Hey Alexa: Was it the Butter, in the Foyer, with the Candlestick?
Understanding Amazon's Echo and Whether the Government can Retrieve its Data

Seth Weintraub
American University Washington College of Law

Follow this and additional works at: https://digitalcommons.wcl.american.edu/aublr

Recommended Citation
Available at: https://digitalcommons.wcl.american.edu/aublr/vol7/iss1/4
HEY ALEXA: WAS IT THE BUTLER, IN THE FOYER, WITH THE CANDLESTICK?
UNDERSTANDING AMAZON’S ECHO
AND WHETHER THE GOVERNMENT
CAN RETRIEVE ITS DATA

SETH WEINTRAUB*

I. Introduction ......................................................................................................................156

II. The Laws Implicating Access to Electronic Data .............................................. 158
   A. The Fourth Amendment .................................................................................. 158
   B. The Third-Party Doctrine ............................................................................... 162
   C. The Electronic Communications Privacy Act and the Stored Communications Act .................................................................164
      1. ECS ........................................................................................................ 165
      2. RCS ...................................................................................................... 168

III. The Echo Under Fourth Amendment, Third-Party Doctrine, and
     ECPA/SCA Jurisprudence ........................................................................169
   A. Accessing Data on the Echo Using the Fourth Amendment
     and the Third-Party Doctrine ........................................................................169
   B. The SCA’s Applicability in the Echo Context ...........................................172
      1. Is the Echo an ECS? ............................................................................ 172
      2. Is the Echo an RCS? ............................................................................... 174

IV. Modifying Current Laws to Encompass Evolving Technology 175

V. Conclusion .....................................................................................................................177

* Managing Editor, American University Business Law Review, Volume 7; J.D. Candidate, American University Washington College of Law, 2018; B.A. Criminology & Criminal Justice, University of Maryland, 2015. I would like to express my utmost gratitude to the American University Business Law Review staff for its time and effort in helping me prepare my Comment for publication. Special thanks to my editors, Kiki McArthur, Hilary Rosenthal, and Nathan Roy, for their tireless effort working with me. Finally, I am eternally grateful for the constant support, love, and encouragement of my friends and family, especially my father, mother, and sister.
I. INTRODUCTION

“In my mind, as well as the minds of a lot of other privacy experts, the Echo has been a ticking constitutional time bomb, along with a lot of other features of smart homes and the internet of things.”¹ As of June 2016, more than 1.6 million homes use the Amazon Echo (“Echo”),² a device capable of providing extensive information at the user’s command.³ For instance, “Alexa,” the Echo’s personal voice assistant, updates users about the latest football scores, prepares daily agendas, and may even resolve murders.⁴ In November 2016, Bentonville, Arkansas, police officers discovered the dead body of Victor Collins.⁵ After conducting an investigation, the police ruled his death a homicide.⁶ In Collins’ home, police specifically uncovered a plethora of “smart” devices,⁷ including an Echo.⁸ Police seized the Echo and served Amazon with a warrant alleging that Amazon held records related to Collins’ murder.⁹ Although requesting this data seemingly imposes an uncomfortable burden on the Echo user’s right to privacy,¹⁰ little data is

---


² BI Intelligence, How Many Amazon Echo Smart Home Devices Have Been Installed?, BUS. INSIDER (June 7, 2016, 8:00 PM), http://www.businessinsider.com/how-many-amazon-echo-smart-home-devices-have-been-installed-2016-6.


⁵ See Wang, supra note 4.

⁶ Id.

⁷ Smart Device, TECHNOPEDIA (Nov. 12, 2017), https://www.techopedia.com/definition/31463/smart-device (defining a smart device as “[a]n electronic gadget that is able to connect, share and interact with its user and other smart devices”).

⁸ See Wang, supra note 4.

⁹ Id.

¹⁰ See Russell Brandom, How Much Can Police Find Out from a Murderer’s
stored on the actual device. Rather, most of the data is stored on the Internet and/or smart phones by way of the user’s Amazon account. Nonetheless, the recordings are time stamped, thereby providing the police or government officials insight into a person’s statements and/or general presence within a particular space.

The debate over data accessibility, namely what government agents should access and how they can access such data emerges when courts are forced to resolve conflicts between one’s right to privacy and society’s reliance on electronic communication. For instance, between 2015 and 2016, the Federal Bureau of Investigation (“FBI”) requested that Apple Inc. (“Apple”) provide an all-access key to investigate iPhone-stored data, including the data stored on the iPhone owned and operated by Syed Rizwan Farook and Tashfeen Malik, the married couple responsible for the San Bernardino shooting—Apple refused. Jeffrey Bezos, Amazon’s Chief Executive Officer (“CEO”), aligned with Apple, noting that consumer privacy is a highly important issue and that the conflict between privacy and national security is an “issue of our age.” “Privacy” is integral to the consumer-retailer relationship. Specifically, should consumers believe that their information is private, they are more inclined to purchase goods that advance said privacy. If, however, consumers believe that their information is

---

1. See id.; see also Mehau Kulyk, Alexa and Google Home Record What You Say. But What Happens to that Data?, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ (demonstrating how the Echo constantly “listens” for commands, then records and streams the clip of what the user says to their account on either the Internet or phone, storing data on the user’s Amazon account until he or she decides to delete it).

2. See Brandom, supra note 10.


4. See id.


freely accessible to third parties, including the government, they hesitate to purchase goods. 18

This Comment will begin by reviewing the jurisprudence surrounding the search and seizure of electronic data under the Fourth Amendment, the third-party doctrine, the Electronic Communications Privacy Act (“ECPA”), and the Stored Communications Act (“SCA”). This discussion requires an understanding of search and seizure law as applied to both people and intangible items, such as data on electronic storage units, and also how search and seizure law has evolved to envelope data stored on electronic mediums. Part III will analyze the case law surrounding electronically stored data and will apply said law to the Echo’s recording process. In doing so, this Comment will reveal the outdated nature of the SCA, and further expose government officials’ overreliance on the third-party doctrine. Part IV will additionally recommend that the SCA be appropriately modified and that the third-party doctrine be expanded to include a categorization requirement to best meet the consumers’ privacy needs and business’ desire to sell. Part V concludes by summarizing the necessary changes to current legal standards to ensure privacy while also upholding the appropriate legal standard.

II. THE LAWS IMPLICATING ACCESS TO ELECTRONIC DATA

A. The Fourth Amendment

Although the United States Supreme Court interprets the Fourth Amendment to protect people, not places, from unreasonable searches and seizures, 19 the language of the Fourth Amendment ostensibly contemplates only physical searches and seizures. 20 The Court’s Fourth Amendment jurisprudence is thus the starting point in any Fourth Amendment analysis, as it identifies what categories of information should be protected and how to guarantee enforcement of that protection. 21

18. See Elliot 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/ (“It is unreasonable to expect consumers to monitor their every word in front of their home electronics. It is also genuinely creepy.”).
20. See U.S. CONST. amend. IV (emphasis added) (“The right of the people to be secure in their persons, houses, papers, and effects.”).
21. See Alexander Scolnik, Note, Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment, 78 FORDHAM L. REV. 349, 351-52 (2009) (surmising that the Framers could neither anticipate technology, nor the concept of online communications, and how courts’ have tried to expand the Fourth Amendment to protect privacy rights in an increasingly technological world).
The intersection between the Fourth Amendment and technology first emerged in *Olmstead v. United States*.\(^{22}\) In this case, the Court determined that wiretapping did not constitute a search or seizure under the Fourth Amendment even when the government wire-tapped Olmstead’s phones.\(^{23}\) Approximately thirty years later, the Court overruled *Olmstead* in *Katz v. United States*.\(^{24}\) In *Katz*, the Government wire-tapped a public phone booth and introduced statements acquired therein as evidence against Katz.\(^{25}\) Rather than following *Olmstead*, the Court determined that even if there is no physical invasion on one’s privacy, the Fourth Amendment proscribes unlawful non-physical invasions of privacy committed by the government.\(^{26}\) In its analysis, the Court established a two-step test for Fourth Amendment cases.\(^{27}\) The test requires courts to evaluate whether the individual alleging harm maintained a reasonable or subjective expectation of privacy given the circumstances and whether society, as a whole, is prepared to recognize the individual’s expectation of privacy as reasonable.\(^{28}\) Additionally, the Court expanded the Fourth Amendment’s protections to the curtilage of a person’s home.\(^{29}\) Curtilage breaks down into three factors: (1) a connection with the home; (2) the proximity a court would regard as curtilage of the home (regardless of the home’s enclosure); and (3) use of the space for private or personal means.\(^{30}\) In one such case, police used drug-sniffing dogs to search

\(^{22}\) *Olmstead v. United States*, 277 U.S. 438, 455 (1928) (presiding over a case about agents wiretapping one’s private telephone conversation).

\(^{23}\) See generally id. at 466 (explaining that evidence obtained by virtue of wiretapping should not be protected because it was not a physical search or seizure as contemplated by the Fourth Amendment).

\(^{24}\) *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (noting that a person’s expectation of privacy is violated, even in a public phone booth, where the government wiretaps his personal conversation).

\(^{25}\) Id. at 348.

\(^{26}\) Id. at 360-61 (Harlan, J., concurring) (“[A]n enclosed telephone booth is an area where, like a home . . . and unlike a field . . . a person has a constitutionally protected reasonable expectation of privacy . . . [and] that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment.”).

\(^{27}\) Id. at 361 (Harlan, J., concurring).

\(^{28}\) Id. (noting that a person must first demonstrated an actual expectation of privacy and also that society recognizes said expectation as reasonable); see also Ann K. Wooster, *Expecation of Privacy in and Discovery of Social Networking Web Site Postings and Communications*, 88 A.L.R.6th 319 (highlighting the case law governing expectations of privacy with respect to different types of Internet communications).

\(^{29}\) See Florida v. Jardines, 569 U.S. 1, 6 (2013) (citing Oliver v. United States, 466 U.S. 170, 180 (1984)) (defining “curtilage” as “the area "immediately surrounding and associated with the home"” and acknowledging that the Fourth Amendment protects the curtilage).

\(^{30}\) See id.
the curtilage of a suspected dealer’s home.\textsuperscript{31} The suspected dealer claimed that the search of the area around his home, while not inside the home, still warranted Fourth Amendment protection because it was unreasonable—the Court agreed.\textsuperscript{32} Additionally, the concept of “curtilage” can be expanded to include what Andrew Guthrie Ferguson calls “digital curtilage” or the area in which data and stored communications exist.\textsuperscript{33} The concept of digital curtilage enhances consumers’ reasonable expectations of privacy with respect to the varied technology in their homes.\textsuperscript{34} Given the Court’s interpretation of the Fourth Amendment, constitutionally-protected individuals can withdraw to their home, wherein they maintain a heightened expectation of privacy from unreasonable government intrusion.\textsuperscript{35} Without this protection, police could stand directly outside a suspected criminal’s window, lurking about for evidence.\textsuperscript{36}

The scope of the Fourth Amendment, or more precisely the Court’s interpretation of its protections, expanded as technology has evolved. Specifically, in \textit{Kyllo v. United States},\textsuperscript{37} police aimed a thermal-imaging device at the petitioner’s home.\textsuperscript{38} The Court found that this constituted an unreasonable search because the thermal-imaging device explores details of a home in a manner not unlike a physical intrusion, and that the device itself is one not typically available to the public.\textsuperscript{39} \textit{Kyllo} clearly demonstrates the

\textsuperscript{31} Id. at 4.
\textsuperscript{32} Id. at 4, 8 (‘‘As it is undisputed that the detectives had all four of their feet and all four of their companion’s firmly planted on the constitutionally protected extension of Jardines’ home, the only questions is whether he had given his leave . . . for them to do so. He had not.’’).
\textsuperscript{33} Andrew Guthrie Ferguson, \textit{The Internet of Things and the Fourth Amendment of Effects}, 104 CAL. L. REV. 805, 809 (2016) (proposing the theory of “digital curtilage” to protect electronic data that “(1) [is] closely associated with the effect; (2) [has] been marked out and claimed as secure from others; and (3) [is] used to promote personal autonomy, family, self-expression, and association”).
\textsuperscript{34} See id. at 866 (describing the need for heightened expectations of privacy with respect to evolving technologies).
\textsuperscript{35} See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (equating a public phonebooth to one’s home, where the expectation of privacy reaches its apogee); see also Silverman v. United States, 365 U.S. 505, 511 (1961) (noting “the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion”).
\textsuperscript{36} See \textit{Jardines}, 560 U.S. at 6 (explaining that without some protection around one’s home, the right to withdraw would be rendered useless as police could simply stand outside one’s window).
\textsuperscript{37} \textit{Kyllo} v. United States, 533 U.S. 29 (2001).
\textsuperscript{38} See id. at 29 (noting that the case involved a thermal-imaging device utilized to detect the amount of heat within the defendant’s home).
\textsuperscript{39} Id. at 34 (“[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical
Court’s willingness to expand Fourth Amendment protections in conjunction with evolving technology. 40

Notwithstanding the Court’s willingness to expand Fourth Amendment protections to ever-evolving technologies, the question remains: will the Court protect the user’s right to privacy when the Government introduces evidence acquired from stored data communications devices, such as the Echo? By way of background, the Echo is a home audio speaker that responds to the name “Alexa”, the Echo’s personal voice assistant. 41 The Echo constantly listens for sound, connects to the user’s Wi-Fi and home network, accesses cloud services, and uses Bluetooth streaming technology. 42 As indicated earlier, most of the Echo’s data is stored on the user’s Amazon account. 43 For police to access the Echo’s data transmitted to a user’s Amazon account, the data itself must be intercepted from the wireless network in which the Echo operates. 44 The U.S. District Court for the Northern District of California attempted to resolve this issue in In re Google Inc. Street View Electronic Communications Litigation. 45 Here, the plaintiffs filed a lawsuit upon learning that Google Street View 46 accessed their wireless communications through Wi-Fi networks and obtained information from their respective computers allegedly in violation of the 1968 Wiretap Act (“Wiretap Act”). 47 The court attempted to determine whether the Wiretap Act, at the time it was enacted, encompassed the

40. See generally id. (concluding that the Fourth Amendment protects against warrantless invasions of a person’s home utilizing advanced technology not readily available to the public).


42. Id. (explaining that the Echo functions upon hearing the user say, “Alexa”, at which point the Echo awakes and listens for the user’s specific commands).

43. See Brandom, supra note 10.


45. See generally id. (finding that the plaintiffs pled sufficient facts to claim a violation of the Wiretap Act where the defendant (Google) created, approved of, and implemented a highly-technical design software into Google Street View vehicles to intercept plaintiffs’ “data packets”).

46. See id. at 1070-71 (describing Google Street View as a feature within Google Maps offering various positions and views using photos taken from “a fleet of specially adapted vehicles commonly known as Google Street View vehicles”).

47. Id. at 1070-72 (noting that Google intentionally implemented a data collection system on Google Street View vehicles).
The court concluded that when Congress enacted the Wiretap Act, it did not contemplate the concept of Wi-Fi. Specifically, the court determined that the Wiretap Act’s definition of “radio communications” should not be expanded to include Wi-Fi. As such, the court explored the legislative intent behind radio communications, concluding that “interpreting ‘radio communication’ broadly would contravene congressional intent to provide protection for technology like cellular phones, which use radio waves to transmit communications, but are architected in such a way as to be private.”

B. The Third-Party Doctrine

The third-party doctrine permits the government to collect “any information given to a third party by a criminal suspect, without running afoul of the Fourth Amendment.” In establishing the third-party doctrine, the Court acknowledged that an individual’s expectation of privacy is diminished when private information is shared with a third party. In United States v. Jones, however, the Court recognized that the third-party doctrine could not be maintained in its current form; yet the Court offered no alternative. In particular, Justice Sonya Sotomayor said “[i]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”

48. See id. at 1082 (explaining that although the plaintiffs’ Wi-Fi network was organized such that the public could access it and transmit electronic communications, the network was set up to protect those transmissions absent the use of advanced technology (i.e., the technology used by Google), and thus, the Wiretap Act applied).

49. See id. at 1076 (stating that “[t]he drafting of [ECPA] provisions predated the spread of wireless internet technologies”).

50. See id. (“[T]he usage of ‘radio communication’ throughout the [ECPA] does not lend itself to a broad interpretation of the term.”).

51. Id. at 1081.


53. See Scolnik, supra note 21, at 354 (explaining that the Supreme Court believes people have a reduced expectation of privacy when items/information is voluntarily exposed to “public view”).


55. See id. at 417 (Sotomayor, J., concurring) (noting that the third-party doctrine is “ill suited [sic] to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks”); see also id. at 413 (finding that the FBI, which placed a Global Positioning System (“GPS”) on Jones’s car to track his movements, violated the Fourth Amendment).

56. See id. at 417.
The scope of the third-party doctrine was refined in *Riley v. California*.\(^{57}\) In this case, the Court refused to extend the Fourth Amendment’s search incident to arrest exception\(^{58}\) to a cellphone.\(^{59}\) Although the Government argued that cellphones are “materially indistinguishable” from certain items, such as wallets or purses, the comparison did not persuade the Court.\(^{60}\) In fact, the Court explicitly stated that the cellphone, albeit a modern device, “implicate[s] privacy concerns far beyond those implicated by the search of . . . a wallet, or a purse.”\(^{61}\) With respect to the third-party doctrine, the Government and California simultaneously argued that information on cell phones can be destroyed by remote wiping conducted by third parties, a process in which “a phone, connected to a wireless network, receives a signal that erases stored data.”\(^{62}\) While the Court acknowledged the possibility of third parties destroying data remotely, it nonetheless determined that said third parties should be of little concern because they are not present at the scene of the arrest.\(^{63}\) As such, *Riley* represents the Court’s willingness to protect electronic communications vulnerable to third-party destruction.

Additionally, in *United States v. Warshak*,\(^{64}\) government agents compelled an Internet Service Provider (“ISP”)\(^{65}\) to share a defendant’s incriminating emails without first obtaining a warrant pursuant to the Fourth Amendment.\(^{66}\) Instead, the agents relied on the SCA, which permits government agents to obtain emails otherwise protected by the Fourth Amendment.\(^{67}\) The U.S. Court of Appeals for the Sixth Circuit acknowledged that the SCA provides

\(^{57}\) Riley v. California, 134 S. Ct. 2473 (2014).

\(^{58}\) Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest*, 19 YALE L. & POL’Y REV. 381 (2001) (affording police the power to search anyone subsequent to that individual’s arrest without first obtaining a search warrant from a neutral magistrate).

\(^{59}\) Riley, 134 S. Ct. 2494-95 (“[T]he search incident to arrest exception does not apply to cell phones . . . .”).

\(^{60}\) See id. at 2488-89 (differentiating between physical items on the arrestee’s person and digital data, noting that cell phones “differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee’s person”).

\(^{61}\) Id. at 2489.

\(^{62}\) Id. at 2486.

\(^{63}\) Id.

\(^{64}\) United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).


\(^{66}\) See Warshak, 631 F.3d at 266.

\(^{67}\) See generally id. (finding that the government violated the defendant’s Fourth Amendment rights, but relied in good-faith on the SCA).
three options for the government to acquire communications stored with a service provider: (1) obtain a warrant; (2) utilize administrative subpoenas; or (3) acquire court orders under section 2703(d).\textsuperscript{68} Regardless, the court concluded that the similarities between email and traditional forms of communication justifies expanding the scope of the Fourth Amendment to protect email correspondence containing “confidential communications.”\textsuperscript{69} Although the third-party doctrine is certainly implicated in the context of remotely stored electronic communications, the court determined that “the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.”\textsuperscript{70} Additionally, the court held that the Fourth Amendment’s exclusionary rule did not apply because the government relied on the good faith exception\textsuperscript{71} listed in sections 2703(b) and 2703(d) of the SCA.\textsuperscript{72}

C. The Electronic Communications Privacy Act and the Stored Communications Act

The Wiretap Act enabled Government officials to intercept electronic communications in several circumstances, including those made during (1) the ordinary course of business for common carriers, or those (2) interceptions assisting permitted law enforcement investigations.\textsuperscript{73} The Wiretap Act also allowed persons acting as government agents under the law to intercept communications with one party’s consent.\textsuperscript{74} As computer systems became more affordable, more individuals had access to electronic forms of communication, such as email.\textsuperscript{75} Concerned that existing laws did

\textsuperscript{68.} See id. at 283.
\textsuperscript{69.} Id. at 285-86, 288.
\textsuperscript{70.} Id. at 286. But see United States v. Miller, 425 U.S. 435, 443 (1976) (noting that the “Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities”).
\textsuperscript{71.} See generally United States v. Leon, 468 U.S. 897 (1984) (finding that evidence should not be barred from admission when the evidence seized was done so reasonably based on a good faith reliance on a search warrant that was subsequently found defective).
\textsuperscript{72.} See Warshak, 631 F.3d at 292 (noting that the government violated the Fourth Amendment, but properly relied upon the SCA’s good faith exception).
\textsuperscript{73.} See Amy McCann Roller, Note, From Ship-to-Shore Telegraphs to Wi-Fi Packets: Using Section 705(a) to Protect Wireless Communications, 68 FED. COMMS. L.J. 525, 534 (2016) (explaining that the Wiretap Act permits interceptions in certain instances).
\textsuperscript{74.} Id. (“[The Wiretap Act] allowed persons acting under the color of law to intercept communications with one party’s consent.”).
\textsuperscript{75.} Melissa Medina, Note, The Stored Communications Act: An Old Statute for Modern Times, 63 AM. U. L. REV. 267, 268-69 (2013) (stating that manufacturers, including IBM and Apple, released more cost-effective computers, thereby initiating the
not adequately protect the privacy of a citizen’s electronic communication, Congress enacted the ECPA in 1986.\(^76\) Title II of the ECPA encompasses the SCA,\(^77\) which protects electronic communications.\(^78\) The ECPA and SCA, further govern and define two types of service providers, respectively: electronic communication services ("ECS")\(^79\) and remote computing services ("RCS").\(^80\) The application of the SCA to a particular case depends on whether electronic communication can be classified as an ECS or RCS, specifically in the context of liability.\(^81\)

1. ECS

The term “ECS” refers to a service providing its users the ability to receive and transmit electronic communications.\(^82\) The SCA proscribes ECS providers from divulging information contained within its electronic storage.\(^83\) Courts have struggled to adopt a uniform definition for ECS

\(^{76}\) Id. at 269.

\(^{77}\) 18 U.S.C. §§ 2701-2712 (2012); see also Medina, supra note 75, at 269 (noting that Congress passed the SCA as part of the ECPA).

\(^{78}\) See Medina, supra note 75, at 269 (explaining that the SCA protects electronic communications by providing a private cause of action against anyone who acquires stored communications, and regulating when service providers can disclose user communication).

\(^{79}\) 18 U.S.C. § 2510(14) (defining ECS as “any wire, radio, electromagnetic, photooptical [sic] or photoelectronic [sic] facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications”).

\(^{80}\) 18 U.S.C. § 2711(2) (defining RCS as “the provision to the public of computer storage or processing services by means of an electronic communications system”).

\(^{81}\) See Medina, supra note 75, at 278-79 (“[T]he scope of the SCA depends on whether an electronic communication is held by an ECS or RCS provider and whether the communication is in electronic storage.”).


\(^{83}\) See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (quoting 18 U.S.C. § 2702(a)(2)) (noting that ECS providers may not “knowingly divulge[r] to any person or entity the contents of a communication while in electronic storage by that service”); see also 18 U.S.C. § 2510(17)(A)-(B) (defining electronic storage as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication”).
providers. In Konop v. Hawaiian Airlines, Inc., the U.S. Court of Appeals for the Ninth Circuit concluded that a secure website was an ECS because when users viewed the website and initiated electronic communication, said communication was sent from the website owner to the users. Additionally, the court determined that once the user has access to the website through which the data is transmitted, the website qualifies as an ECS.

Further, in Kaufman v. Nest Seekers, LLC, the plaintiff brought a lawsuit under Title II of the ECPA (i.e., the SCA), alleging unlawful access to stored communications on a website that purportedly acted as an ECS. The U.S. District Court for the Southern District of New York concluded that the website at issue, which acted like an electronic bulletin board, facilitated electronic communication as an ECS provider. Although the court determined that it was “premature” to find the website, at the pleadings stage, to be an ECS provider, it nonetheless concluded that a website permitting users to engage “in private electronic communications with third-parties” may act as an ECS provider.

Conversely, in United States v. Steiger, the U.S. Court of Appeals for the Eleventh Circuit concluded that the SCA did not apply to a home computer because it did not operate like an ECS provider. As the court indicated, the “SCA . . . generally prohibits an entity providing an [ECS] to the public from disclosing information absent an applicable exception,” but in this case, Steiger’s home computer did not provide an ECS for which the SCA could apply.

84. Compare Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002) (qualifying Konop’s secure website bulletins as an ECS), with In re JetBlue, 379 F. Supp. 2d at 308-09 (explaining that JetBlue’s website, alone, could not make the company an ECS provider).
85. Konop, 302 F.3d at 879 (explaining that the website at-issue is an ECS provider).
86. See id. at 874-75 (explaining that the Inter enables users to exchange electronic communication worldwide, and that websites, like Konop’s, receives, transmits, and stores electronic communications akin to an ECS provider).
87. Id. at 875-76 (defining and concluding Konop’s website as an ECS).
89. Id.
90. Id. (quoting United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990)) (“A[n] [electronic bulletin board] system is a computer program that simulates an actual bulletin board by allowing computer users who access a particular computer to post messages, read existing messages, and delete messages.”).
91. See id. at *5 (“An electronic bulletin board fits within the definition of an electronic communication service provider.”).
92. See id. at *6 (acknowledging that an on-line business, like the one at-issue, that allows users to receive and transmit electronic communications acts as an ECS provider).
93. 318 F.3d 1039 (11th Cir. 2003).
94. Id. at 1049 (noting that there is “no evidence to suggest that Steiger’s computer maintained any ‘electronic communication service’”).
Additionally, in *In re JetBlue Airways Corp. Privacy Litigation*, the U.S. District Court for the Eastern District of New York determined that JetBlue Airways Corporation ("JetBlue"), which operated a website enabling it to communicate with customers in the ordinary course of business, did not automatically transform into an ECS provider by virtue of operating that type of website. Even though JetBlue controlled the website in question, the court found that JetBlue was never the provider of electronic communication services as contemplated by the SCA because it did not allow information to be transmitted over the Internet. As such, the information disclosed did not violate the law. Likewise, in *Crowley v. CyberSource Corp.*, the U.S. District Court for the Northern District of California determined that Amazon’s website did not qualify as an ECS. Crowley sued Amazon after it divulged Crowley’s personal information to CyberSource Corporation to verify Crowley’s credit card information. In assessing Amazon’s liability for improper disclosure under section 2702(a)(1), the court determined that Amazon must have “provide[d] either electronic communication service or remote computing service.” Although Amazon received emails from Crowley, the court held that it was not an ECS. The court further noted that to hold otherwise would make the ECS definition over inclusive, unnecessarily equating users with providers—a distinction explicitly

95. *Id.* (explaining that the SCA does not apply in this case, but that the SCA may apply “to the extent the source accessed and retrieved any information stored with Steiger’s Internet service provider”).


97. *See id.* (“Rather, JetBlue is more appropriately characterized as a provider of air travel services and a consumer of electronic communication services.”).

98. *See id.* at 306-07 (noting that JetBlue’s Passenger Reservation System was merely a website operated by JetBlue and did not convert JetBlue into an ECS provider); *see also* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263 (N.D. Cal. 2001) (finding the website at-issue to be user of, rather than a provider of ECS).

99. 166 F. Supp. 2d at 1263.

100. *See id.* at 1270 (noting that Amazon, which receives emails from users, is not an ECS provider as contemplated by the SCA).

101. *See id.* at 1265 (alleging that Amazon shared identifiable information without consent to a third party after a user purchased goods through Amazon’s website).

102. 18 U.S.C. § 2702(a)(1) (2012) (“[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.”).

103. *Crowley*, 166 F. Supp. 2d at 1270.

104. *Id.* (noting that to hold Amazon as an ECS provider would unnecessarily equate a “user with a provider” in conflict with the SCA).
referenced in section 2701(c) of the ECPA.  

2. RCS

To qualify as an RCS, the provider’s electronic storage must be available to the public through an electronic communications system, meaning “any wire, radio, electromagnetic, photooptical [sic] or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” Loosely put, an RCS is maintained through another computer, which stores and processes data subject to future retrieval. The term “electronic communication” encompasses many forms of communication, including signs, signals, images, and data by wire, radio, electromagnetic, photoelectric or photo-optical system affecting interstate or foreign commerce; however, Wi-Fi does not appear in section 2510(12) of the ECPA. Unlike ECS providers, the SCA prevents RCS providers from disclosing any communication carried or maintained by the provider for the sole purpose of storage or computer processing services. Additionally, should the provider’s services remain available only to a select few, not the public at-large, courts are reluctant to find liability based on the provider’s existence as an RCS. In fact, the U.S. District Court for the Northern District of Illinois determined that an internal email system available only to select staffers, or those with a special relationship to the provider, constituted a system restricted to the community at-large and, thus, the provider was not

105. Id.; see 18 U.S.C. § 2701(c) (defining providers and users in separate subsections).
108. See 18 U.S.C. § 2510(12); see also United States v. Herring, 993 F.2d 784, 787 (11th Cir. 1993) (suggesting that “electronic communication” is a broad, all-encompassing term).
109. See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973 (C.D. Cal. 2010) (noting that RCS providers cannot disclose information it receives, maintains, or stores, if the RCS provider is not permitted to access “the contents of [the] communications for purposes of providing . . . services other than storage or computer processing”).
110. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (indicating that gaining access to an internal email system does not fall under the statutory definition of “to the public” because the individual who gained access was not “any member of the community at large”).
III. THE ECHO UNDER FOURTH AMENDMENT, THIRD-PARTY DOCTRINE, AND ECPA/SCA JURISPRUDENCE

A. Accessing Data on the Echo Using the Fourth Amendment and the Third-Party Doctrine

Government agents seeking to intercept or access data stored on the Echo without a warrant do so in clear violation of the Fourth Amendment.\(^\text{111}\) As such, agents conducting warrantless searches with respect to data must demonstrate that one of the Fourth Amendment’s exceptions, such as the third-party doctrine, apply.\(^\text{112}\) Compelling disclosure of data stored on the Echo, specifically electronic communications reasonably transmitted in confidence, violates that user’s subjective expectation of privacy under the Fourth Amendment.\(^\text{113}\) Applying the Court’s analysis in \textit{Katz} to governmental searches involving the Echo, it becomes evident that in conducting searches, even those touching only electronic communications, agents must satisfy the two-step test announced in \textit{Katz}.

To that end, the Echo user maintains an expectation of privacy because his relationship with the device itself, including each Echo-specific command, presumably occurs in the confines of his home, wherein he maintains a heightened expectation of privacy.\(^\text{116}\) While the user’s interaction with the Echo unlikely involves

\(^{111}\) \textit{Id.} at 1043 (concluding that the plaintiff acted as the defendant’s employee rather than a member of the community at-large, and further, the mere fact that the email server could communicate with the public did not transform the defendant into an ECS provider).

\(^{112}\) See \textit{Katz v. United States}, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (explaining that warrantless governmental searches in constitutionally protected areas are “presumptively unreasonable”).

\(^{113}\) See \textit{id.} at 362 (noting that warrants are generally required, but agents can nevertheless conduct warrantless searches when one of the Fourth Amendment’s exceptions apply).

\(^{114}\) See Medina, \textit{supra} note 75, at 294-95 (noting that Fourth Amendment privacy protections focus on necessity and expectation, and that electronic communications should be similarly analyzed).

\(^{115}\) \textit{Katz}, 389 U.S. at 361 (Harlan, J., concurring) (clarifying the Court’s two-prong inquiry for searches, noting that the first prong focuses on the individual’s subjective expectation of privacy, and that the second prong addresses whether society accepts the individual’s expectation as reasonable).

\(^{116}\) See \textit{id.} at 360 (implying that the home is a place, albeit the most important place, where individuals maintain the most constitutionally protected expectation of privacy); see also Ferguson, \textit{supra} note 33, at 837 (“The Fourth Amendment protects houses and effects . . . [and] [i]f police entered the house without a warrant, you would have a physical invasion of the home.”).
the consistent dissemination of highly-confidential or revealing information, the user, who is more likely to confide intimate details of his life in his own home, might nevertheless disclose confidential information to the Echo that is protected by the Fourth Amendment.\textsuperscript{117} Furthermore, the user’s subjective expectation of privacy when interacting with the Echo is likely one that society deems reasonable.\textsuperscript{118} Because technology pervades society and most people have access to smart devices, the total diminution of privacy with respect to technological advancements is simply unfathomable, albeit from society’s perspective.\textsuperscript{119}

Additionally, the Court has proscribed governmental searches within the curtilage of a person’s home.\textsuperscript{120} Indeed, the Court’s understanding of one’s curtilage is ambiguous at best; however, the Court makes fairly clear that the concept of curtilage is familiar enough that it is comprehensible from daily experiences.\textsuperscript{121} If curtilage entails “the area ‘immediately surrounding and associated with the home’” and remains “part of the home itself for Fourth Amendment purposes,”\textsuperscript{122} it seems likely that the user’s expectation of privacy with respect to each command aimed at the Echo in his home falls under the protection of the Fourth Amendment.\textsuperscript{123} Listening for or attempting to access conversations carried out in the user’s home, even conversations converted to data via the Echo, violates the Fourth Amendment, as well as one’s right to privacy, and therefore, constitutes an

\begin{itemize}
  \item[117.] See Ferguson, supra note 33, at 862 (noting that the Fourth Amendment “embraces both a preservation of personal autonomy and a protection against arbitrary or unreasonable intrusions. Whether conceived of as the right to be left alone, or a space for intimate activities, or other protections of personal autonomy”).
  \item[118.] See Katz, 389 U.S. at 361-62 (Harlan, J., concurring) (“the expectation [must] be one that society is prepared to recognize as ‘reasonable.’”).
  \item[119.] See Ferguson, supra note 33, at 807-08 (explaining that the advent of emerging technologies “poses a problem for a Fourth Amendment protecting ‘persons, houses, papers, and effects’ from unreasonable searches and seizures”); see also Bill Wasik Gear, In The Programmable World, All Our Objects Will Act as One, WIRED (May 14, 2013, 6:30 AM), https://www.wired.com/2013/05/internet-of-things-2/ (predicting that “smart,” interconnected objects will expand in number, reaching at minimum fifty billion objects by 2020).
  \item[120.] See Florida v. Jardines, 569 U.S. 1, 6 (2013) (noting that the right to withdraw in one’s home would be of little value if agents could stand within the curtilage of that home to obtain evidence).
  \item[121.] See id. at 4 (emphasis added) (internal quotations omitted) (quoting Cal. v. Ciraolo, 476 U.S. 207, 213 (1986)) (explaining that the curtilage is an “area around the home intimately linked to the home, both physically and psychologically”).
  \item[122.] Jardines, 569 U.S. at 6.
  \item[123.] See Ferguson, supra note 33, at 837-38 (acknowledging that the interception of non-tangible data poses Fourth Amendment problems, but “[u]nder a reasonable expectation of privacy test . . . this type of high-acquisition of information” would violate the individual’s reasonable expectation of privacy).
\end{itemize}
unreasonable search and seizure.\textsuperscript{124}

In addition to the Court’s definition of traditional curtilage, the notion of digital curtilage is particularly important in today’s world.\textsuperscript{125} Digital curtilage requires various factors, including “first, a connection with the home; second, a claimed and marked space to exclude others . . . and third, the use of this space which relates to personal or family activities.”\textsuperscript{126} Digital curtilage—a concept that recognizes the advanced nature of today’s technology—embraces the fact that confidential communication can occur both in one’s home and beyond its walls.\textsuperscript{127} By expanding the protectability of the user’s electronic communications beyond his home to include areas where digital information is accessible, digital curtilage enhances the user’s ability to enjoy technology with the same expectation of privacy as in his home.\textsuperscript{128} Additionally, the notion of digital curtilage provides sufficient guidance for those seeking the data itself (i.e., government agents), particularly in instances where third parties are compelled to disclose seemingly protected information.\textsuperscript{129} Digital curtilage arguably prevents government agents from over relying on exceptions, such as the SCA’s good-faith exception, in accessing electronic communications, and instead, compels agents to abide by boundaries, albeit loose ones, established to protect information otherwise beyond the traditional curtilage of one’s home.\textsuperscript{130}

Furthermore, as indicated above, in \textit{Kyllo} and \textit{In re Google}, when government agents conduct a search utilizing technology generally unavailable to the public, courts are more inclined to believe that the search

\begin{itemize}
  \item \textsuperscript{124} See \textit{Kyllo} v. United States, 533 U.S. 27, 40 (2001) (noting that where advanced technology not in general public use is used to conduct a search, the search itself is unreasonable without a warrant); see also \textit{In re Google Inc. St. View Elec. Commc’ns Litig.}, 794 F. Supp. 2d 1067, 1082 (N.D. Cal. 2011) (implying that advanced technologies, such as wireless sniffers, pose a threat to one’s privacy where information intended to be confidential is involuntarily shared with a third party).
  \item \textsuperscript{125} See generally Ferguson, supra note 33, at 809 (proposing the theory of digital curtilage, a concept born out of the Court’s notion of “physical curtilage,” to resolve privacy issues introduced by emerging technologies).
  \item \textsuperscript{126} Id. at 866
  \item \textsuperscript{127} Id. (“Traditional curtilage recognizes that while many of our most private activities take place inside the home, they can also occur beyond the four walls of the actual homestead . . . [which] also deserves a heightened level of protection.”).
  \item \textsuperscript{128} See id. (noting that digital curtilage should come with a heightened expectation of privacy akin to physical curtilage).
  \item \textsuperscript{129} See id. (noting that digital curtilage provides a useful framework for situations involving technology that implicate the Fourth Amendment).
  \item \textsuperscript{130} See In re Google Inc. v. St. View Elec. Commc’ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011) (preventing access to data transmitted over wireless networks).
\end{itemize}
itself violates the Fourth Amendment.\textsuperscript{131} Regarding the Echo, intercepting its data transmitted over Wi-Fi requires advanced technology, specifically highly-technical data collection systems, such as the packet analyzer or wireless sniffer employed in In re Google.\textsuperscript{132} As the court in In re Google acknowledged, the wireless sniffer “secretly captures data packets . . . [and these] data packets are not readable by the general public absent . . . sophisticated decoding and processing technology.”\textsuperscript{133} Given the Court’s disdain for governmental searches reliant upon advanced technology not in general public use,\textsuperscript{134} searches involving highly-technical data collection systems, including those capable of intercepting data transmitted via the Echo, violate the Fourth Amendment as unreasonable searches akin to physical intrusions.\textsuperscript{135} As such, the Government must possess a warrant to reasonably intercept, decode, and analyze data transmissions via the Wi-Fi network in which the Echo device exists.\textsuperscript{136}

B. The SCA’s Applicability in the Echo Context

1. Is the Echo an ECS?

To access data electronically stored on the user’s Amazon account, government agents must adhere to the SCA, which requires (1) a warrant, (2) an administrative subpoena, or (3) a court order pursuant to section 2703(d) of the SCA.\textsuperscript{137} However, as indicated above, the government can only compel service providers identified as either an ECS or RCS to disclose

---

\textsuperscript{131} See id. (describing Google’s data collection system utilized to collect, decode, and analyze data transmitted through Wi-Fi); see also Kyllo v. United States, 533 U.S. 27, 33-34 (2001) (noting that a thermal-imaging device was used in violation of the Fourth Amendment to acquire evidence).

\textsuperscript{132} See generally In re Google, 794 F. Supp. 2d at 1070-71 (using advanced technology to access a consumer’s Wi-Fi network).

\textsuperscript{133} Id. at 1071.

\textsuperscript{134} See Kyllo, 533 U.S. at 39 (holding that where the Government uses a device not in general public use, it has conducted an unreasonable search in violation of the Fourth Amendment).

\textsuperscript{135} See id. (concluding that a thermal-imaging device, one not in general public use, enabled agents to acquire information that would have been unavailable without a physical invasion of privacy, and therefore, the search was unreasonable under the Fourth Amendment).

\textsuperscript{136} See id. (indicating that a search reliant on thermal-imaging technology was unreasonable without a warrant).

\textsuperscript{137} See 18 U.S.C. § 2703 (2012) (noting that compelled disclosure of electronic information is permitted in certain situations); see also United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010) (noting that the Government can access emails without a warrant, an administrative subpoena, or an SCA-approved court order).
electronic communications under exceptions included in the SCA. To classify the Echo as an ECS, the device must enable its user to transmit or receive wire or electronic communications.

The Echo, or more precisely Amazon, is not an ECS for several reasons. First, the Echo uses, rather than provides, electronic communications with Amazon. Like In re JetBlue, where the court determined that a website with mere Internet access and the ability to transmit and receive information to and from its users did not automatically make the provider an ECS, Amazon similarly uses its online platform to advertise goods without acting as an Internet provider, and, as the court in Crowley recognized, the mere fact that Amazon transmits and receives data to and from its users does not make it an ECS provider under the SCA. Additionally, Amazon, like the company Andersen Consulting LLP, is a company that purchases Internet services, rather than providing Internet services, rendering it nothing more than an ECS-user.

Because Amazon is likely not an ECS, government agents cannot access information stored on the Echo pursuant to the SCA. Nonetheless, like the secure website in Konop, Amazon also includes a username and password component for individuals holding Amazon accounts. As the court in Konop acknowledged, the “nature of the Internet . . . is such that if a user enters the appropriate information . . . it is nearly impossible to verify the

---

138. See Warshak, 631 F.3d at 282 (internal quotations omitted) (“The Stored Communications Act . . . permits a governmental entity to compel a service provider to disclose the contents of [electronic] communications in certain circumstances.”); see also United States v. Steiger, 318 F.3d at 1039, 1049 (11th Cir. 2003) (noting that electronic communications are protected so long as they remain in electronic storage).

139. See 18 U.S.C. § 2510(15); see also Steiger, 318 F.3d at 1049 (noting that the SCA covers information stored with the following ECS providers: 1) a phone company; 2) ISPs; or 3) electronic bulletin boards).

140. See In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005) (noting that JetBlue does not provide internet access, “just as the use of a telephone to accept telephone reservations does not transform the company into a provider of telephone service”).

141. See Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (“[The court] rejects the argument that because Amazon receives e-mails from [plaintiff] it provides an electronic communication service. Additionally, such a definition would equate a user with a provider . . . .”).

142. See In re JetBlue Airways Corp., 379 F. Supp. 2d at 308 (citing Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998)) (distinguishing between companies that purchase Internet services and companies that provide Internet services).

143. See AMAZON, https://www.amazon.com/ (last visited Oct. 18, 2017); see also Konop v. Hawaiian Airlines, Inc., 302 F.3d. 868, 875 (9th Cir. 2002) (“While most websites are public, many, such as Konop’s, are restricted. For instance, some websites are password-protected . . . .”).
true identity of that user.” Notwithstanding this concern, data transmitted by the Echo qualifies as electronic communication under section 2510(12) of the Wiretap Act. Therefore, as indicated by the court in Konop, any interception, or “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device,” acquired during transmission violates the Wiretap Act. As such, should a court conclude that Amazon is an ECS, government actors seeking to intercept data transmitted as electronic communication through the Echo cannot do so during transmission without running afoul of the Wiretap Act.

2. Is the Echo an RCS?

The Echo is also likely not an RCS provider simply because it relates to Amazon’s website. Again, to qualify as an RCS provider, the data transmitted by the Echo must be available to the public and not the product of a special relationship, such as an employer-employee relationship. Amazon’s website qualifies as publically available because it is available to any member of the general population who complies with requisite procedures.

Nevertheless, Amazon’s website, with respect to Echo users, is the product of a special relationship between the Echo, or Amazon generally, and its user. Therefore, Amazon is not an RCS in the Echo context. Using Andersen Consulting LLP as an example, where the court found that mere

144. Konop, 302 F.3d at 875.
145. See 18 U.S.C. § 2510(12) (2012) (noting that electronic communication entails sounds, data, or intelligence of any nature transmitted by a “wire, radio, electromagnetic, photoelectronic or photooptical [sic] system”); see also Konop, 302 F.3d at 876 (noting that Konop’s website fits the definition of electronic communication because information is transferred from the website to the user through one the mediums specified in the Wiretap Act).
146. 18 U.S.C. § 2510(4) (emphasis added).
147. See Konop, 302 F.3d at 876, 878 (noting that Congress intended the definition of “Intercept” to be narrow).
148. See id. at 878 (noting that website interception violates the Wiretap Act if it occurs during transmission, not while it is in electronic storage). But see Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (noting that ECS providers, under the SCA, may not “knowingly divul[g]e to any person or entity the contents of a communication while in electronic storage by that service”).
149. See generally 18 U.S.C. §§ 2510(16); 2711(2); Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (noting that simply providing an employee access to the company’s email system does not equate to providing email services to the public).
access to an employer’s internal email system (i.e., its database) did not constitute the employer as an RCS provider, the relationship between Amazon and Echo users is better understood. A special relationship between a site and its users, as noted by the court in that case, undermines publicly available services, even if said site is available to the public at-large. With respect to Amazon and Echo users, the mere fact that Amazon’s site offers public services, namely in the form of ordering goods, the Echo, likely operated within the confines of one’s home, is privately maintained. Specifically, when the user commands his Echo, such commands are likely made pursuant to a reasonable expectation of privacy, and as such, a court would likely find that the commands (i.e., speech) are unavailable to the public and the product of a special relationship between the user and Amazon by way of the Echo, undermining the argument that Amazon is an RCS provider.

IV. MODIFYING CURRENT LAWS TO ENCOMPASS EVOLVING TECHNOLOGY

To keep up with technological advancements, it is essential to modify the Fourth Amendment, the third-party doctrine, and the SCA. Such modifications are necessary to ensure that Amazon is not forced to divulge confidential information transmitted through the Echo. With respect to the third party doctrine, should government agents request data transmitted by the Echo and/or stored on the user’s Amazon account, courts should remove third parties from the SCA’s purview entirely. Although Warshak held that government agents can acquire information under the SCA despite violating the Fourth Amendment, the SCA’s good faith exception does not comport with Fourth Amendment jurisprudence. In holding that the SCA’s good faith exception might trump the Fourth Amendment, namely a person’s reasonable expectation of privacy, the court in Warshak

152. See id. at 1042.
153. See also id. at 1041.
154. See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (“[A] man’s home is, for most purposes, a place where he expects privacy . . . .”).
155. See Andersen Consulting LLP, 991 F. Supp. at 1043 (finding special relationships cannot constitute an RCS).
156. See Tsukayama, supra note 15.
157. See United States v. Warshak, 631 F.3d 266, 292 (6th Cir. 2010) (noting that the contents of one’s emails, stored with an ISP, are accessible pursuant to the SCA even if obtained in violation of the Fourth Amendment).
158. See id.; see also Ferguson, supra note 33, at 870 (noting that a better definition of digital curtilage could refine what government intrusion means should Fourth Amendment jurisprudence creep into technological issues).
unnecessarily complicated an already complex problem.\textsuperscript{159}

Additionally, to protect confidential electronic communications from third parties, the third-party doctrine must be modified.\textsuperscript{160} Because roughly eighty percent of Americans rely on the Internet,\textsuperscript{161} it is simply unreasonable to maintain the third-party doctrine in its current form.\textsuperscript{162} To counteract this problem, courts should implement a categorization requirement for the third-party doctrine itself.\textsuperscript{163} In doing so, courts should implement a reasonableness test before admitting information under the third-party doctrine, wherein government agents must demonstrate that there was at least a reasonable suspicion that information could be obtained from the third party in a reasonable manner.\textsuperscript{164}

Additionally, Congress should amend the SCA to include data stored via a voice command center, such as the Echo. Absent such a revision, the SCA, as it currently reads, does not adequately protect a vast majority of emerging technologies, including voice command centers, from governmental intrusion.\textsuperscript{165} Additionally, Congress should expand the SCA to include more than merely ECS and RCS providers to include protections for electronic communication involuntarily shared with third parties.\textsuperscript{166} Further, Congress should articulate what constitutes online communication and whether the SCA applies to online communication through the current RCS or ECS definitions—if at all.\textsuperscript{167} There is currently no consistent or universal understanding of what technological or online communicating means,

\textsuperscript{159} See Smith, supra note 1 (noting that the Echo is a “ticking constitutional time bomb”). \textsuperscript{160} See United States v. Jones, 565 U.S. 400, 417-20 (2012). \textsuperscript{161} Matthew Tokson, Automation and the Fourth Amendment, 96 IOWA L. REV. 581, 588 (2011). \textsuperscript{162} See id. at 581 (noting that the controversial third-party doctrine has become “increasingly problematic in an age where a large proportion of personal communications and transactions are carried out over the Internet”). \textsuperscript{163} See Issacharoff & Wirshba, supra note 52, at 1003 (identifying certain categories of information that are particularly ripe for exemption from the third-party doctrine). \textsuperscript{164} See id. at 1034 (depicting a test where first, an officer can point to reasonable suspicion that the search of the third party will turn up relevant information and, second, the search should be reasonable). \textsuperscript{165} See William Jeremy Robinson, Note, Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 GEO. L.J. 1195, 1235 (2010) (“The SCA already provides some quantum of privacy in online communications and content, but as society embraces new technologies, including cloud computing, the balance of the [SCA] struck more than two decades ago may no longer be appropriate.”). \textsuperscript{166} See 18 U.S.C. §§ 2701-12 (2012); see also Medina, supra note 75, at 277. \textsuperscript{167} See In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 308 (E.D.N.Y. 2005).
particularly with respect to the Echo. To that end, without additional clarification from either Congress or the judiciary, albeit both, it is unclear whether the Echo would be defined as an ECS, RCS, or nothing at all.

V. CONCLUSION

The advent of smart technology has created several social and legal dilemmas. Given the popularity of smart devices, smartphones, computers, and voice command centers alike, the majority of people using them presumably do not understand the sacrifice to privacy incurred by way of smart technology. Additionally, the law has repeatedly failed to keep up with the rapid pace of this evolving technology. As such, it is essential, as argued above, to expand the SCA to encompass emerging technologies, such as voice command centers (i.e., the Echo), to modernize Fourth Amendment jurisprudence surrounding the third-party doctrine, and to expand the term “curtilage” to include digital forms of communication in the Fourth Amendment context. Doing so ensures that the privacy expectations of each consumer are upheld in an ever-shrinking world.

168. See O’Boyle, supra note 4 (noting that when the Echo permits a person to order items, it effectively creates an in-the-air billboard: if the user knows what he or she is buying, the advertisement stands).

169. Compare Konop v. Hawaiian Airlines, Inc., 302 F.3d. 868 (9th Cir. 2002) (confirming an employee’s private, personal website as an ECS), and Becker v. Toca, No. 07-7202, 2008 WL 4443050, at *1, *4 (E.D. La. Sept. 26, 2008) (permitting classification of an online business or retailer as an ECS provider if the business operates a website offering customers the ability to send and receive electronic communications with third parties), with Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1263 (N.D. Cal. 2001), and United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (concluding that a home computer, merely connected to the Internet, is not an ECS).