonable" level of security around personal data.[175]

Until a federal data privacy law is passed by Congress, however, digital users are left with little to no control over how their personal information is used by ECSPs under existing law.[176] The Wiretap Act's

171. Mark Sullivan, *Inside the Upcoming Fight over a New Federal Privacy Law*, FAST COMPANY (Jan. 4, 2019), https://www.fastcompany.com/90288030/inside-the-upcoming-fight-over-a-new-federal-privacy-law [https://perma.cc/YG2E-FZVT] ("There may be as many as six major bills circulating in the Senate by mid-2019. And with the new Democratically controlled House, such a bill may have a good chance of passage."); *see also* Ratnam, *supra* note 167 ("Senate Commerce, Science and Transportation Chairman Roger Wicker is aiming to have a federal data privacy bill written and passed by Congress this year as technology companies, privacy advocates and civil rights groups press lawmakers to act decisively to avoid a patchwork of state legislation.").

172. Consumer Data Protection Act, S. 2188, 115th Cong. § 1 (2018).

173. Sullivan, *supra* note 171.

174. Data Care Act, S. 3744, 115th Cong. § 1 (2018).

175. Sullivan, *supra* note 171.

176. Digital users are, however, suing ECSPs under the Wiretap Act in unprecedented contexts. *See, e.g.*, Satchell v. Sonic Notify, Inc., 234 F. Supp. 3d 996, 1000 (N.D. Cal. 2017) (alleging that an app provider used beacon technology to turn on a user's smartphone microphone and record the user's communications in order to track how the user interacted with marketing and advertisements); Rackemann v. LISNR, Inc., No. 117-CV-00624-TWP-MJD, 2017 WL 4340349 at *1–2 (S.D. Ind. Sept. 29, 2017)

"conflicting privacy standards that create uncertainty and confusion for law enforcement, for the business community, and for American consumers"[177] will inevitably worsen as technology continues to advance[178] and tech giants such as Amazon enter the digital marketing industry.[179]

It is time that Americans receive adequate protection under a law that provides them the ability to retain control over how their personal information is shared. That time is now.

Helen Jazzar[†]

(same); *In re* Lenovo Adware Litig., No. 15-MD-02624-RMW, 2016 WL 6277245 at *1 (N.D. Cal. Oct. 27, 2016) (alleging that a manufacturer sold computers with pre-installed adware programs that collected the user's data, redirected the data to a third party to generate relevant advertisements, and then "transmit[ed] those advertisements back to the user's web browser as part of a webpage or in a pop-up ad"); Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078, 1083–84 (N.D. Cal. 2018) (alleging that Uber used spyware to secretly collect information from Lyft's servers and Lyft's customers' smartphones, such as a Lyft driver's precise geolocation data, her willingness to provide rides, and an estimated ride price for the ride).

177. *Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 2 (2011) (statement of Vermont Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary).

178. *See* Raymond Ku, *Foreword: A Brave New Cyberworld?*, 22 T. JEFFERSON L. REV. 125, 127 (2000) ("From smart credit cards which tell stores not only whether we can make the purchase but what we have purchased in the past, to cellular telephones that allow us to reach out to anyone around the world while making it possible for others to reach us, to on-board automobile navigation systems that help us to find a friend's home and which also allow others to track our movements, to home security systems that not only sound an alarm when someone tries to enter the home, but allow us to turn lights on and off from remote locations, we live in a world increasingly interconnected by technology.").

179. Julie Creswell, *Amazon Sets its Sights on $88b Online Ad Market*, GULF NEWS (Sept. 4, 2018, 2:56 PM), https://gulfnews.com/technology/media/amazon-sets-its-sights-on-88b-online-ad-market-1.2274472 [https://perma.cc/7MSZ-NFCZ] ("Amazon . . . is quickly gathering momentum in a new, highly profitable arena: online advertising, where it is rapidly emerging as a major competitor to Google and Facebook.").

† J.D. Candidate, 2020, Case Western Reserve University School of Law; B.A., Ursuline College. The author would like to thank Professor Emeritus Jonathan L. Entin for advice and support in writing this Note as well as the Case Western Reserve Law Review editors for their great work improving it. The author would like to dedicate this Note to her loving and supportive family.