NOTE

Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home

Allegra Bianchini[*]

ABSTRACT

What do you say in your home when you think no one is listening? Have you ever contemplated that someone might be listening? What would you do if a recorded log of what you say and do behind closed doors could be used against you? With the recent rise of digital assistant devices, often referred to as "always on, always listening" devices, this circumstance is a tangible reality. Given the state of digital data protection, the information collected by these devices and stored on service provider "clouds" remains ambiguously protected and in some cases subject to warrantless government searches. This Note proposes that, given the intimate nature of this data and the rationale supporting recent Supreme Court decisions concerning the Fourth Amendment, it should be afforded a higher level of protection than it currently receives under the Electronic Communications Privacy Act of 1986 ("ECPA"). Instead, it should be treated as a physical aspect of a user's home, consistent with the Supreme Court's analysis in Kyllo v. United States. *Bolstered by the reasoning used by the Supreme Court, this Note proposes that Congress amend the ECPA to provide such protection for digital information beyond just "communications" in order to maintain the high level of privacy in one's home that has been valued by the United States since the time of its founders.*

INTRODUCTION

On November 22, 2015, Victor Parris Collins was found dead in a patio hot tub at the home of James Andrew Bates in Bentonville,

[*] J.D., expected May 2018, The George Washington University Law School; B.A., 2014, Colgate University.

Arkansas.[1] According to Bates's affidavit, the two men had spent the night drinking and watching football with two other friends.[2] After going to bed, leaving Collins with another friend in the hot tub, Bates claimed he woke up several hours later and found his friend floating dead in the hot tub.[3] Three months later, Bates was arrested on charges of first-degree murder.[4] Classic techniques, including forensics, descriptions of the scene, and evidence found in Bates's home, have guided prosecutors in their investigation in the months since November 22, 2015.[5] But notably, prosecutors turned to modern technology to develop their case in a new way,[6] using a set of digital information that did not exist less than a decade ago.[7] This information was collected by an Amazon Echo,[8] an "always-on" device designed to listen to its owner, record orders, and send these orders to the cloud to process and carry out.[9] The prosecutors wanted to learn what Bates's Echo heard during the events of the night, hoping to gain information to aid in the prosecution of the case.[10] Aside from the unlikely

---

1 *See* Zuzanna Sitek & Dillon Thomas, *Bentonville PD Says Man Strangled, Drowned Former Georgia Officer*, 5NEWS, http://5newsonline.com/2016/02/23/bentonville-pd-says-man-strangled-drowned-former-georgia-officer/ (last updated Feb. 25, 2016, 10:43 PM).

2 *See id*.

3 *See id*.

4 *See* Josh Hart, *Smart Meter Data at Crux of Arkansas Murder Case*, STOP SMART METERS! (Aug. 26, 2016), http://stopsmartmeters.org/2016/08/26/smart-meter-data-at-crux-of-arkansas-murder-case/ [https://perma.cc/4QNQ-NLEN].

5 *See* Sitek & Thomas, *supra* note 1.

6 *See* Hart, *supra* note 4; Eliott C. McLaughlin & Keith Allen, *Alexa, Can You Help with this Murder Case?*, CNN (Dec. 28, 2016, 8:48 PM), http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/; Sitek & Thomas, *supra* note 1.

7 *See* Eugene Kim, *The Inside Story of How Amazon Created Echo, the Next Billion-Dollar Business No One Saw Coming*, BUS. INSIDER (Apr. 2, 2016, 12:01 PM), http://www.businessinsider.com/the-inside-story-of-how-amazon-created-echo-2016-4 (discussing the advent of the Amazon Echo).

8 *See* McLaughlin & Allen, *supra* note 6.

9 *See* Richard Baguley & Colin McDonald, *Appliance Science: Alexa, How Does Alexa Work? The Science of the Amazon Echo*, CNET (Aug. 4, 2016, 5:00 AM), https://www.cnet.com/news/appliance-science-alexa-how-does-alexa-work-the-science-of-amazons-echo; Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo?redirect=blog/free-future/privacy-threat-always-microphones-amazon-echo [https://perma.cc/2F3Q-3HPU].

10 *See* McLaughlin & Allen, *supra* note 6. The police in the Bates case did obtain a warrant. *See* Billy Steele, *Police Seek Amazon Echo Data in Murder Case (updated)*, ENGADGET (Dec. 27, 2016), https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case/. As discussed below, however, this Note focuses on the intersection of several legal frameworks that converge to regulate these devices, and concludes that, although a statutory requirement to obtain a warrant for this type of information does not

possibility that anyone perpetrating a crime would purposely engage a device of this sort in the events, police were hoping that the device might have been activated accidentally, thereby recording something it was not supposed to hear.[11]

This case brings to light new questions about the boundaries of privacy in one's home. Most prominent is the question of whether consumers maintain an expectation of privacy when they bring listening devices into their homes.[12] Further complicating this situation, these products are not self-contained processing devices, but rather require interaction with and storage on their host companies' data clouds in order to function.[13] Finally, the devices combine the capabilities and characteristics of previously separate devices that up until now have been subject to separate regulatory schemes, rendering the privacy protections applicable to digital assistants difficult to determine.[14] The question thus becomes: to what extent is data protected from government acquisition when a user knowingly allows it to be processed and stored on public servers? In the case of smart-home technology, the question is particularly compelling, given the deeply personal nature of the data being collected and stored.[15] The advent of smart-home technology, in conjunction with the explosive growth of cloud computing, has opened private homes to vulnerability through the internet, raising new questions concerning data privacy and the protections of the Fourth Amendment.

The main source of constitutional privacy protection in the United States, the Fourth Amendment, was drafted at a time when citizens could hardly conceive of the issues raised by these modern devices. Even as Congress and the courts have attempted to apply privacy protections to the digital age, new inventions rapidly render laws obsolete as they continue to push the bounds of technological capabilities.[16]

Fourth Amendment jurisprudence pertaining to physical intrusions into

---

currently exist, the Supreme Court's recent Fourth Amendment jurisprudence suggests that a warrant for this information may well be constitutionally required.

11 *See* McLaughlin & Allen, *supra* note 6.

12 *See id*.

13 *See* Baguley & McDonald, *supra* note 9; Elyse Betters, *What Are Google Home, Home Max, and Home Mini and What Can They Do?*, POCKET-LINT (Feb. 15, 2018), http://www.pocket-lint.com/news/137665-what-is-google-home-how-does-it-work-and-when-can-you-buy-it [https://perma.cc/96B9-3DZD].

14 *See infra* Section III.B.

15 *See infra* Section I.A.

16 *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 375–76 (2014) (explaining how various technological changes, including the "plummeting costs of [data] storage" and the global nature of the internet, have rendered existing electronic privacy law "outdated").

one's home is well established and provides protection against unreasonable searches and seizures.[17] This physical protection extends even into situations of temporary occupation, such as apartments, storage lockers, and hotel rooms.[18] Fourth Amendment protection of digital information, however, has historically been substantially lower due to the third-party doctrine.[19] The third-party doctrine eliminates privacy protection of information an owner discloses to a third party.[20] While this distinction has been a practical divergence for existing technology, the new smart-home technologies require revisiting the divergent path.[21] By enacting the Electronic Communications Privacy Act of 1986 ("ECPA"),[22] Congress attempted to extend privacy protection to electronic information but was limited by the focus on existing technology.[23] By only protecting what was classically considered "communication," Congress may have left all other noncommunicative digital data under the protection of the more general Fourth Amendment jurisprudence.[24] This protection is wholly inadequate given the existence of the third-party doctrine and provides a level of protection inconsistent with modern notions of privacy within the home.[25]

Technology such as the modern digital assistant has pushed past mere communication capabilities and has become integrated into daily life in countless ways.[26] Because of the intimacy with which smart digital

---

17 *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (applying Fourth Amendment analysis to modern technology); Katz v. United States, 389 U.S. 347 (1967) (establishing the modern framework of Fourth Amendment jurisprudence).

18 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 810 (2004).

19 *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 634 (2011) ("According to what was, for a time at least, the accepted wisdom, there is virtually no Fourth Amendment protection for any information conveyed over the Internet or other digital intermediary.").

20 *See* Christina Raquel, Comment, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud*, 55 SANTA CLARA L. REV. 467, 477 (2015) ("Under the third party doctrine, an individual relinquishes his or her reasonable expectation of privacy when he or she knowingly reveals private information to another person, effectively assuming the risk that the other person will reveal the once-private information to the government.").

21 *See* Stanley, *supra* note 9.

22 Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

23 *See* Kerr, *supra* note 16, at 378–86 (describing the technology that existed at the time of the enacting of the ECPA, and the influence it exerted on the drafting of the Act).

24 *See infra* Part III.

25 *See infra* Section IV.A.

26 *See infra* Section I.A.

assistants like the Amazon Echo and the Google Home are integrated into modern homes, the data received from the devices and stored in the companies' clouds should be treated as a physical component of the user's home and should be subject to the Fourth Amendment protections afforded to physical property. Congress should pass a statutory amendment to the ECPA allowing for the protection of this small but deeply personal category of information. This Note does not argue that information of this sort should be wholly inaccessible to law enforcement, but rather that it should be afforded the same protection as the physical aspects of a user's home.

Part I of this Note discusses modern digital assistants, specifically the Amazon Echo and the Google Home, and describes both their capabilities and storage capacity. Part I also explains how the technology works and focuses specifically on the "cloud" aspect of the technology that makes data privacy in this area so contentious. Part II presents the various regulatory schemes that may apply to digital assistants. Part III explains why the regulatory framework cannot be coherently united to apply to the modern digital assistant and points out the reasons that a new, more cohesive regime is required. Part IV proposes an amendment to the ECPA that uses the Supreme Court's more recent language in *Kyllo v. United States*[27] to provide a section on noncommunicative information, and discusses the more general interests that are advanced by amending the ECPA in this way.

I. MODERN DIGITAL ASSISTANTS: HOW THEY WORK

Recent technological advances have allowed for a new wave of digital assistants: small electronic devices capable of looking up the weather forecast, searching the internet, or placing an order on Amazon—all conveniently controlled by the user's voice.[28] Though there are new devices entering the market each year that implicate similar data privacy questions, this Note focuses on two in particular as examples of the broader technological landscape: the Amazon Echo and the Google Home. This Part explains the mechanics of how users interact with the devices and the "cloud" platforms that enable them to function.

A. The Amazon Echo and the Google Home

Both the Amazon Echo and the Google Home are small devices that take up only a few square inches of counter space, and, through the internet, can perform a range of tasks from playing a certain song to

---

[27] 533 U.S. 27 (2001).

[28] *See* Baguley & McDonald, *supra* note 9; Betters, *supra* note 13.

checking the weather.[29] They are always on and always passively listening for their activation "wake words" ("Ok Google" for the Google Home; "Alexa" for the Amazon Echo), which trigger the devices to record the next few seconds of the user's voice, process the request, and respond to the command.[30] But unlike other small electronic devices, the computing power on these devices is not contained on the devices themselves.[31] Instead, the computing processes take place in the "cloud," the term that refers to the vast online storage space shared by companies offering internet services, called "internet servers."[32] For the Amazon Echo, the information is sent to Amazon's cloud for processing.[33] Once received by Amazon's cloud, the information is processed by Amazon's platform, Alexa Voice Services, which interprets the voice recording and extracts the command.[34] The Echo then interprets this command and carries it out,[35] the whole process occurring in a matter of seconds.[36] The Google Home follows a similar process, whereby the device listens for what Google calls the "hotword" and then records a few seconds of voice, which is ultimately sent to Google to process.[37] The data is saved in Google's data centers until the user deletes it.[38]

Fresh out of the box, both devices can perform basic tasks such as responding to audio requests for information, looking up traffic conditions, or checking a calendar.[39] Given a few steps of setup, both can be further integrated into a user's home to perform tasks such as turning on lights.[40] Integration to control lightbulbs, smart meters, and phone apps, like Uber,

---

29 *See id*.

30 *See id*.

31 *See* Baguley & McDonald, *supra* note 9.

32 *See* Joanna Stern, *What Is the 'Cloud'?*, ABC NEWS (June 26, 2012), http://abcnews.go.com/Technology/cloud-computing-storage-explained/story?id=16647561.

33 *See* Baguley & McDonald, *supra* note 9.

34 *See id*.

35 *See id*.

36 *See* Techfreshness, *Amazon Echo Review (Best Echo Demo on YouTube)*, YOUTUBE (Dec. 11, 2015), https://www.youtube.com/watch?v=QXsPcYLcrw0.

37 *See Data Security & Privacy on Google Home*, GOOGLE, https://support.google.com/googlehome/answer/7072285?hl=en [https://perma.cc/YD4C-NPCH] (last visited Feb. 16, 2018).

38 *See id*.

39 *See* Anna Attkisson, *What Is the Amazon Echo?*, TOM'S GUIDE (Oct. 2, 2016, 7:30 AM), http://www.tomsguide.com/us/amazon-echo-faq,review-3377.html [https://perma.cc/3Y6X-C6TX]; *Google Home*, GOOGLE, https://store.google.com/product/google_home (last visited Feb. 16, 2018).

40 *See* Baguley & McDonald, *supra* note 9; *Here's Everything That Works with Google Home and Home Mini*, CNET, (Oct. 3, 2017, 9:28 AM), https://www.cnet.com/pictures/everything-that-will-work-with-google-home/.

allows nearly complete virtual control of a user's home,[41] and the possibility of more capabilities is limited only by programmers' imaginations.[42] Though the devices do not constantly monitor all of these aspects of a user's home, each command is recorded.[43] Thus, the stored information yields deeply private information regarding when a user is home and what the user is doing, based on when he or she is interacting with the digital assistant. If an individual has multiple devices in different rooms of his or her home, the logs together can even yield information such as which room of the home an individual is in at any given time, based on when the individual was speaking to each device. Essentially, these devices have created a new, intimate digital aspect of one's home. Information that previously required surveillance and constant monitoring, such as when users are home, their day-to-day schedules, which room of the house they are in at what time, and how often they use certain appliances and security, are now conveniently logged into a record. Actions that were once purely physical, like flicking on the lights, are now digitized and recorded, creating a detailed record of what goes on behind closed doors. Given that the technology is becoming increasingly widespread (an estimated 5.2 million Echos were sold globally in 2016),[44] the time has come to understand the parameters and protections afforded to this class of information stored on the elusive "cloud."

B. What Is the "Cloud"?

The rise of interconnectivity between devices through the internet has resulted in an internet-based storage "cloud" that is characterized by storage on internet servers rather than individual devices.[45] Computers typically rely on "local storage," whereby data is stored on a local disk contained within the device itself.[46] Even though a user's data may be more

---

41 *See Echo (2nd Generation)*, AMAZON, https://www.amazon.com/gp/product/B0749WVS7J/ref=ods_ac_dp_dr_ps [https://perma.cc/26S2-9JAL] (last visited Feb. 16, 2018).

42 *See* Baguley & McDonald, *supra* note 9.

43 *See id*.

44 *See* Jeff Dunn, *It's Been a Good Year for the Amazon Echo*, BUS. INSIDER (Dec. 28, 2016, 3:51 PM), http://www.businessinsider.com/amazon-echo-sales-figures-stats-chart-2016-12. The device even sold out during the 2016 Christmas season. *See* Kif Leswing, *Amazon Echo Is Sold Out for Christmas*, BUS. INSIDER (Dec. 21, 2016, 10:40 AM), http://www.businessinsider.com/amazon-echo-dot-fire-stick-shipping-dates-after-christmas-2016-12.

45 *See* Stern, *supra* note 32.

46 *See* David Tom, *The Data Management Debate: Local vs. Cloud Storage*, STORAGECRAFT RECOVERY ZONE, http://www.storagecraft.com/blog/the-data-management-debate-local-vs-cloud-storage/ [https://perma.cc/SP89-HGUX] (last visited Feb. 16, 2018).

privately held in local storage, given that the data is self-contained and not accessible to others, a user is limited by storage space and by the computing capabilities of the user's own device.[47] By contrast, "[t]he cloud is a collection of interconnected computers and servers publicly accessible via the Internet."[48] Rather than storing information directly on their own devices, users store data on remote servers hosted by cloud computing providers.[49] The contents of the cloud are altered and influenced both by users, who upload and store data, and internet service providers, who provide the necessary internet platforms.[50]

The National Institute of Standards & Technology ("NIST") defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[51] This integrated system allows users to share information with others and provides higher capacity and ease of access than users would typically realize on their own devices.[52]

The NIST classifies service providers into three categories, based on the capabilities the cloud provides to its users: (1) Software-as-a-Service ("SaaS"), (2) Platform-as-a-Service ("PaaS"), and (3) Infrastructure-as-a-Service ("IaaS").[53] SaaS clouds "provide[] software to users" but do not allow users to "manage or control the actual physical computer networks belonging to the provider."[54] PaaS allows the user to deploy consumer-made products on the cloud.[55] In other words, it allows users to have some

---

47 *See* Juan Carlos Torres, *Cloud Versus Local Storage: A Tug-of-War for Your Data*, ANDROID COMMUNITY (Apr. 17, 2014), https://androidcommunity.com/cloud-versus-local-storage-a-tug-of-war-for-your-data-20140417/.

48 Raquel, *supra* note 20, at 471.

49 *See* Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 621 (2011).

50 *See* Shahid Khan, *"Apps.Gov": Assessing Privacy in the Cloud Computing Era*, 11 N.C. J.L. & TECH. ONLINE 259, 265 (2010).

51 PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011).

52 *See* Raquel, *supra* note 20, at 472, 474.

53 *See* Khan, *supra* note 50, at 265–66.

54 *Id*. at 265. This includes software such as "word processing, spreadsheet, and presentation programs" as well as "entertainment hubs (video and music) and video conferencing systems." Hien Timothy M. Nguyen, Note, *Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing*, 86 NOTRE DAME L. REV. 2189, 2201 (2011) (footnotes omitted).

55 *See* Nguyen, *supra* note 54, at 2201.

"limited control" over the software,[56] so that "aspiring developers can quickly create and manage applications"[57] rather than just use them. IaaS provides only fundamental storage and network capabilities.[58] Overall, cloud computing allows consumers to perform functions that they would normally have to run entirely on local computers, to sidestep the need to purchase expensive infrastructure for additional storage, and to access data remotely "anytime, anywhere."[59] Though this convenience has many benefits, the storing of data on remote servers also raises questions about the level of privacy protection to which users are entitled.[60] Given the nature of cloud storage, a user who creates data may no longer hold and protect that data—rather, the data is maintained by the cloud provider.[61] The nature of this relationship raises a wide array of privacy questions involving when companies and other individuals can access a user's data, but this Note focuses on the question of when the government may be able to access that data. The Fourth Amendment is the guiding authority on government access to individual property, but applying historical interpretations of the Fourth Amendment to advancing technology such as cloud computing has created new problems.[62]

II. CURRENT REGULATORY REGIME

There is currently a dual system of constitutional protection of individual property in the physical world through the Fourth Amendment and statutory protection of individual property in the digital world through the ECPA. This Part presents the parallel schemes, with particular focus on the characteristics of protected information that courts and Congress have considered compelling.

A. Constitutional Protection: The Fourth Amendment

An individual's constitutional right to privacy stems from the protections provided by the Fourth Amendment. The Fourth Amendment to the United States Constitution reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,

---

56 *See* Khan, *supra* note 50, at 266.

57 Nguyen, *supra* note 54, at 2201.

58 *See id*. ("An example might be Netflix, an established online video rental service, moving its existing Internet technology to the cloud via Amazon Web Services."); Raquel, *supra* note 20, at 473.

59 *See* Kattan, *supra* note 49, at 622–23.

60 *See* Raquel, *supra* note 20, at 474–75.

61 *See* Kattan, *supra* note 49, at 621.

62 *See infra* Part III.

> shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[63]

It protects the rights of individuals with respect to "searches and seizures conducted by government agents."[64] Those protections have historically focused on physical intrusions by the government, specifically intrusions on persons and property.[65] A search under the Fourth Amendment is "a governmental intrusion onto private property for the purpose of obtaining information or a governmental violation of a person's legitimate expectation of privacy."[66] The Fourth Amendment explicitly provides a "reasonableness standard" to limit the nature of governmental searches and seizures, and over the years, the Supreme Court has provided further guidance on the boundaries of this standard.[67]

1. From Boyd *to* Riley*: Modern Fourth Amendment Jurisprudence*

Historically, Fourth Amendment jurisprudence has been characterized by strong correlations to real property law.[68] "[I]n most (though not all) cases, an expectation of privacy [is] 'reasonable' only when it is backed by a right to exclude borrowed from real property law."[69] In *Boyd v. United States*,[70] considered the first Supreme Court decision on the Fourth Amendment,[71] the Court provided Fourth Amendment protection to "all invasions on the part of the government and its employ[ee]s of the sanctity of a man's home and the privacies of life."[72]

With the decision in *Katz v. United States*,[73] the Supreme Court

---

63 U.S. CONST. amend. IV.

64 *Investigations and Police Practices*, 45 GEO. L.J. ANN. REV. CRIM. PROC. 3, 3 (2016).

65 *See id.* at 5–6, 12–15; Raquel, *supra* note 20, at 475 ("The Fourth Amendment, applicable to federal, state, and local investigators, serves as the primary regulator of law enforcement conduct in the course of physical-world criminal investigations." (footnote omitted)).

66 *Investigations and Police Practices*, *supra* note 64, at 5–6 (footnote omitted).

67 *See* Raquel, *supra* note 20, at 475–76.

68 *See* Kerr, *supra* note 18, at 809–10 (describing the connection between the Fourth Amendment and real property law).

69 *Id.*

70 116 U.S. 616 (1886).

71 *See* Paul Breer, Comment, *When the Television Listens: Fourth Amendment Protection Is Not Keeping Up with New Technology*, 85 UMKC L. REV. 255, 257–58 (2016).

72 *Boyd*, 116 U.S. at 630; *see also* Breer, *supra* note 71, at 257–58 (discussing *Boyd*'s initial impact).

73 389 U.S. 347 (1967).

slightly diverged from the purely physically based explanation of Fourth Amendment protection to a deeper understanding of when individuals may have a "reasonable expectation of privacy."[74] *Katz* concerned evidence collected during government surveillance of telephone calls placed by the defendant from a public telephone booth.[75] The defendant argued that the telephone booth was a "constitutionally protected area" and that the surveillance was a violation of the Fourth Amendment.[76] The Court agreed and held that "the Fourth Amendment protects people, not places."[77] The Supreme Court went so far as to say "[o]ne who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[78] Rather than absolute protection of an individual's home based on the physical area, the Supreme Court shifted the doctrine to apply to the individuals themselves.[79] This is not to say that geographical notions of Fourth Amendment protection no longer play any role.[80] Nevertheless, the Court in *Katz* pulled partly away from using a purely physically driven analysis.[81]

The theory of applying privacy consideration to individuals rather than property was explained in Justice Harlan's concurrence,[82] where he introduced the now-controlling "reasonable expectation of privacy" test.[83] Following *Katz*, the existence of a reasonable "expectation of privacy" is

---

[74] *See* Kerr, *supra* note 18, at 815–16. The approach does not, however, entirely abandon a property-based approach, but rather elaborates on the privacy interest itself that is protected. *See id*. Professor Kerr notes that the Court was still informed by property law when protecting *Katz*'s *momentary* property rights in a physical space. *See id*. at 823.

[75] *See Katz*, 389 U.S. at 348.

[76] *Id*. at 348–49.

[77] *Id*. at 351.

[78] *Id*. at 352.

[79] *See* Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1187 (1995).

[80] *See* Kerr, *supra* note 18, at 815–27 (arguing that *Katz* did not entirely wipe out property-based considerations, but rather that the case promotes an approach one step below the strict common law view of property).

[81] Justice Marshall recounted the Court's divergence from property-based evaluation in his dissent from *Oliver v. United States*, 466 U.S. 170 (1984), when he said:

> In *Katz v. United States*, we expressly rejected a proffered locational theory of the coverage of the [Fourth] Amendment, holding that it "protects people, not places." Since that time we have consistently adhered to the view that the applicability of the provision depends solely upon "whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."

Id. at 187–88 (Marshall, J., dissenting) (citations omitted).

[82] *See Katz*, 389 U.S. at 360–62 (Harlan, J., concurring).

[83] *See id*.; Kerr, *supra* note 18, at 820.

determined by a two-part test: (1) The individual "must have a subjective expectation of privacy in a place or thing" and (2) society must "recognize that expectation as objectively reasonable."[84] In other words, the individual has to demonstrate that, not only did he have an expectation of privacy under the circumstances, but also that the expectation was reasonable and that others would have the same expectation.[85]

Overall, this protection is considered at its strongest within one's home—"[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[86] But more generally, "[t]he uses to which a place is put are highly relevant to the assessment of a privacy interest asserted therein."[87] If the activities that the government is intruding on "are of a kind in which people should be able to engage without fear of intrusion by private persons or government officials," then the Fourth Amendment protects the privacy of those activities.[88]

In *Katz*, the Supreme Court emphasized that the Fourth Amendment protects *people*, not *places*.[89] An individual may be entitled to Fourth Amendment protection of "what he seeks to preserve as private, even in an area accessible to the public . . . ."[90] Thus, the protection that the Fourth Amendment affords does not depend necessarily on the form of the information sought, but rather on the relationship that an individual creates with the information and his surroundings that may give rise to an expectation of privacy.[91] With this principle in mind, the Supreme Court later faced the need to reevaluate Fourth Amendment jurisprudence in light of the rapidly shifting technological landscape. Determining a privacy relationship between an individual and his or her possessions from the physical context was difficult enough at the time of *Katz*, but technological advancement in the form of infrared technology widened the universe of information that the government could obtain from outside the physical confines of one's home.[92] This next hurdle was addressed by the Court in

---

84 *Investigations and Police Practices*, *supra* note 64, at 6–8.

85 *See* Kattan, *supra* note 49, at 624.

86 Silverman v. United States, 365 U.S. 505, 511 (1961).

87 Oliver v. United States, 466 U.S. 170, 191 (1984) (Marshall, J., dissenting).

88 *Id*. (citing *Katz*, 389 U.S. at 352–53).

89 *See Katz*, 389 U.S. at 351; s*ee also* Sergent, *supra* note 79, at 1187.

90 *Katz*, 389 U.S. at 351–52.

91 *See* Kerr, *supra* note 18, at 822 ("The 'critical' fact was the relationship that Katz had established when he occupied the phone booth, shut the door behind him, and 'pa[id] the toll that permit[ted] him to place a call.'" (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

92 *See* Kyllo v. United States, 533 U.S. 27, 32–33 (2001).

Kyllo v. United States.[93]

In *Kyllo*, the government used a thermal imaging device to survey the defendant's home to gather evidence on the possibility that the defendant was growing marijuana in the house.[94] In an opinion penned by Justice Scalia, the Court found that the intrusion constituted an impermissible warrantless search.[95] The Court held that a warrantless search conducted with the thermal imaging technology violated the Fourth Amendment because it produced "details of the home that would previously have been unknowable without physical intrusion . . . ."[96] The Court placed particular emphasis on the aspects of the thermal imaging technology that allowed law enforcement to collect more information than they otherwise would have been able to just by observing the exterior of the house, such as where people were located behind the walls.[97] In applying the *Katz* "reasonable expectation of privacy" test to the facts of *Kyllo*, the Court explained that the home, by its nature, is entitled to a reasonable expectation of privacy:[98]

> [I]n the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area" constitutes a search . . . .[99]

Despite the divergence from the purely physical line of analysis, the opinion in *Kyllo* retained strong Fourth Amendment protection over what

---

93 *See id*.

94 *See id*. at 29–30.

95 *See id*. at 40.

96 *Id*.

97 *See id*. at 35–36 (refusing to allow governmental intrusion through technology "that could discern all human activity in the home"); *id*. at 38 (noting that thermal imaging technology could reveal the presence of a resident in her bathroom).

98 *See id*. at 34.

99 *Id*. (citation omitted). The Court qualified this statement as applying to information collected by technology "at least where (as here) the technology in question is not in general public use." *Id*. Although this language was important at the time, the Court's recent extension of the Fourth Amendment to cellular phones in *Riley v. California*, 134 S. Ct. 2473 (2014), indicates the Court's willingness to apply such protection to technology that is in public use. *See id*. at 2490, 2494–95.

the Court called the "sanctity of the home."[100] The Court went so far as to delineate protection of even seemingly nonintimate details such as the location of a rug that would be discovered if law enforcement "barely crack[ed] open the front door."[101] The Court explained that "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[102] The Court's holding, most importantly, was not contingent on the *level* of intimacy of the information collected by technology, but rather on the fact that "*all* details" within an individual's home are considered "intimate" for purposes of the Fourth Amendment.[103] Thus, law enforcement's warrantless use of its newly found ability to collect any details of the home constituted a violation of the Fourth Amendment, regardless of the "intimacy" of those details.[104] The Court concluded with an explicit protection of the home: "We have said that the Fourth Amendment draws 'a firm line at the entrance to the house.' That line, we think, must be not only firm but also bright—*which requires clear specification of those methods of surveillance that require a warrant*."[105]

In *Riley v. California*,[106] the Supreme Court addressed the question of whether a warrantless search of cell phone data incident to arrest was permissible under the Fourth Amendment.[107] The Court unanimously held that a warrant was required because "[a] search of the information on a cell phone bears little resemblance to the type of brief physical search" held to be appropriate in searches incident to arrest.[108] Comparing a person's privacy interest in the typical "objects that might be kept on an arrestee's person"[109] with that in the data stored in a modern cell phone, Chief Justice Roberts noted that "the possible intrusion on privacy is not physically

---

100 *Kyllo*, 533 U.S. at 37.

101 *Id.*

102 *Id.*

103 *See id.* at 37–38.

104 *See id.* at 38–39, 40.

105 *Id.* at 40 (emphasis added) (citation omitted) (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

106 134 S. Ct. 2473 (2014).

107 *See id.* at 2482, 2484. While the discussion in *Riley* focuses on searches of an individual's person incident to arrest, and is therefore a brief departure from this Note's focus on searches of the home, the Court's analysis in *Riley* is relevant in establishing the pervasive regulatory scheme of Fourth Amendment jurisprudence as a whole.

108 *Id.* at 2485. The *Riley* Court compared the search at issue with the search in *United States v. Robinson*, 414 U.S. 218 (1973), where the Court upheld the warrantless search incident to arrest of Robinson's coat pocket, inside of which officers found and examined a crumpled cigarette packet containing heroin capsules. *See Riley*, 134 S. Ct. at 2483–84 (citing *Robinson*, 414 U.S. at 220, 223, 236).

109 *Riley*, 134 S. Ct. at 2489.

limited in the same way when it comes to cell phones,"[110] which may contain sufficient data to reveal the "sum of an individual's private life."[111] An individual would not carry on his person every picture he has taken in the last three years in hard copy, nor would he carry a call log of everyone he has contacted in the last week, but that precise information is available on a modern cell phone.[112] Thus, it is not the nature of the information in and of itself, but rather the sheer volume and added detail of viewing the information in the aggregate that compelled the Court to extend Fourth Amendment protection to and require a warrant for such searches.

2. Third-Party Doctrine

The above framework is controlling where an individual maintains information privately, but the constitutional protection of that information shifts when an individual discloses it to third parties.[113] The third-party doctrine, which provides that "[b]y disclosing to a third party, [an individual] gives up all of his Fourth Amendment rights in the information revealed,"[114] is a common barrier to invoking Fourth Amendment protection. Disclosure to a third party involves any situation where an individual "knowingly reveals private information to another person."[115] In revealing the information to a third party, the individual "assume[s] the risk that the other [party] will reveal the . . . information to the government."[116] If an individual has assumed the risk of disclosing his information to a third party, then that individual no longer has an "expectation of privacy" in that information.[117] The Supreme Court has consistently applied the third-party doctrine to preclude protection from government intrusion.[118]

---

110 *Id*.

111 *Id*.

112 *See id*. The Chief Justice also noted that "a cell phone search would typically expose to the government far *more* [potentially incriminating records] than the most exhaustive search of a house." *Id*. at 2491.

113 *See* Raquel, *supra* note 20, at 477.

114 Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

115 *See* Raquel, *supra* note 20, at 477.

116 *Id*.

117 *See id*.

118 *See id*. at 477–78. First, in *Couch v. United States*, 409 U.S. 322 (1973), the Court held that an individual could not assert Fourth Amendment claims to prevent the government from obtaining tax-related records she provided her accountant. *See id*. at 335–36. Next, in *United States v. Miller*, 425 U.S. 435 (1976), the Court held that an individual does not have an expectation of privacy in his or her bank records because they constitute information that was revealed to a third party. *See id*. at 442–43. Importantly, the third-party doctrine applies even when the information "is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be

The third-party doctrine calls into question the extent of Fourth Amendment protection to which individuals are entitled in light of technological advances. In *City of Ontario v. Quon*,[119] the Court did not address the third-party doctrine when it considered whether Fourth Amendment protection applied to a government search of text messages sent by a police officer on his government-issued pager.[120] *Quon* alludes to the possibility that the Court may have recognized that the third-party doctrine is no longer sustainable given modern technologies,[121] but a more concrete answer is needed. Given that the growth of technology has led to a more sustained presence and dependence on electronic devices, clear guidance is needed to determine whether individuals relinquish *all* information they choose to place on or transmit through a device. Part III discusses the implications of this uncertainty with regard to modern digital assistants.

B. Statutory Protection: The Electronic Communications Privacy Act of 1986

In the midst of the evolution of Fourth Amendment jurisprudence, Congress was quick to recognize the potential inconsistencies in applying the developing law, particularly with respect to new advancements in technology.[122] Most pressing of these modern technologies was email.[123] This concern caused Congress to commission its Office of Technology Assessment ("OTA") to help determine how the Fourth Amendment should apply in these new contexts.[124] The OTA's report concluded that, despite recent guidance from the Supreme Court, the extent of privacy protection of email was "weak, ambiguous, or nonexistent."[125] The report outlined

---

betrayed." *Id.* at 443. Finally, in *Smith v. Maryland*, 442 U.S. 735 (1979), the Court held that an individual does not have an expectation of privacy in the telephone numbers he dials because an individual knows that the telephone company must route those numbers through its switching equipment in order for the call to be placed. *See id.* at 744–45.

119 560 U.S. 746 (2010).

120 *See* Strandburg, *supra* note 19, at 615–18.

121 The Court took a deliberate approach in light of the implications posed by emerging technology as well as the workplace setting. *See Quon*, 560 U.S. at 759 ("Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."); *cf.* Strandburg, *supra* note 19, at 618.

122 *See* Kattan, *supra* note 49, at 626–27 (citing OFFICE OF TECH. ASSESSMENT, U.S. CONG., OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 21 (1985)).

123 *See* Raquel, *supra* note 20, at 479–80.

124 *See* Kattan, *supra* note 49, at 627.

125 OFFICE OF TECH. ASSESSMENT, *supra* note 122, at 45; *see also id.* at 50–51 (discussing the third-party privacy implications of email).

various policy options that Congress could adopt to provide firmer guidance.[126] In response, Congress enacted the ECPA, designed to address the gap in Fourth Amendment protection caused by the third-party doctrine.[127]

The ECPA comprises "the Wiretap Act, the Pen Register statute, and the Stored Communications Act [("SCA")]."[128] The ECPA is designed to apply to "electronic communication[s]," which it defines as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic or photooptical system."[129] Both the Wiretap Act[130] and the Pen Register Statute[131] regulate government access to real-time communications, while the SCA regulates prior, or "stored," communications.[132] The three statutes together "create a set of privacy protections . . . roughly analogous to the privacy protections that the Fourth Amendment offers in the physical world."[133] The remainder of this Note focuses on the implications of the ECPA as it applies to stored communications under the SCA.

In promulgating the SCA, Congress provided that "'[f]or the person or business whose records are involved, the privacy or proprietary interest in that information should not change' solely because the information is maintained and stored by a service provider as opposed to one's person or one's business premises."[134] Thus, Congress maintained an individual's reasonable expectation of privacy by statute—even when communications were stored with service providers—despite the Fourth Amendment's third-party doctrine.[135] Nevertheless, given that the application of the SCA is constrained to storage of "communications," and that the SCA can no longer be applied coherently to information collected by new devices with vast capabilities, the SCA's protections are now wholly inadequate in the

---

126 *See id*. at 4–5, 51–52.

127 *See* Raquel, *supra* note 20, at 479.

128 Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 815 (2003).

129 18 U.S.C. § 2510(12) (2012).

130 *Id*. §§ 2510–2522.

131 *Id*. §§ 3121–3127.

132 *Id*. §§ 2701–2712.

133 Kerr, *supra* note 128, at 816.

134 Raquel, *supra* note 20, at 481–82 (quoting S. REP. NO. 99-541, at 3 (1986)).

135 *See* Kerr, *supra* note 128, at 816; Raquel, *supra* note 20, at 482 ("By statutorily codifying end-users' privacy rights for their stored account information held by third party network service providers, the SCA addresses the inherent imbalances between the Fourth Amendment and the Internet's function.").

face of modern technological advances.[136]

A key component of the SCA is that it does not require a warrant for all government intrusions into stored data.[137] Government searches of stored communications are covered in the "compelled disclosure" section of the SCA,[138] which categorizes stored communications based on three dichotomies.[139] First, categorization of a stored communication depends on the function that a company is performing for the user in storing it.[140] Under the SCA, a provider can either be an Electronic Communications Service ("ECS"), providing users "the ability to send or receive wire or electronic communications," or a Remote Computing Service ("RCS"), providing online "storage or processing services" to users.[141] The second dichotomy is based on the length of time that the communication has been stored.[142] Under the SCA, communications stored with an ECS for less than 180 days and those stored for more than 180 days are separate categories.[143] Third, a communication is categorized based on whether the government is trying to obtain the contents, or noncontent information of the communication.[144] In an email, the body of the message would be considered the "contents," while the name and email address of the recipient would be considered "noncontents."[145] Hence, the SCA cannot be applied categorically to different types of data, but rather each communication must be categorized individually with respect to its content and the provider's role with respect to that communication.[146]

Depending on how the communication is categorized under the three dichotomies, the government can compel disclosure through three main mechanisms: search warrant, court order, or subpoena.[147] If a service provider is not acting as either an ECS or an RCS with respect to a particular communication, then the SCA does not apply at all.[148] If "content" information is held for 180 days or less by an ECS service

---

136 *See infra* Part III.

137 *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1218–19 (2004).

138 *See id*. at 1218 (citing 18 U.S.C § 2703 (2012)).

139 *See* Raquel, *supra* note 20, at 483.

140 *See* Kerr, *supra* note 137, at 1214.

141 *Id*.

142 *See* Raquel, *supra* note 20, at 483.

143 *See id*.

144 *See id*.

145 *See* Kerr, *supra* note 137, at 1228.

146 *See* Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 42 (2015).

147 *See* Raquel, *supra* note 20, at 482.

148 *See* Borchert, *supra* note 146, at 42.

provider, then the government must obtain a warrant to compel disclosure of the communication.[149] However, "[t]o compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose contents," the government has the option of obtaining a warrant, or the government can obtain the information through a subpoena or a court order as long as it gives prior notice to the user.[150] What makes these differing disclosure standards concerning is that modern technology has surpassed pure ECS/RCS[151] and content/noncontent distinctions.[152] Service providers no longer either store information or send it for a user, but rather can perform both functions seamlessly.[153] Similarly, modern communications may not always contain clear boundaries between "content" and "noncontent" information.[154] As a result, application of the SCA to modern stored information has become unclear and results in variable levels of protection from government intrusion.[155]

With the passage of the ECPA, Congress attempted to provide clear and easily applicable privacy protections for electronic communications. However, technology has now surpassed the bounds of this rigid division and has produced devices that store data that may logically fall under either the ECPA analysis, the more general Fourth Amendment analysis, or even under both, depending on how it is categorized. Part III discusses how the rigid division between constitutional and statutory protection is no longer workable given these novel and sophisticated technologies.

III. THE CURRENT REGULATORY REGIME IS INADEQUATE IN THE MODERN TECHNOLOGICAL LANDSCAPE

Although the promulgation of the SCA was an adequate response to the technological developments that existed in 1986, it has since become woefully outdated. First, the very definitions and categorizations that the SCA relies on have become outdated in recent years, making it difficult to determine when stored data does or does not fall under the purview of the SCA.[156] Second, the distinction between constitutional and statutory

149 *See* Kerr, *supra* note 137, at 1218.

150 *Id*. at 1218–19.

151 *See id*. at 1229–31.

152 *See id*. at 1227–28.

153 *See id*. at 1215–16 (highlighting the inherent difficulties in categorizing a modern service provider as providing either ECS or RCS services).

154 *See id*. at 1227–28 (discussing the difficulties in distinguishing between content and noncontent information).

155 *See* Kerr, *supra* note 16, at 387 ("Under this framework, the SCA offers less protection than a warrant to regulate government access to many remotely stored personal files.").

156 *See supra* text accompanying note 148.

protections depends on the assumption that technologies function independent of one another and can be categorically relegated to fit in one bucket or the other,[157] which is no longer true given the advent of the digital assistants.[158] A regulatory scheme that attempts to differentiate between these two categories becomes difficult to apply when considering such devices that fall in both categories, and even extend past those bounds altogether. This Part explains these difficulties and demonstrates why an amendment to the ECPA is necessary to resolve the resulting gaps in data protection.

A. Difficulties in Applying the Current Framework

The definitions and categorizations on which application of the SCA is based are no longer applicable to the modern digital assistant. Most critical to determining whether the SCA and broader ECPA apply is determining whether the information sought was an "electronic communication."[159] The ECPA definition of "electronic communication," which includes a "transfer of signs, signals, writing . . . by a wire"[160] was an attempt to describe email, as it was then understood.[161] For example, today, when a user says to a device, "Alexa, please email my sister that I will be over for lunch," it is unclear whether that statement in and of itself is a communication. Though the statement contains all of the elements of the email that will eventually reach the recipient, the statement itself was not a message to that recipient, but rather a command to the digital assistant. Further, modern interaction with the internet has surpassed pure communication between individuals, as technology has allowed humans to interact with a machine or online platform to accomplish such tasks—whereby individuals are no longer messaging each other directly, but rather interacting with computing clouds that send messages for them. Take, for instance, a search query entered into a search engine, such as Google. Mechanically, this seems to fit the definition of a transfer of signals or writing across wires, but at the same time, it is not a transfer of information from one individual to another, as is

---

157 *See supra* notes 135, 151–155 and accompanying text.

158 *See supra* Section I.A.

159 *See* Kerr, *supra* note 16, at 395–96 (noting the difference between the classically protected "communication," which covers contents for purposes of "connectivity or messaging," as opposed to the modern information that users release onto the internet in the form of search queries into search engines). "The second fundamental dichotomy in ECPA is the distinction between providers of electronic communication service and remote computing service. . . . The ECS protections covered email; the RCS protections covered contents of communications transmitted for remote storage and processing by services available to the public." *Id*. at 395.

160 18 U.S.C. § 2510(12) (2012).

161 *See* Kerr, *supra* note 16, at 383.

the email function on which Congress based the definition.[162] It is unclear whether Congress meant for the ECPA to encompass technologies, like Google search, that were not yet invented at the time of its passage.[163]

Additionally, the categorization dichotomies that the SCA relies on—(1) the ECS/RCS distinction; (2) the length of storage; and (3) the contents/noncontents distinction[164]—can no longer be applied rigidly to the vast array of technologies that have been developed. Take, for instance, the same Google search query. As Professor Kerr hypothesized, "ECPA likely offers no protection for access to stored search queries . . . because it does not fit the 1986 dichotomies codified by the statute."[165] Search engines do not send messages to others, and a search query is not entered into Google for the purpose of storage; thus, the service providers function as neither ECS nor RCS servers.[166] Similarly, a command given to a digital assistant is neither sent to another individual nor given for the purpose of being stored. These commands are also not given for the purpose of "processing" as defined under the statute, because the user does not intend them to be part of a large, remote processing program such as "number-crunching."[167] Rather, commands entered into a search engine and those spoken to a digital assistant are given for the purpose of executing a query, a function that is not expressly covered under the ECPA.[168] Likewise, 180 days is no longer a significant time period for storage, because these devices can store information indefinitely.[169]

Finally, the contents/noncontents dichotomy is also no longer workable as applied to the digital assistant technology. Under the earlier example of commanding an Amazon Echo or Google Home to email one's sister to plan a lunch, the "contents" and "noncontents" of an email are combined within one command. The command discloses both who the recipient is and what the content of the email is meant to communicate. It is

---

162 *See id*. at 395–98 (describing the ambiguous situation presented by modern search queries).

163 Google was launched in 1998, twelve years after the ECPA was enacted. *See* Alyson Shontell, *Here's What Google Looked Like the First Day It Launched in 1998*, BUS. INSIDER (Sept. 27, 2013, 1:39 PM), http://www.businessinsider.com/heres-what-google-looked-like-the-first-day-it-launched-in-1998-2013-9.

164 *See supra* notes 138–145 and accompanying text.

165 Kerr, *supra* note 16, at 396.

166 *See id*.

167 *See id*.

168 *See id*. at 396–97 ("Although the issue is difficult and not free from doubt, it appears likely that the most private of today's communications receive no statutory protection from ECPA." (footnote omitted)).

169 The Google Home will maintain its log until a user deletes it. *See supra* text accompanying note 38.

unclear whether this command would be considered "content," in the sense that it discloses the message that the recipient will read, or "noncontent," because it is not the actual email, but rather a command to the digital assistant. Digital assistant technology has rendered the distinction ambiguous, making it uncertain whether the ECPA would apply to this situation. Thus, the definitions and distinctions that Congress drafted to apply to the technologies existing in 1986 no longer seem logical when applied to modern developments.

B. Difficulties with Multifunctional Devices

In addition to the mechanical difficulties of applying only the SCA to modern technology, the constitutional and statutory frameworks are no longer concurrently workable when applied to the modern digital assistant. Specifically, the modern digital assistant combines the capabilities of an online communication service, to which the SCA would apply;[170] an online data processor, to which the third-party doctrine would apply;[171] and a device collecting information about an individual's home, to which strong Fourth Amendment protections would apply.[172] Each of these types of data is currently regulated by separate frameworks.

1. Communication Service

The communication component of digital assistants would likely be covered under the SCA. Email is the classic example of SCA-protected information.[173] As discussed above, modern digital assistants are capable of sending and receiving email if they are connected to an email-enabled server.[174] Because both the digital assistant processer (Amazon or Google) and the associated email server would be enabling the sending of messages and thus be providing ECS service, this communication would likely be protected by the SCA[175] and thus be subject to one of the three vehicles by which the government can compel disclosure under the statute.[176] As explained above, the three dichotomies would determine whether the government would be required to obtain a warrant, and it is possible that this portion of a digital assistant's log would be subject to a lesser

---

170 *See supra* text accompanying note 141.

171 *Cf.* Smith v. Maryland, 442 U.S. 735, 744–45 (1979).

172 *See* Riley v. California, 134 S. Ct. 2473, 2490–91 (2014).

173 *See* Kerr, *supra* note 16, at 383.

174 *See supra* Section II.B.

175 This assumption simplifies the analysis of the difficulties in applying the ECS/RCS dichotomy. *See supra* text accompanying notes 164–168.

176 *See supra* text accompanying note 147.

requirement.[177]

2. Data Processor

The Amazon Echo and the Google Home are also capable of conducting search queries. As discussed above, the SCA is unlikely to apply to search queries.[178] If the statutory protection of the SCA does not apply, then this portion of the data log would only be entitled to constitutional protection under the Fourth Amendment.[179] By disclosing the command to a digital assistant for execution, a court would likely hold that an individual voluntarily disclosed the information to either Amazon or Google. This disclosure would destroy any expectation of privacy under the third-party doctrine and thereby eliminate any warrant requirement.[180]

3. Sanctity of the Home

Finally, given the capabilities of the digital assistants to control virtually every aspect of the modern home,[181] the digital assistants would also be collecting information of the nature discussed by the Supreme Court in *Kyllo*.[182] Commands given to the digital assistants can reveal what room of the home an individual is in at a given time, what items an individual intends to purchase on his next shopping trip, or what activities an individual engages in within the confines of his home.[183] Information of this sort was exactly the type of information that the Court expressly protected in *Kyllo* when it extended Fourth Amendment protection to *any* detail that occurs within the walls of an individual's home.[184]

Until now, implementing the distinctions in regulatory treatment pursuant to the Fourth Amendment and the SCA has been sustainable, as the devices yielding information protected by the Fourth Amendment, by only the SCA, or by neither have been distinct. However, modern digital assistants combine the capabilities of the various technologies and yield one record log containing the various categories of information.[185]

---

177 *See supra* notes 149, 151–155 and accompanying text.

178 *See supra* notes 159–162 and accompanying text.

179 *See supra* Section II.A.1.

180 *See supra* Section II.A.2 (describing the impact of the third-party doctrine on Fourth Amendment protection).

181 *See supra* text accompanying notes 40–42.

182 *See* Kyllo v. United States, 533 U.S. 27, 32–40 (2001); *see also supra* notes 98–103 and accompanying text.

183 *See supra* Section I.A.

184 *See Kyllo*, 533 U.S. at 37–38.

185 Professor Kerr identified this growing problem in a more general sense by recognizing that many internet functions are "multifunctional" and present difficulties in determining the appropriate privacy protections. *See* Kerr, *supra* note 16, at 397 ("The

Therefore, separating out the information that might fall under one scheme or another has become an almost insurmountable task if the government wants to obtain information that a digital assistant overhears. Even if this information could be categorized effectively, it is unlikely to be accomplished without an analysis of the log that would itself render any protection irrelevant in the first place. As a result, there is a risk that the government may be allowed to rely on the lowest thresholds provided in the SCA, e.g., a subpoena or a court order, to obtain the entire record even if some of the information might be entitled to protection by a warrant.

IV. SOLUTION: AMENDING THE ECPA

As laid out in Part III, the different levels of protection between judicially defined Fourth Amendment protection and that of the ECPA cannot be combined coherently to apply to technologies that span both schemes. To address this problem, this Part proposes widening the scope of the ECPA to encompass information that cannot be characterized clearly as "communications" but nevertheless should be afforded explicit protection consistent with congressional intent to exempt digital information from the third-party doctrine.

A. The Need for Statutory Amendment to the ECPA

At the time that Congress drafted the ECPA, it formed the Act's protections with the technology of the 1980s in mind.[186] Congress thus had little perception of future developments beyond its concept of the "innovative communications systems" that it intended to promote.[187] Likewise, the ECPA was passed with the intent of protecting "certain information stored electronically in the same manner as information stored locally,"[188] yet few could have predicted that such interactive and invasive devices as the Amazon Echo and Google Home would soon exist. Given the ideals and goals that have driven both constitutional and statutory privacy protections thus far, this Note proposes that the divergent constitutional and statutory paths that have developed should reconnect under one unified scheme given the technology that has developed and the

multifunctional nature of modern Internet services creates headaches for ECPA by raising complex and perhaps unanswerable questions about what the statute protects."). Digital assistant technology further exemplifies this difficulty not only by incorporating services that are simply excluded from the ECPA and should not be afforded protection, but also by incorporating services that may be technically excluded but for which lack of protection would be inconsistent with congressional intent or Supreme Court precedent.

186 *See supra* text accompanying notes 122–123.

187 *Cf.* Borchert et al., *supra* note 146, at 41.

188 *Id.*

intimate role it plays in the lives of its users.

The crux of the Supreme Court's opinion in *Kyllo* was that the government should not have warrantless access to "details of the home that would previously have been unknowable without physical intrusion."[189] Opposite of this ideal is the SCA, which provides variable protection for digital data depending on outdated categorizations.[190] But when the digital data is of such a nature that it fits with the Supreme Court's decisions protecting information from new technologies,[191] the SCA should provide for that enhanced coverage. In *Kyllo*, the government was able to gather data on the existence of objects within the defendant's home without actually entering the home, thus leading to the Supreme Court's holding that such an intrusion was unconstitutional.[192] Similarly, a time log of such an intimate nature as which room of the home someone is in at what time of day is information that would not normally be known to the government with the use of classic law enforcement practices. Allowing a continuation of the divergent paths would potentially allow the government to circumvent the high bar set by *Kyllo* and *Riley* and instead conduct a search of the same record—the data collected by the smart-home devices—by obtaining a court order or subpoena under the SCA, rather than a warrant. This potential backdoor eliminates the protection afforded by the Supreme Court and is no longer workable in today's landscape.

Further, the digital data collected by digital assistants is fundamentally more similar to the information at issue in *Kyllo* than it is to the information protected under the SCA because it is collected within an individual's home. The digital assistant is physically present in an individual's home and constantly collecting intimate information regarding one's activities behind closed doors. In contrast, the communicative information protected by the SCA may rise to varying levels of intimacy depending on whether it is classified as content or noncontent information,[193] a distinction that Congress explicitly afforded differing levels of protection.[194] In other words, Congress anticipated that the information covered by the SCA might not always be intimately tied to an individual's privacy. At the time of drafting, however, Congress could not have anticipated the intimacy with which digital assistants would be integrated into individuals' homes. Thus, the ECPA should be amended to

---

189 *Kyllo*, 533 U.S. at 40.

190 *See supra* Section III.A.

191 *See* Riley v. California, 134 S. Ct. 2473 (2014) (applying Fourth Amendment protections to cell phone data).

192 *See Kyllo*, 533 U.S. at 29–30, 40.

193 *See* Kerr, *supra* note 137, at 1228.

194 *See id*. at 1218–20.

protect information of this nature.

B. Proposed Amendment to the ECPA

To reconcile these inconsistencies, the scope of the ECPA should be broadened with a fourth statute to encompass noncommunicative intimate information collected by digital assistants. This statute should apply where a device collecting the information is intimately tied to the home, such as a digital assistant. In other words, the exact technology that collects the information is not the crucial point, but rather the *nature* of the information collected will trigger the application of this statute. The proposed language is as follows:

> **(a) Contents of record logs produced by home-based electronic devices.** A governmental entity may require the disclosure by a provider of cloud computing services of information collected by a physically home-based electronic device collecting data of such a nature that it would previously have been undiscoverable without physical intrusion only pursuant to a warrant issued under the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.
>
> > **(i) Exception.** A governmental entity need not obtain a warrant, but rather may proceed under a court order in situations where a court determines that the nature of an individual's disclosure of the information to the public has yielded all expectations of privacy in the information.

First, the title and body of the text constrain the application of the statute to those technologies that are physically home based, thereby excluding mobile devices such as cellular phones. The device must be a physical fixture in an individual's home to the extent that it is an appliance that consistently records an individual's statements whenever activated. In this way, the protection will stem from the information's link to the details of the home, not necessarily to the individual, as the Supreme Court envisioned in *Kyllo*.[195] Second, the statute explicitly identifies cloud computing in order to exclude devices such as desktop computers, which are physically home-based devices but that store data in a traditional local disk method that does not implicate the elaborate cloud computing framework described above.[196] Additionally, the explicit cloud computing

---

[195] *See supra* text accompanying notes 100–105.

[196] *See* Kerr, *supra* note 137, at 1215 ("While a home computer configured as a mail server could provide ECS in theory, the home computer of an end user is not protected by the SCA. This is consistent with the SCA's purpose: home computers are already protected

delineation specifically includes the categories of information that currently lose protection under the third-party doctrine.[197] Third, the statute incorporates the language used by the Supreme Court in *Kyllo*[198] to constrain application only to the sort of information that would not be discoverable without the aid of the digital assistants. This language is necessary to ensure that the "home-based" information that the Supreme Court found crucial in *Kyllo* continues to receive the utmost level of privacy. Fourth, the statute requires a warrant to obtain all information collected by covered devices in order to ensure that all private information is afforded a consistent level of protection. By requiring a warrant to access all such information, the statute would allow the government access to the information through a unified vehicle—a warrant—rather than through a subpoena or court order, which are the current vehicles for certain categories of information.[199] For example, in obtaining the record log of the Amazon Echo, the government would not need to go through the acrobatics of distinguishing which commands were communications and which were not, but would obtain all such data only through a warrant. Finally, the statute provides for an exception in situations where an individual has disclosed the contents of her digital assistant log, thereby destroying her expectation of privacy.[200] This exception codifies the third-party doctrine to apply to disclosed information that was previously collected by these devices. For instance, if a user publishes her Amazon Echo log on an online blog, warrant protection would no longer apply to that log.

In interpreting this statute, courts should keep in mind the reasoning in *Kyllo*—to provide a bright-line rule for consistency in application. The Supreme Court in *Kyllo* afforded Fourth Amendment protection to any minute detail that would not have been observable by law enforcement from the exterior of an individual's home absent thermal imaging technology.[201] This statute codifies that threshold; therefore, courts should apply this statute to protect that sort of information collected by digital assistants, such as where individuals are in their homes at any given time. Even more fundamentally, absent a digital assistant, law enforcement would not be able to listen to commands spoken within an individual's

---

by the Fourth Amendment, so statutory protections are not needed." (footnotes omitted)).

197 *See supra* Section II.A.2.

198 The proposed language "previously have been undiscoverable without physical intrusion" mirrors "previously have been unknowable without physical intrusion" as used by the Court in *Kyllo*. Kyllo v. United States, 533 U.S. 27, 40 (2001).

199 *See* Kerr, *supra* note 137, at 1222–23; *see also* Kerr, *supra* note 16, at 411–12 (proposing similar legislation).

200 *See* Raquel, *supra* note 20, at 477.

201 *Kyllo*, 533 U.S. at 37–40.

home; thus, this statute should apply to the entirety of a digital assistant's log without a need to analyze the nature of each separate command.

C. How This Solution Will Allow for Currently Unforeseen Development

The main problem with the current statutory structure is that it is unsustainable in the face of current, let alone future, technology.[202] Time has shown that given the exponential growth of technology, society is ill-equipped to predict what future protections may be required. When the ECPA was written, imagination had only stretched into the possibility that individuals could communicate with one another through technology.[203] Modern innovation has already surpassed this threshold. In aligning privacy protection with fundamental understandings of how society should protect information of such a nature as *details of the home*, this statutory amendment would allow for future unpredictable technological developments by constantly requiring the government to return to the question of what the information means to the individual, rather than the method by which it is collected or the nature of the device that collects it.

D. Why the Third-Party Doctrine Should Remain Intact

The proposed language would explicitly keep the door open to the continuing presence of the third-party doctrine. Though other scholars have approached the problems of privacy protection in the digital age by proposing abolition of the third-party doctrine,[204] this Note proposes that the continuation of the doctrine in some form is consistent with broader legal scholarship and important policy reasoning. The concept that confidentiality or privacy is abolished upon disclosure to a third party is a principle present throughout the legal landscape, including, for example, privileges in the evidentiary context.[205] In the case of data stored on the cloud, it is important to preserve these notions of third-party disclosure to encourage users to be mindful of the data they put on the internet. Though this amendment aims to afford some protection to such data, the legal community still retains an interest in reminding people that the internet is

---

202 *See supra* Part III (discussing the difficulty in applying the ECPA to evolving technologies).

203 *See supra* text accompanying notes 122–123.

204 *See, e.g.*, Natasha H. Duarte, Recent Development, *The Home Out of Context: The Post-*Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1142–44 (2015) (citing divergent scholarly opinions and noting that the Supreme Court might be prepared to limit the third-party doctrine in some circumstances).

205 *See* Kenneth S. Broun & Daniel J. Capra, *Getting Control of Waiver of Privilege in the Federal Courts: A Proposal for a Federal Rule of Evidence 502*, 58 S.C. L. REV. 211, 224–29 (2006) (explaining the scope of waiver of attorney-client privilege through disclosure).

forever and that any data they put on the internet, although protected, may still be searchable. A complete abolition of the third-party doctrine would erase any incentive for individuals to at least carefully consider their actions before engaging in the use of modern technology.

CONCLUSION

This Note's proposed amendment aims to address the ambiguity of applying an outdated regulatory scheme to rapidly evolving technology. Following the Supreme Court's ruling in *Kyllo*, information pertaining to details of an individual's home should be afforded the utmost privacy protection. Given the advent of digital assistants, those details are now stored on the internet, rendering the current regulatory framework inadequate. Congress should amend the ECPA to provide the necessary protection of this rapidly growing network of information.