Washington Law Review

Volume 93 | Number 1

3-1-2018

Alexa, What Should We Do about Privacy? Protecting Privacy for Users of Voice-Activated Devices

Anne Pfeifle

ALEXA, WHAT SHOULD WE DO ABOUT PRIVACY? PROTECTING PRIVACY FOR USERS OF VOICE-ACTIVATED DEVICES

Anne Pfeifle*

Abstract: Alexa, Amazon's digital voice assistant, and devices like it, are increasingly common. With this trend comes growing problems, as illustrated by a murder investigation in Bentonville, Arkansas. Police wanted Amazon to turn over data associated with the suspect's Echo device, hoping it had overheard something on the night of the murder. The case sparked wide-spread interest in the privacy implications of in-home devices that record audio of users. But the biggest threat to user privacy is not that Alexa may overhear a crime—it is that law enforcement will use such devices in new ways that users are not prepared for during investigations. Thus, a solution is needed for users to have the confidence and certainty that bringing these devices into their homes will not erode their privacy. This Comment proposes that companies should ensure privacy protections are engineered into their devices, and that legislatures should adopt forward-looking statutes to ensure protections for users.

INTRODUCTION

Several San Diego households were surprised when, in January 2017, Amazon notified them that they had attempted to buy a dollhouse.[1] None of the families had placed an order for a dollhouse, yet Amazon tried to confirm the order anyway.[2] Why did Amazon think each of these families had tried to order a dollhouse? The answer is Amazon's in-home, voice-activated device: the Echo.[3]

Amazon's voice-activated digital assistant, Alexa, powers Echo devices.[4] The Echo works by listening for a wake word; by default, that

* J.D. Candidate, University of Washington School of Law, Class of 2018. I would like to thank Professor Ryan Calo for his guidance, edits, and input. I would also like to thank the stellar team at *Washington Law Review*, without which this piece would not be possible.

1. Andrew Liptak, *Amazon's Alexa Started Ordering People Dollhouses After Hearing Its Name On TV*, VERGE (Jan. 7, 2017, 5:52 PM), https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse [https://perma.cc/UH38-354N].

2. *Id.*

3. *Id.*

4. Robert Hackett, *Amazon Echo's Alexa Went Dollhouse Crazy*, FORTUNE (Jan. 9, 2017), http://fortune.com/2017/01/09/amazon-echo-alexa-dollhouse/ [https://perma.cc/EL4L-YCWX].

word is "Alexa."[5] Once "awake," the Echo device responds to requests.[6] It can check the weather, order from Amazon, and search the internet.[7] In short, people use the Echo by talking to it.

Returning to the mystery dollhouses: each of the dollhouse-ordering families owned an Echo and had been tuned into a certain news segment.[8] That news segment detailed the story of an enterprising six-year-old girl who had used her family's Echo to order herself a dollhouse and four pounds of cookies.[9] Near the end of the segment, the anchor said, "I love the little girl saying, 'Alexa order me a dollhouse.'"[10] That was enough to trigger Echo devices all around the San Diego area.[11]

Though accidental orders are ultimately harmless, not all accidental Echo uses are as innocent. For example, police sought data from an Echo related to a Bentonville, Arkansas murder investigation.[12] On November 22, 2015, James Andrew Bates called the police to report that Victor Parris Collins was dead in Bates's hot tub.[13] During the investigation, police discovered that Bates's Echo may have been used to play music that night.[14] Accordingly, officers sought the Echo's data.[15] Bentonville police served Amazon with two warrants, each requesting the Echo's data.[16] But Amazon initially failed to provide information to the Bentonville police—specifically the recordings transmitted from the Echo to Amazon's servers.[17] In refusing to turn over the data, Amazon asserted opposition to broad requests for information and sought to

5. *Change the Wake Word*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201971890 [https://perma.cc/R2ZY-78UZ].

6. *Differences Between Alexa Devices*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202009700 [https://perma.cc/6S7Q-VTUX].

7. Taylor Martin & David Priest, *The Complete List of Alexa Commands So Far*, CNET (Dec. 18, 2017, 3:20 PM), https://www.cnet.com/how-to/the-complete-list-of-alexa-commands/ [https://perma.cc/TQ6N-6G5H].

8. Liptak, *supra* note 1.

9. *Id.*

10. *Id.*

11. *Id.*

12. Search Warrant Return at 9, State v. Bates, No. CR-16-370-2 (Ark. Apr. 18, 2016).

13. Zuzanna Sitek & Dillon Thomas, *Bentonville PD Says Man Strangled, Drowned Former Georgia Officer*, 5NEWSONLINE (Feb. 23, 2016, 8:40 AM), http://5newsonline.com/2016/02/23/bentonville-pd-says-man-strangled-drowned-former-georgia-officer/ [https://perma.cc/QB95-Q37J].

14. *See* Search Warrant Return, *supra* note 12, at 9.

15. *Id.*

16. *Id.*

17. *Id.* at 9–10.

protect Echo users' privacy.[18] But on March 3, 2017, Amazon finally agreed to turn over the requested data.[19]

The rising prevalence of in-home, voice-activated devices like the Echo present on-going privacy concerns.[20] Experts caution that the Bentonville case is merely the beginning—for example, the Echo could be remotely configured to record every word said in a home.[21] Adding to this concern, current privacy laws are generally ill-suited to new technologies.[22]

This Comment examines the current state of privacy protections for electronic communications, like the audio recordings captured by Alexa. This Comment proposes forward-looking solutions to deal with the increasing pace of innovation and will use in-home recording devices, like Amazon's Alexa-enabled devices, as a way to explore this issue. This Comment focuses on Amazon and Alexa because the Bentonville murder case provides a timely example of the issues that all tech companies face—the on-going conflict between tech companies and law enforcement over users' data.

Part I will discuss current technologies and the current relevant law. First, section I.A will examine the existing legal protections for electronic communications. Next, it will review expert proposals for updating electronic communications protections. Then, this Comment will detail Alexa's functionality, followed by the ongoing conflicts between law enforcement and technology companies. Part II will propose a two-pronged solution: one technological, one legal. Companies should "bake in" privacy protections so that the devices are engineered to protect users more effectively. In addition, this Comment

---

18. Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. TIMES (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html [https://perma.cc/7PB5-PCM7] ("Without addressing specifics of the case, Amazon said in a statement that, as a matter of course, it 'objects to overbroad or otherwise inappropriate demands.'").

19. Stipulation and Consent Order at 1, *Bates*, No. CR-16-370-2 (Ark. Mar. 3, 2017). Arkansas eventually dropped the case. Motion to Nolle Prosequi for Good Cause at 1, *Bates*, No. CR-16-370-2 (Ark. Dec. 5, 2017).

20. *See generally*, Mele, *supra* note 18 (describing privacy concerns related to in-home recording devices).

21. *See infra* section II.A.

22. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited 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." (citations omitted)).

will argue that new, flexible, forward-looking schemes are needed to protect users' privacy, and that state law is best situated for that task.

I. NEW TECHNOLOGIES REQUIRE RETHINKING OUR APPROACH TO PRIVACY

First, this Part will provide a backdrop of the current legal landscape, discussing current privacy laws, including Supreme Court jurisprudence, federal law, and state law. Next, this Part considers experts' proposals to revise current privacy law. Then, it will examine in-home technologies that capture voice recordings. Finally, this Part will analyze the historical disputes between law enforcement and technology companies.

A. The Application of Current Privacy Laws to New Technologies Can Be Uncertain, Though Some States Are Making Changes

As technology advances, and law enforcement seeks to use those advances to aid in criminal investigations, the current legal regime struggles to deal with novel situations and new uses of technology. This section will discuss the current landscape of privacy protections for digital communications. First, the section will review the state of current federal law regarding electronic privacy. Next, it will describe recent state laws aimed at consumer privacy for technological developments. Finally, this section will examine experts' proposals on protecting privacy.

1. The Supreme Court Has Not Yet Recognized a Privacy Interest in All Electronic Communications

The Fourth Amendment protects the sanctity of the home,[23] but the meaning of "home" grows more muddled as technology advances. In *Kyllo v. United States*,[24] the Court held that the home's sanctity cannot be breached by technology not in general public use.[25] Law enforcement suspected that Kyllo was growing marijuana in his home in Oregon using high-intensity lamps, which give off a large amount of heat.[26] Accordingly, agents from the Department of the Interior used a thermal

23. Kyllo v. United States, 533 U.S. 27, 40 (2001).

24. 533 U.S. 27 (2001).

25. *Id.* at 40.

26. *Id.* at 29–30.

imager to scan the house from a van across the street.[27] The imager showed that Kyllo's house was significantly warmer than other neighboring houses, leading agents to conclude that Kyllo was growing marijuana.[28] Traditionally, courts tie Fourth Amendment search questions to common-law trespass.[29] But as technology has progressed, the analysis has shifted and courts now increasingly evaluate whether there was a reasonable expectation of privacy using the standard set out by the Supreme Court: "'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'"[30] The Court then found that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[31]

In contrast, when information leaves the home and is shared with third parties, courts have held that there is no reasonable expectation of privacy.[32] In *California v. Greenwood*,[33] law enforcement agents suspected Greenwood was trafficking narcotics.[34] The officer investigating Greenwood asked the neighborhood's trash collector to give her Greenwood's trash bags.[35] The collector agreed, and the officer discovered items in the trash that indicated Greenwood used narcotics.[36] The officer used this evidence to get a warrant to search Greenwood's home, where law enforcement officers found cocaine.[37] Greenwood challenged the warrantless search and seizure of his garbage.[38] But the Court found that leaving the garbage at the curb sufficiently exposed it to the public because garbage bags and bins are often accessible by "animals, children, scavengers, snoops, and other members of the

27. *Id.*

28. *Id.* at 30.

29. *Id.* at 31.

30. *Id.* at 33 (citation omitted).

31. *Id.* at 40.

32. California v. Greenwood, 486 U.S. 35, 39–42 (1988); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

33. 486 U.S. 35 (1988).

34. *Id.* at 37.

35. *Id.*

36. *Id.* at 37–38.

37. *Id.* at 38.

38. *Id.* at 39.

public."[39] Similarly, the Court also held that there is no expectation of privacy in dialed phone numbers.[40] Likewise, the Court has not afforded checks, deposit slips, and other bank documents Fourth Amendment protection as they are shared with a third party: the bank.[41] This idea that information shared with a third party is not subject to Fourth Amendment protection is known as the third-party doctrine.[42]

However, cell phones are distinct, and they require their own warrant per *Riley v. California*.[43] The Court held that a warrantless search of a cell phone was not reasonable, and the search did not fall under the exception provided by the incident to arrest doctrine.[44] The Court explained that this heightened protection is needed because so much information can be stored on a cell phone—essentially a person's entire life.[45] The Court's recognition of the vast amounts of data stored on cell phones—and generated by modern, daily life—was exciting to experts and commentators, because it seemed to signal the Court's recognition that the digital world would require rethinking old decisions.[46] But the Court limited the impact of its holding: "these cases do not implicate the

39. *Id.* at 35.

40. Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that installing a pen register at the telephone company and using it to learn the telephone numbers called from a private telephone was not a search because the numbers were revealed to a third party).

41. United States v. Miller, 425 U.S. 435, 442 (1976).

42. *Id.* at 443.

43. __ U.S. __, 134 S. Ct. 2473 (2014).

44. *Id.* at 2493.

45. *Id.* at 2488–89 ("Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. . . . [M]any of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity.").

46. *See, e.g.*, Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment,* Riley*'s Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 160 (2014) ("Going forward, the Court may well find that when a citizen voluntarily provides information for storage with a third-party ISP she has not relinquished her Fourth Amendment protections."); Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California*, a Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSBLOG (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/ [https://perma.cc/XZ28-2END] ("The Court's argument takes clear aim at the third-party rule . . . ."); *How the Supreme Court Changed America This Year*, POLITICO MAG. (July 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497?o=2 [https://perma.cc/P4WR-GDJE] (comments of Stephen Vladeck) ("But the rhetoric and reasoning of the majority opinion . . . reflect a court coming to terms with the ways in which modern technology destroys decades-old constitutional assumptions about the line between what's public and what's private, assumptions that only made sense in an analog world.").

question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[47]

That question—whether the collection or inspection of aggregated digital information amounts to a search—has now come to the Supreme Court in the form of cell site location information (CSLI).[48] CSLI refers to the records service providers keep on which cell site a cell phone connects to during a call or text message.[49] As a cell phone—and its user—moves through an area, it connects to different cell sites.[50] This record of different cell sites allows investigators to approximate the location of the phone at different times.[51] Thus, because service providers store CSLI, some courts have held that CSLI falls under the third-party doctrine.[52] This group includes the Third Circuit,[53] the Fourth Circuit,[54] the Fifth Circuit,[55] the Sixth Circuit,[56] and the Eleventh Circuit.[57] In contrast, district courts in the Second[58] and Ninth[59] Circuits

47. *Riley*, 134 S. Ct. at 2489–90 n.1.

48. Carpenter v. United States, __ U.S. __, 137 S. Ct. 2211 (2017) (mem.) (granting certiorari).

49. WESLEY CHENG, CTR. FOR ADVANCEMENT OF PUB. INTEGRITY, DOES SEEKING CELL SITE LOCATION INFORMATION REQUIRE A SEARCH WARRANT? 2 (2016), http://web.law.columbia.edu/sites/default/files/microsites/public-integrity/files/does_seeking_cell_site_location_information_require_a_search_warrant_-_wesley_cheng_-_august_2016_update_0.pdf [https://perma.cc/TKB3-VH5E].

50. *Id.*

51. *Id.*

52. Orin Kerr, *Fourth Circuit Adopts Mosaic Theory, Holds That Obtaining "Extended" Cell-Site Records Requires a Warrant*, WASH. POST: VOLOKH CONSPIRACY (Aug. 5, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/05/fourth-circuit-adopts-mosaic-theory-holds-that-obtaining-extended-cell-site-records-requires-a-warrant [https://perma.cc/CBW9-82HA]; *see also* CHENG, *supra* note 49, at 1.

53. *See In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010).

54. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016).

55. *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

56. United States v. Carpenter, 819 F.3d 880, 886–90 (6th Cir. 2016), *cert. granted*, __ U.S. __, 137 S. Ct. 221 (2017).

57. United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015).

58. *In re* United States for an Order Authorizing Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20 (E.D.N.Y. 2011). *But see* United States v. Serrano, No. 16CR169 (WHP), 2017 WL 3055244, at *3 (S.D.N.Y. July 18, 2017) (finding that CSLI does not require a warrant because it falls under the third-party doctrine).

59. *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1036 (N.D. Cal. 2015) ("[T]he Court concludes that the third-party doctrine established in *Miller* and *Smith* does not defeat cell phone users' reasonable expectation of privacy in the historical CSLI associated with their cell phones. The government therefore conducts a 'search' within the meaning of the Fourth Amendment when it asks cellular service providers to release that information . . . .").

have ruled that law enforcement access of CSLI requires a warrant. Even the Fourth Circuit, which held that CSLI is subject to the third-party doctrine, indicated its uneasiness with its own decision, and noted that the time was ripe for the Supreme Court to step in and sort out the confusion: "[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case."[60] The Supreme Court subsequently granted certiorari in another case to resolve this confusion over CSLI.[61]

Although appellate courts have not found that CSLI requires a warrant, they have been quicker to grant protections to other types of electronic information, such as the Sixth Circuit's third-party doctrine decision in *United States v. Warshak*.[62] Warshak was the head of an herbal supplement company that allegedly engaged in numerous fraudulent schemes.[63] Warshak, and others affiliated with the company, were charged with numerous crimes including conspiracy to commit mail and wire fraud.[64] Before trial, the government had obtained Warshak's emails from his internet service provider (ISP).[65] Warshak argued that the government violated his Fourth Amendment rights by seizing about 27,000 emails without a warrant.[66] The Sixth Circuit agreed.[67]

The court first held that Warshak had a reasonable expectation of privacy in his emails.[68] Second, the court noted that letters received protection, and it did not make sense for email to be afforded less protection than letters.[69] Because the court found that emails were the functional equivalent of a letter or phone call, ISPs were thus equivalent to a post office or a phone company—the ISP makes the communication

---

But see United States v. Elima, No. SACR 16-00037-CJC, 2016 WL 3546584, at *4 (C.D. Cal. June 22, 2016) (holding that CSLI falls under the third-party doctrine).

60. United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016).

61. *See Carpenter*, 819 F.3d at 880.

62. 631 F.3d 266 (6th Cir. 2010).

63. *Id.* at 280–81.

64. *Id.* at 281.

65. *Id.*

66. *Id.* at 282.

67. *Id.*

68. *Id.* at 284.

69. *Id.* at 286.

possible.[70] And the court clarified that even if an ISP had an agreement with the user that the ISP could access the user's emails, that access was not enough to defeat Fourth Amendment protections.[71]

The Sixth Circuit noted that its decision was vulnerable in light of *United States v. Miller*.[72] *Miller*, a Supreme Court decision from 1976, held that checks, deposit slips, and other bank documents do not receive Fourth Amendment protection because they are shared with a third party: the bank.[73] But the Sixth Circuit distinguished *Miller* on two grounds.[74] First, the relevant records in *Miller* were business records, not the potentially confidential records at issue in *Warshak*.[75] Second, Miller gave the bank his records so that the bank could use them, while the ISP in *Warshak* was not the intended recipient of the emails, but merely an intermediary.[76] Accordingly, the court found that "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."[77]

But *Warshak*'s holding has not been adopted by the Supreme Court, despite the Sixth Circuit's confidence that its holding can be distinguished from *Miller*'s holding.[78] Moreover, though the Supreme Court has granted certiorari to resolve the confusion over CSLI, no decision has been released as of this Comment's publication.[79] Although the third-party doctrine remains as it was in 1976,[80] Justice Sotomayor has suggested it is time for change:

> [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. This approach is ill suited to the digital age, in which people reveal a great deal

70. *Id.*

71. *Id.* The Court noted that in certain cases, an ISP with a broad right of access could "snuff out a reasonable expectation of privacy." *Id.* at 287.

72. *Id.* at 287 (citing United States v. Miller, 425 U.S. 435 (1976)).

73. *Miller*, 425 U.S. at 442.

74. *Warshak*, 631 F.3d at 288.

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

79. *See* United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016), *cert. granted*, __ U.S.__, 137 S. Ct. 221 (2017).

80. United States v. Miller, 425 U.S. 435, 442 (1976).

of information about themselves to third parties in the course of carrying out mundane tasks.[81]

2. *The Status of New Technologies Under Federal Privacy Laws Is Uncertain*

The primary federal statute on technological privacy is the Electronic Communications Privacy Act (ECPA).[82] The ECPA authorizes prosecution of any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[83] An electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce . . . ."[84] The Act protects these communications while they are being made, while they are in transit, and when they are stored on computers.[85]

Congress enacted the Stored Communications Act[86] (SCA) as a subsection of the ECPA.[87] It prevents stored communications from being divulged without consent.[88] Under the SCA, electronic storage means "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. . . ."[89] There are exceptions for communications related to missing or exploited children, communications received inadvertently, and communications related to the commission of a crime.[90]

---

81. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (citations omitted).

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

83. 18 U.S.C. § 2511(1)(a) (2012).

84. *Id.* § 2510(12).

85. *Electronic Communications Privacy Act of 1986*, JUSTICE INFO. SHARING (July 30, 2013), https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 [https://perma.cc/9293-3H6R].

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

87. *Id.*

88. 18 U.S.C. § 2702.

89. *Id.* § 2510(17)(A)–(B).

90. *Id.* § 2702(b).

The ECPA differentiates between communications intercepted in transit and information obtained from storage.[91] It varies the legal protections afforded to communications based on the importance of the privacy interest involved.[92] Consequently, some information requires a subpoena, including the amount of time a person has used an email address; some a special court order, such as opened email messages in storage; and some a search warrant, for example, the entire contents of an email account.[93] Thus, information obtained from storage receives a more relaxed standard than information obtained in transit.[94] Additionally, if law enforcement seeks to access some types of data, then law enforcement must notify the subscriber—the person who owns the digital-storage account.[95] For example, by giving notice, law enforcement can obtain everything in a subscriber's account—except unopened email and voicemail—that has been in the account for less than 180 days, which they would not be able to do without notice.[96]

But even in cases that require notice, the ECPA allows the government to obtain secrecy orders, so that the technology company cannot tell their users that the users' data has been requested.[97] Courts grant these orders when a law enforcement officer has "reason to believe" that the company's disclosure might hinder an investigation.[98] These orders have many critics—including a recent challenge by Microsoft, which noted that "[n]othing in the statute requires that the 'reason to believe' be grounded in the facts of the particular investigation, and the statute contains no limit on the length of time secrecy orders may be kept in place."[99] Microsoft alleged that in a twenty-month period, federal courts issued 3,250 secrecy orders to

91. *Id.* §§ 2510–11.

92. *See Electronic Communications Privacy Act of 1986*, *supra* note 85.

93. 18 U.S.C. § 2703; *see also Electronic Communications Privacy Act of 1986*, *supra* note 85.

94. 18 U.S.C. § 2510.

95. *Electronic Communications Privacy Act of 1986*, *supra* note 85.

96. 18 U.S.C. § 2703(a). *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) (disagreeing with the government's interpretation of ECPA and holding that email messages were in "electronic storage" regardless of when they were first accessed) ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage. Because plaintiff's e-mail messages were in electronic storage regardless of whether they had been previously delivered, the district court's decision cannot be affirmed on this alternative ground.").

97. 18 U.S.C. § 2705(b).

98. *Id.*

99. First Amended Complaint at 1, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016).

Microsoft alone to prevent it from communicating with customers about requests for data, and of those about two-thirds had no end date.[100] Microsoft also asserted that users should not expect differing privacy protection schemes just because emails are stored in the cloud, rather than on the user's hard-drive.[101]

Experts, commentators, and service providers (like Microsoft) have criticized the ECPA for failing to keep up with changing technologies.[102] For example, ECPA does not provide transparency to users of technology.[103] Similarly, experts call it a confusing statute because it is dense, and there are few cases interpreting it.[104] Even the original drafter of the bill has called for it to be updated to match changing technologies.[105] In short, many scholars have noted that the ECPA has not kept pace with changing technology.

3. State Laws Respond More Quickly to New, Specific Technologies, and Have Greater Privacy Protections for Users

State legislatures have taken a more proactive approach to changing technologies. For example, Washington limits the use of cell site simulator devices, which allow law enforcement to track a phone's location in real time.[106] Several states have enacted laws concerning access to and use of EDRs (Event Data Recorders, or "black boxes" in

---

100. *Id.*

101. *Id.*; Brad Smith, *Keeping Secrecy the Exception, Not the Rule: An Issue for Both Consumers and Businesses*, MICROSOFT ON THE ISSUES (Apr. 14, 2016), https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/#sm.000kdpjs21cmjdjbqlm2pl8sea7ki [https://perma.cc/T9G6-5443] ("If policymakers update the rules governing secrecy orders, we hope they will be guided by . . . principles that we think are important for our customers and for law enforcement. . . . [D]igital neutrality: Customers generally shouldn't be entitled to less notice just because they have moved their emails to the cloud.").

102. Alexandra D. Vesalga, *Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data*, 43 GOLDEN GATE U. L. REV. 459, 460 (2013) ("[ECPA] fail[s] to consistently protect the geolocational data associated with electronic communications.").

103. *See* First Amended Complaint, *supra* note 99, at 3.

104. 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, 1208 (2004).

105. Press Release, Sen. Patrick Leahy, Leahy Marks 25th Anniversary of ECPA, Announces Plan to Mark Up Reform Bill (Oct. 20, 2011), www.leahy.senate.gov/press/press_releases/release/?id=56C35200-EFDC-497A-9EAF-A75B498515B8 [https://perma.cc/FUU4-4XKG] ("[T]oday, this law is significantly outdated and out-paced by rapid changes in technology.").

106. WASH. REV. CODE § 9.73.270 (2016).

cars).[107] But no state has specifically addressed software like Alexa or devices like Echo.[108]

States are well-suited to provide users with increased privacy protections because many state constitutions provide higher standards for privacy.[109] For example, Washington has what is known as the "private affairs doctrine": "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."[110] Because of this doctrine, Washington does not use the "reasonable expectation of privacy" framework used in federal courts;[111] instead, the analysis focuses on whether something is a private affair:

> In determining whether something is a private affair (meaning "those privacy interests which citizens of this state have held, and should be entitled to hold, safe from government trespass absent a warrant"), we consider both "the nature and extent of the information which may be obtained as a result of the governmental conduct" and the historical protection afforded to the interest asserted.[112]

Thus, the private affairs doctrine leads to broader privacy protections than those provided by the U.S. Constitution.[113] Specifically, government access to the following requires a warrant: phone records,[114] garbage,[115] and motel registry information.[116]

However, even the heightened protection provided by some states is not enough protection in a rapidly changing world for data that includes Alexa recordings, according to privacy advocates who continue to call

---

107. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 153–54 (2015); *Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONFERENCE STATE LEGISLATURES (Dec. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx [https://perma.cc/WQ2R-JNBX].

108. *See generally* Peppet, *supra* note 107 (discussing regulations that currently exist concerning the Internet of Things).

109. *See, e.g.*, State v. Hinton, 179 Wash. 2d 862, 868–69, 319 P.3d 9, 12 (2014) (describing Washington State's constitution).

110. WASH. CONST. art. I, § 7.

111. *See* State v. Myrick, 102 Wash. 2d 506, 515, 688 P.2d 151, 153–54 (1984), *abrogated on other grounds by* Brendlin v. California, 551 U.S. 249 (2007).

112. State v. Samalia, 186 Wash. 2d 262, 269, 375 P.3d 1082, 1086 (2016) (citation omitted).

113. *See, e.g.*, *id.* (describing Washington's constitutional protections for privacy).

114. State v. Gunwall, 106 Wash. 2d 54, 63, 720 P.2d 808, 813 (1986).

115. State v. Boland, 115 Wash. 2d 571, 578–79, 800 P.2d 1112, 1116–17 (1990).

116. State v. Jorden, 160 Wash. 2d 121, 130, 156 P.3d 893, 898 (2007).

for expanded protections.[117] A few states have responded to this call. In May 2017, Montana adopted a new statute limiting access to electronic communications stored by third parties.[118] Significantly, Montana now requires probable cause before a government entity can require an electronic communications provider to disclose a user's communications.[119] But experts still have qualms about this statute[120] because governmental agencies can request that companies not disclose to users that their information has been requested.[121] Referring to these requests as "gag orders," experts note that Microsoft has challenged a similar issue on First Amendment grounds, arguing that orders preventing them from communicating with customers restrict their speech.[122] Accordingly, privacy advocates are disappointed that a similar "gag order" provision was included the Montana statute.[123]

Privacy advocates hail California's law—the California Electronic Communications Privacy Act (CalECPA)—as "the most privacy-protective legislation of its kind."[124] The law expands on California's already heightened privacy protections.[125] California's constitution protects privacy explicitly,[126] and California does not recognize the third-party doctrine.[127] CalECPA provides more comprehensive

117. *See, e.g.*, David Lazarus, *When Your TV Can Spy on You*, L.A. TIMES (Aug. 25, 2015, 4:00 AM), http://www.latimes.com/business/la-fi-lazarus-20150825-column.html [https://perma.cc/K66B-9U5S] (describing concerns about in-home recording technology).

118. H.B. 148, 65th Leg., Reg. Sess. (Mont. 2017) (to be codified in scattered sections of MONT. CODE ANN. § 46).

119. *Id.*

120. *See* Adam Schwartz & Andrew Crocker, *Montana Protects Communications Privacy, But Allows Gag Orders*, ELEC. FRONTIER FOUND. (June 1, 2017), https://www.eff.org/deeplinks/2017/06/montana-protects-communications-privacy-allows-gag-orders [https://perma.cc/6FNP-SHKN].

121. *Id.*

122. *See id.*

123. *See id.*

124. Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, 33 BERKELEY TECH. L.J. (forthcoming 2018) (manuscript at 1), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2939412 [https://perma.cc/F3KY-GBVQ]; *see also* ACLU News, *In a Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communications Privacy Act into Law*, ACLU N. CAL. (Oct. 8, 2015), https://www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy [https://perma.cc/A3YJ-ZND7]; Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [https://perma.cc/6L3Q-PHWJ].

125. *See* CAL. CONST. art I, § 1.

126. *Id.*

127. *See* People v. Chapman, 679 P.2d 62, 68, 71 (Cal. 1984) (requiring a search warrant for police access to a person's unlisted name, phone number, and address), *overruled on other grounds*, People v. Palmer, 15 P.3d 234 (Cal. 2001); People v. Blair, 602 P.2d 738, 747–48 (Cal. 1979)

protection to more categories of information than any other state.[128] Under CalECPA, law enforcement must obtain a warrant—limited appropriately in scope—before compelling the disclosure of electronic communications information from service providers.[129] Though all warrants in California require that the warrant "particularly describe" what law enforcement agents intend to search,[130] CalECPA goes further by requiring that the warrant describe "the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought."[131] Thus, CalECPA narrows potentially overly broad warrants by requiring that law enforcement more carefully delineate the parameters of the warrant.[132] By adding more requirements to adequately circumscribe warrants, CalECPA prevents "fishing expeditions that violate the spirit, if not the letter, of the Fourth Amendment."[133]

And though warrants under CalECPA must be narrow, the definition of "service provider" is broad, and includes services like Dropbox, Facebook, and Gmail.[134] Because that definition is broad, it provides protections for users of a wide variety of services.[135] Similarly, "electronic information" is broad and includes "technologically neutral language," which ensures that future technological development is included.[136] Significantly, CalECPA requires that the target of a warrant be notified.[137] If that notice is delayed, the requesting governmental entity must explain why, once notice is given.[138] In addition, when the target of a search is not identified, the California Department of Justice must be notified.[139] This notification scheme is used in investigations where information is collected from unidentified targets, such as cell

---

(protecting telephone numbers); Burrows v. Superior Court, 529 P.2d 590, 594–95 (Cal. 1974) (protecting bank records).

128. Freiwald, *supra* note 124, at 12.

129. *Id.* at 15.

130. CAL. PENAL CODE § 1525 (West 2017).

131. *Id.* § 1546.1(d)(1).

132. Freiwald, *supra* note 124, at 21–22.

133. *Id.* at 22 (footnote omitted).

134. *Id.* at 16.

135. *Id.*

136. *See* CAL. PENAL CODE § 1546.

137. *Id.* § 1546.2.

138. *Id.*

139. *Id.*

tower dumps, where the government compels cell phone providers to turn over all the data from several cell towers that served a crime scene during the window in which the crime occurred.[140] In short, "[c]ompared to ECPA, CalECPA requires warrants for more investigations, its warrants impose more restrictive requirements; it provides more notice to targets, and it furnishes more significant remedies."[141]

Experts note a few remaining problems with CalECPA, however. First, when and how information becomes an electronic communication is unclear in edge cases, such as if the communication is sent without human involvement.[142] And because the definition of "service provider" depends on whether service providers give their subscribers the ability to send or receive electronic communications,[143] the exact scope of the term remains murky as long as the definition of "electronic communication" remains unclear.[144] Additionally, "subscriber information" is not subject to warrant requirements,[145] but an "IP address" is subject to warrant requirements because it is an electronic communication.[146] Sometimes an IP address acts more as an identifier for subscribers, such as when IP addresses are fixed and attached to devices, not communications.[147] Thus, though experts suggest fixed IP addresses would require a warrant, courts have yet to clarify the issue.[148]

Separately from CalECPA, California also has a law on connected televisions.[149] Passed in response to consumers' worries about their televisions "eavesdropping" on them,[150] the law prevents recordings used to improve the voice recognition feature from being used for advertising purposes, and requires that "a person or entity shall not compel a manufacturer or other entity providing the operation of a voice recognition feature to build specific features for the purpose of allowing an investigative or law enforcement officer to monitor communications

140. Freiwald, *supra* note 124, at 28; *see also In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 674 (S.D. Tex. 2015) (describing cell tower dumps).

141. Freiwald, *supra* note 124, at 30.

142. *Id.* at 38.

143. CAL. PENAL CODE § 1546(j).

144. Freiwald, *supra* note 124, at 38–39.

145. CAL. PENAL CODE § 1546.1(f).

146. *Id.* § 1546(j).

147. Freiwald, *supra* note 124, at 39.

148. *Id.*

149. CAL. BUS. & PROF. CODE § 22948.21 (West 2016).

150. Lazarus, *supra* note 117.

through that feature."[151] In short, this law addressed worries about in-home recording devices eavesdropping on consumers and protections for technology companies who hope to avoid being compelled to engineer their products in a way that is useful for law enforcement, instead of consumers.[152]

Other states have moved towards enhanced protections as well. In March 2018, Washington passed a bill to "protect[] an open internet."[153] Legislatures in twenty-six states have introduced bills requiring internet service providers to ensure various net neutrality principles.[154] These laws are a response to Congress lifting the Federal Communications Commission's (FCC) ban on selling users' data without consent.[155] The bills are focused on what companies can and cannot do with users' information, and not whether the government needs a warrant to access a user's information.[156] But they show the increased support for and focus on what happens to users' digital information.[157] In sum, there is momentum in many states for more privacy protections for users of online service providers.

4. Experts Propose Solutions at Every Level: Federal, State, and Entity

To keep pace with quickly changing technology, experts, scholars, and privacy advocates have proposed a number of solutions to protect users' privacy. Some scholars propose keeping the third-party doctrine for searches of electronic communications, but advocate that the law should distinguish between content and non-content.[158] Content refers to the information contained in a communication, while non-content is

---

151. CAL. BUS. & PROF. CODE § 22948.20.

152. *Id.*

153. S.H.B. 2282, 65th Leg., Reg. Sess. (Wash. 2018). Governor Jay Inslee signed the bill on March 5, 2018. *Bill Information*, WASH. GOVERNOR, https://www.governor.wa.gov/office-governor/official-actions/bill-action [https://perma.cc/GR2G-5EL3].

154. *Net Neutrality Legislation in States*, NAT'L CONF. ST. LEGIS. (Feb. 23, 2018), http://www.ncsl.org/ncsl-in-dc/publications-and-resources/net-neutrality-legislation-in-states.aspx [https://perma.cc/S3U5-86U9].

155. Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the Federal Communications Commission rule "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"); *see Net Neutrality Legislation in States*, *supra* note 154.

156. *See Net Neutrality Legislation in States*, *supra* note 154.

157. *See id.*

158. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007–08 (2010).

information relating to those communications.[159] For example, the body of an email is content, while the size of the email, the date and time, and the recipient are non-content.[160] Scholars propose that, once that distinction is made, courts should proceed "by applying the warrant requirement with person-based particularity restrictions."[161] These proposed restrictions would require that warrants be directed to a person, not a certain account, as people may have multiple accounts or share them with others.[162] This approach would also exclude information found to be incidental to the specific person and crime.[163]

However, other scholars contend that all digital information should be classified as content due to the vast quantities of data generated by modern life.[164] They also worry that "re-entrenching the content/non-content distinction will not address the longer-term concern: how to protect the privacy interests at stake."[165] Electronic communications blur the line between content and non-content, so scholars assert that continuing to hang substantive rights on rapidly eroding distinctions only narrows privacy rights.[166] Because so much of modern life depends on entrusting third parties with information, some experts no longer think that it makes sense to rely on the third-party doctrine and would abandon it.[167]

Another scholar proposes keeping the third-party doctrine, but returning it to the pre-*Smith*, "reasonable expectation of privacy" analysis[168] as espoused in *Katz v. United States*.[169] This proposal cites Justice Sotomayor's concurrence in *Jones* to signify that the time has come for the Supreme Court to revisit the doctrine, and uses the concept of "smart homes," or homes connected to the internet via devices like the Echo, to examine the doctrine.[170] Given that in-home devices cross

159. *Id.* at 1008.

160. *Id.* at 1030.

161. *Id.* at 1048.

162. *Id.* at 1047.

163. *Id.* at 1047–48 ("[C]ourts should not admit evidence of crimes found in a search pursuant to an Internet warrant unless the evidence under consideration falls within the scope of the warrant.").

164. Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 663 (2016).

165. *Id.* at 663.

166. *Id.* at 678.

167. *Id.*

168. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1942–45 (2017).

169. 389 U.S. 347 (1967).

170. Note, *supra* note 168, at 1932–33.

into the sanctity of the home, the proposal recommends that "the Court, when examining cases that implicate the third-party doctrine, can—and should—apply the *Katz* test in each instance."[171] In other words, this scholar proposes that the Court should hold that the proper inquiry is a "reasonable expectation of privacy" even when information is disclosed to a third-party.[172]

But other privacy advocates call for the focus to be on expanding existing state laws instead of waiting for the courts to abolish the third-party doctrine or to modify it.[173] California—with CalECPA—is a model in this area.[174] Experts predict that state legislatures will look to eavesdropping statutes as a basis for expanding privacy protections.[175] However, current eavesdropping statutes turn on consent, but most devices owners are considered to have consented to the device's listening.[176] Experts suspect, though, that many users do not completely understand the scope of the recordings.[177] In short, experts fear that users do not understand that they have already consented to being recorded, and that their consent means the recording could be used in court.[178]

In sum, courts and legislatures have begun recognizing the privacy implications of electronic communications devices, though at differing rates. Federal lawmakers and the Supreme Court have generally been slower to anticipate change than state lawmakers. For example, the Supreme Court has yet to revisit the third-party doctrine,[179] though at least one justice has suggested that it is time to do so.[180] Experts also note the necessity of revisiting the third-party doctrine, given that sharing vast amounts of information with third parties is a virtual necessity of modern life.[181] But other experts propose retaining the third-party doctrine, and returning the doctrine to its "reasonable expectation

171. *Id.* at 1945.

172. *Id.*

173. Lazarus, *supra* note 117.

174. CAL. PENAL CODE § 1546 (West 2017).

175. Alison DeNisco Rayome, *Amazon Echo Murder Case Raises IoT Privacy Questions for Enterprise Users*, TECHREPUBLIC (Jan. 11, 2017, 9:34AM), http://www.techrepublic.com/article/amazon-echo-murder-case-raises-iot-privacy-questions-for-enterprise-users [https://perma.cc/WWW6-EXEX].

176. *Id.*

177. *Id.*

178. *Id.* ("It's likely that we will soon see state legislation looking more carefully at eavesdropping statutes.").

179. *See* Note, *supra* note 168.

180. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

181. *See* Donohue, *supra* note 164.

of privacy" roots.[182] In contrast, statutes like CalECPA require a warrant before the disclosure of electronic communications and are technologically neutral, meaning the statute does not reference any specific, current technologies, but instead anticipates that technology will change.[183] In short, new technologies have thus far inspired a variety of proposals and responses.

B. Alexa, Amazon's Voice-Activated Digital Assistant, Is a Powerful Tool

Devices like the Echo have sparked significant interest from consumers and law enforcement alike, though many misunderstand the technology. This section will discuss Alexa, Amazon's voice-activated digital assistant, describe what kinds of devices use it, and explain how the software operates. Then the section will explain Amazon's privacy policy and how data from Alexa-enabled devices are used. Finally, the section will discuss requests by law enforcement for users' data.

1. Alexa Records Users, Transmits and Stores Those Recordings, and Uses Them to Learn

Alexa is Amazon's voice-activated digital assistant.[184] Alexa Voice Service can power any computing device connected to the internet that has a microphone and speaker.[185] As the engine behind Amazon devices like the Amazon Echo, Echo Dot, and Tap, Alexa enables these wireless speakers to perform many tasks.[186] These devices perform similar functions—responding to spoken requests—but vary by size and portability.[187]

---

182. *See* Note, *supra* note 168, at 1945.

183. *See* CAL. PENAL CODE § 1546 (West 2017).

184. *Amazon Alexa*, AMAZON DEVELOPER, https://developer.amazon.com/alexa [https://perma.cc/7BSA-3ANM].

185. *Alexa Voice Service*, AMAZON DEVELOPER, https://developer.amazon.com/alexa-voice-service [https://perma.cc/RB5T-RHAR].

186. Grant Clauser, *What is Alexa? What is the Amazon Echo, and Should You Get One?*, WIRECUTTER (Jan. 6, 2017), http://thewirecutter.com/reviews/what-is-alexa-what-is-the-amazon-echo-and-should-you-get-one/ [https://perma.cc/48F7-4MWZ]; *Echo Dot*, AMAZON, https://www.amazon.com/All-New-Amazon-Echo-Dot-Add-Alexa-To-Any-Room/dp/B01DFKC2SO [https://perma.cc/Y2XD-9RY3].

187. *Echo and Alexa Devices*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202009700 [https://perma.cc/6S7Q-VTUX].

Amazon calls Alexa's voice-driven capabilities "skills."[188] Alexa can check the weather, report headlines, create shopping lists, order products from Amazon, search the internet, turn lights on and off, and even tell jokes.[189] Developers can build these voice-controlled skills like they build phone applications.[190] As a result, more and more skills are added to Alexa's repertoire.[191] For example, the number of skills grew from 1,000 to 7,000 in seven months.[192]

Like Alexa's skills, the number of in-home digital assistants like the Echo is growing as well. In 2016, Amazon reported sales nine times greater than 2015.[193] Many companies are introducing dozens of voice-enabled devices, from refrigerators to televisions to cars.[194] By 2020, the market for digital assistants is estimated to grow to $3.6 billion.[195]

To use voice-enabled devices like the Echo or Echo Dot, users can use a wake word.[196] By default, Alexa's wake word is "Alexa." Amazon engineers chose this word because it was unique, and users are unlikely to say it in natural conversation and inadvertently trigger Alexa to take action.[197] When the device detects the wake word, it begins to record and transmit that recording, including a fraction of a second of audio before the wake word.[198] To cut down on false positives, the device will transmit the recording to a cloud-based verification system, which

---

188. *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/LFW8-QLPT].

189. Martin & Priest, *supra* note 7.

190. *See Alexa Skills Kit*, AMAZON DEVELOPER, https://developer.amazon.com/alexa-skills-kit#Ready%20to%20start%3F [https://perma.cc/H8CC-5LKY].

191. *Id.*

192. David Pierce, *Alexa Just Conquered CES. The World Is Next*, WIRED (Jan. 6, 2017, 6:15 AM), https://www.wired.com/2017/01/ces-alexa-in-everything/ [https://perma.cc/M9JR-7V6D].

193. *Alexa Devices Top Amazon Best-Seller List this Holiday – Millions of Alexa Devices Sold Worldwide*, BUS. WIRE (Dec. 27, 2016, 9:00 AM), http://www.businesswire.com/news/home/20161227005118/en/ [https://perma.cc/6GJ5-LBC3]. Amazon does not report actual sales numbers.

194. Pierce, *supra* note 192.

195. *Intelligent Virtual Assistant Market Overview*, ALLIED MKT. RESEARCH (Jan. 2016), https://www.alliedmarketresearch.com/intelligent-virtual-assistant-market [https://perma.cc/RDF2-9LFH].

196. *Talk to Your Alexa Device*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202013720 [https://perma.cc/9XQZ-V2RP].

197. *See, e.g.*, Julie Bort, *Amazon Engineers Had One Good Reason and One Geeky Reason for Choosing the Name Alexa*, BUS. INSIDER (July 12, 2016, 7:05 PM), http://www.businessinsider.com/why-amazon-called-it-alexa-2016-7 [https://perma.cc/2UHD-LHVD] (explaining how the name "Alexa" was chosen). The name "Alexa" also comes from the Library of Alexandria—the source of all knowledge. *Id.*

198. *Alexa and Alexa Device FAQs*, *supra* note 188.

double-checks to be sure that the wake word was uttered.[199] Alexa can then respond to the request.[200] During activation, audio is streaming to the cloud.[201] Storing data in the cloud allows uninterrupted access to the data, greater storage capacity, and lower cost, as there is no need for storage hardware.[202] Data sent from an Alexa device to the cloud is encrypted.[203]

Cloud storage also allows Amazon to associate recordings with the user's Amazon account,[204] which helps to improve Alexa.[205] Alexa can learn a user's voice patterns to better understand the user's requests.[206] Gradually, the devices learn the user's preferences and voice patterns.[207] Because Alexa is cloud-based, and not bound by a single device's hardware constraints, complex computing—such as Automatic Speech Recognition and Natural Language Understanding—can be done.[208] Amazon also aggregates the anonymized recordings to help improve Alexa's understanding of different speech patterns.[209] Users can delete their recordings from their account, but Amazon cautions that deleting recordings will impair Alexa's performance.[210]

---

199. Ted Karczewski, *Cloud-Based Wake Word Verification Improves "Alexa" Wake Word Accuracy on Your AVS Products*, AMAZON DEVELOPER (May 15, 2017), https://developer.amazon.com/blogs/alexa/post/b136b3e7-0ba8-4589-aaf9-2a037fc4e9c9/cloud-based-wake-word-verification-improves-alexa-wake-word-accuracy-on-your-avs-products [https://perma.cc/LK2M-9AEL].

200. *Talk to Your Alexa Device*, *supra* note 196.

201. *Alexa and Alexa Device FAQs*, *supra* note 188. The cloud refers to software and services (like storage) that run on the internet, and not on personal hardware, like a laptop or phone. Bonnie Cha, *Too Embarrassed to Ask: What Is 'The Cloud' and How Does It Work?*, RECODE (Apr. 30, 2015, 4:00 AM), http://www.recode.net/2015/4/30/11562024/too-embarrassed-to-ask-what-is-the-cloud-and-how-does-it-work [https://perma.cc/5NXR-DWG3].

202. *What is Cloud Storage?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is-cloud-storage/ [https://perma.cc/74TN-AE8A].

203. Tim Moynihan, *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/[https://perma.cc/VVT2-R85Q].

204. *Alexa and Alexa Device FAQs*, *supra* note 188.

205. *Id.*

206. *Id.*

207. *Echo Dot*, AMAZON, https://www.amazon.com/All-New-Amazon-Echo-Dot-Add-Alexa-To-Any-Room/dp/B01DFKC2SO [https://perma.cc/T4S8-A4AA].

208. *Alexa Voice Service*, AMAZON DEVELOPER, https://developer.amazon.com/alexa-voice-service/what-is-avs [https://perma.cc/6F9V-Z6F7].

209. Jing Cao & Dina Bass, *Why Google, Microsoft, and Amazon Love the Sound of Your Voice*, BLOOMBERG TECH. (Dec. 13, 2016), https://www.bloomberg.com/news/articles/2016-12-13/why-google-microsoft-and-amazon-love-the-sound-of-your-voice [https://perma.cc/5DW7-ATQ8] ("Every hour, Amazon uploads Alexa queries to a vast digital warehouse.").

210. *Id.*

2. Police Sought Information from an Echo Device in an Investigation, and Amazon Pushed Back

In what is believed to be the first case of its kind, police investigating a murder in Bentonville, Arkansas sought a warrant for records from an Echo in late December 2015.[211] On November 22, 2015, James Andrew Bates called the police to report that Victor Parris Collins was dead in his hot tub in Bentonville, Arkansas.[212] Bates, Collins, and a few other friends had gathered at Bates's home to watch a football game.[213] After the game, Collins and the others used the hot tub, while Bates went to bed.[214] In the morning, Bates discovered Collins in the hot tub.[215] During the execution of a search warrant, officers found an Echo in Bates's kitchen,[216] as well as other "smart home" devices that control the temperature and an alarm system.[217] Because the Echo may have been activated around the time of Collins's death, they sought to retrieve the records uploaded from Bates's Echo.[218]

Police served Amazon on December 4, 2015.[219] Amazon did not provide the requested data.[220] Police served Amazon with a second warrant, but Amazon still did not provide the information, specifically the recordings transmitted from the Echo to its servers.[221] It moved to quash the search warrant, arguing that a heightened burden for compelled production applied in this case.[222] Amazon also argued that the recordings may contain expressive content protected by the First Amendment.[223] Seeking to protect users' privacy rights from government intrusion, Amazon argued its customers' data was expressive content, and was thus protected by the First Amendment: "[t]he fear of government tracking and censoring one's reading, listening, and viewing choices chills the exercise of First Amendment

211. Search Warrant Return, *supra* note 12, at 9.

212. Sitek & Thomas, *supra* note 13.

213. *Id.*

214. *Id.*

215. *Id.*

216. Search Warrant Return, *supra* note 12, at 8.

217. *Id.* at 9.

218. *Id.*

219. *Id.*

220. *Id.*

221. *Id.*

222. Motion to Quash Search Warrant at 1, *Bates*, No. CR-16-370-2 (Ark. Feb. 17, 2017).

223. Memorandum of Law in Support of Motion to Quash Search Warrant at 2, *Bates*, No. CR-16-370-2 (Ark. Feb. 17, 2017).

rights."[224] Amazon asserted that both recordings of a user's speech and a transcript of Alexa's response are protected First Amendment speech.[225] This protection stems from First Amendment protection of "not only an individual's right to speak, but also his or her 'right to receive information and ideas.'"[226]

Amazon first argued that recordings of users' requests for information are expressive information.[227] It cited cases where an individual's records of bookstore purchases were protected,[228] and noted that Echo users play music, stream podcasts, and play audio books through their devices.[229] Because the recordings reveal more information than bookstore records do, Amazon argued that they are subject to heightened First Amendment protections.[230] Amazon then argued that Alexa's responses are also protected. Alexa's responses could include expressive material, like podcasts or audiobooks.[231] In addition, the responses also include Amazon's protected speech.[232] Speech produced by search engines is protected,[233] and like the content produced by those search engines, Alexa decides what information to include and the order in which it displays responses.[234]

Amazon noted that its users' purchases are expressive content, subject to First Amendment protections.[235] Thus, like purchase history, Amazon argued that recordings from an Alexa-enabled device are also protected: "[u]sers convey, and the Alexa Voice Services returns, expressive content through their Alexa-enabled devices."[236]

---

224. *Id.* at 2 (quoting Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154, 1168 (W.D. Wash. 2010)).

225. *Id.* at 9.

226. *Id.* at 10 (quoting Stanley v. Georgia, 394 U.S. 557, 564 (1969)).

227. *Id.* at 11.

228. *Id.* at 10–11 (quoting United States v. Rumely, 345 U.S. 41, 57–58 (1953) (Douglas, J., concurring)) (citing Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1056–59 (Colo. 2002) (en banc)).

229. *Id.*

230. *Id.*

231. *Id.* at 11.

232. *Id.*

233. *E.g.*, Search King, Inc. v. Google Tech., Inc., No. Civ-02-1457-M, 2003 WL 21464568, at *4 (W.D. Okla. May 27, 2003) (holding that search engine speech is protected).

234. Memorandum of Law in Support of Motion to Quash Search Warrant, *supra* note 223, at 11–12, (citing *Search King, Inc.*, 2003 WL 21464568, at *4).

235. *Id.*

236. *Id.* at 5.

Because both the user's recording and Alexa's response are protected First Amendment speech, Amazon concluded that a heighted level of scrutiny applies when the government seeks data from Echo-enabled devices.[237] So, according to Amazon, the government must show a compelling interest and a sufficient nexus between the information sought and the underlying investigation.[238] Moreover, Amazon noted that past courts have applied this heighted standard when the government requested Amazon customer information.[239] When the government requested customer information, it "chill[ed] the exercise of First Amendment rights . . . [and] 'would frost keyboards across America.'"[240] Finally, Amazon asked for an in camera review if the government's request met this heightened level of scrutiny to "ensure that First Amendment concerns are properly protected with respect to the specific materials requested."[241]

But whether users' recordings and Alexa's responses are protected First Amendment speech with a heightened level of scrutiny is still an unsettled question: Amazon's motion was dismissed as moot[242] because on March 3, 2017, Amazon agreed to give the government the requested data.[243]

---

237. *Id.* at 12.

238. *Id.* (citing *In re* Grand Jury Subpoenas Duces Tecum, 78 F.3d 1307, 1312 (8th Cir. 1996) (applying heightened standard to grand jury subpoena for records of campaign contributions); *In re* Faltico, 561 F.2d 109, 111 (8th Cir. 1977) (per curiam) (applying heightened standard to grand jury subpoena for membership of trade association); *In re* Grand Jury Investigation of Possible Violations of 18 U.S.C. § 1461, 706 F. Supp. 2d 11, 13, 16–21 (D.D.C. 2009) (applying heightened standard to grand jury subpoena seeking to compel company to produce records of customer purchases of movies); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002) (applying heightened standard to search warrant for criminal suspect's book purchase records); *In re* Grand Jury Subpoena to Kramerbooks & Afterwords, 26 Media L. Rep. 1599, 1601 (D.D.C. 1998) (applying heightened standard to grand jury subpoena for Monica Lewinsky's book-purchase records)).

239. *Id.* at 12–13 (citing *In re* Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D. 570, 572–74 (W.D. Wis. 2007) (buyers' personal identities and titles of books purchased through Amazon); Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154, 1168 (W.D. Wash. 2010) (all Amazon purchases, including expressive materials)).

240. *Id.* at 14 (quoting In re *Grand Jury Subpoena to Amazon.com Dated August 7, 2006*, 246 F.R.D. at 573).

241. *Id.* at 15.

242. Stipulation and Consent Order, State v. Bates, No. CR-16-370-2 (Ark. Mar. 6, 2017).

243. *Id.* It is unknown why Amazon changed its position, and ultimately, Arkansas dismissed the case. Motion to Nolle Prosequi for Good Cause, *supra* note 19.

3. *Law Enforcement Requests for Data from the Latest Technology Are Nothing New, but That Is Not the Most Pressing Concern for In-Home Listening Devices*

The showdown between Amazon and the Bentonville Police Department is just the latest in an on-going string of clashes between technology companies and law enforcement agents regarding users' information.[244] The continuing disputes show there is a clear need for guidance from lawmakers.[245]

The FBI in particular is an early adopter of technology. For example, in 2003, the FBI wanted to use technology like OnStar to eavesdrop on drivers.[246] OnStar can provide audio and location information when the in-car cellular connection is switched on.[247] Moreover, some cars equipped with satellite radio, like SiriusXM, can provide continuous location information to law enforcement.[248]

As users share more data with more companies, requests for private data from those devices are becoming more common—and more concerning. In January 2017, law enforcement officers used data from an Ohio man's pacemaker to charge him with arson.[249] The Ohio man claimed that he awoke to the smell of smoke, rushed to gather his possessions, then leapt out the window. But the pacemaker data contradicted his story and showed that he did not exert himself when he

---

244. *See infra* notes 246–56.

245. *See* United States v. Jones, 565 U.S. 400, 417, (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431, 435–36 (2013) ("[W]e now live in a world of ubiquitous third party information.").

246. BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U., DON'T PANIC. MAKING PROGRESS ON THE "GOING DARK" DEBATE 13 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/6AG2-LBVB]; Adam Liptak, *Court Leaves the Door Open for Safety System Wiretaps*, N.Y. TIMES (Dec. 21, 2003), http://www.nytimes.com/2003/12/21/automobiles/court-leaves-the-door-open-for-safety-system-wiretaps.html [https://perma.cc/ZKY6-MR8C].

247. Liptak, *supra* note 246.

248. Thomas Fox-Brewster, *Cartapping: How Feds Have Spied on Connected Cars for 15 Years*, FORBES (Jan. 15, 2017), http://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/#165713c649b5 [https://perma.cc/9FDD-452A].

249. Cleve R. Wootson, Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story.*, WASH. POST (Feb. 8, 2017), https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story [https://perma.cc/9PVL-MBBE].

claimed he did.[250] The data from the pacemaker were so helpful that the officers have since made more requests for pacemaker data, leading to two homicide arrests.[251] Data from fitness trackers, like the Fitbit, have been used to support a personal injury claim,[252] undermine a rape claim,[253] and contradict a suspect's account of a murder.[254] The power and promise of technological advances have intrigued law enforcement for a long time. But technology companies have trouble striking the balance between using their vast amounts of data to assist law enforcement[255] and protecting their users' privacy.[256]

Though the Bentonville case is over,[257] and as experts predicted, the outcome of the case did not change the status of privacy laws,[258] the Bentonville case continues to provoke wide-spread interest and concern regarding the privacy implications of having a listening device in the home.[259] And there are other ways that voice-activated devices could be used to assist law enforcement investigations.[260] For example, the devices could be configured to constantly record a suspect.[261] The

250. *Id.*

251. *Id.*

252. Kate Crawford, *When Fitbit Is the Expert Witness*, ATLANTIC (Nov. 19, 2014), https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936 [https://perma.cc/J74V-ETTY].

253. Kashmir Hill, *Fitbit Data Just Undermined a Woman's Rape Claim*, SPLINTER (June 29, 2015, 2:57 PM), https://splinternews.com/fitbit-data-just-undermined-a-womans-rape-claim-1793848735 [https://perma.cc/P5DD-NUDB] ("[A] Fitbit device [the alleged victim] was wearing told a different story . . . . The device, which monitors a person's activity and sleep, showed [the victim] was awake and walking around at the time she claimed she was sleeping.").

254. Jessa Schroeder, *Fitbit Fitness Tracker Cracks Connecticut Murder Case*, N.Y. DAILY NEWS (Apr. 24, 2017, 12:25 PM), http://www.nydailynews.com/news/crime/police-solve-connecticut-murder-clues-fitbit-activity-article-1.3094802 [https://perma.cc/ME7B-44CV].

255. *See Google 'Reveals User' Over Gmail Child Abuse Images*, BBC (Aug. 4, 2014), http://www.bbc.com/news/technology-28639628 [https://perma.cc/UQY6-VKS2].

256. J. Freedom du Lac & Ellen Nakashima, *Tim Cook: U.S. Government Wants 'Something We Consider Too Dangerous to Create,'* WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/02/17/apple-ceo-the-u-s-government-wants-something-we-consider-too-dangerous-to-create [https://perma.cc/YK7V-5YBB].

257. Motion to Nolle Prosequi for Good Cause, *supra* note 19, at 1.

258. Ángel González, *Amazon Echo Search Warrant Could Spur New Prosecution Methods, Expert Says*, SEATTLE TIMES (Jan. 3, 2017, 6:00 AM), https://www.seattletimes.com/business/amazon/amazon-echo-search-warrant-could-portend-new-prosecution-methods-expert-says/ [https://perma.cc/6E8B-9Y9M] ("Ryan Calo, a professor at the UW School of Law who specializes in privacy, robotics and cyberlaw issues, says the Bentonville Police Department's fishing expedition is 'unlikely to yield anything.'").

259. *Id.*

260. *Id.*

261. *Id.*

devices would then serve as a bugging device—a microphone in someone's house.[262] A suspect's interactions with a voice-activated device could also corroborate alibis.[263] In addition, these devices could be configured to "listen" for keywords, much like the way Google or Microsoft scan emails or their cloud storage services for images of child abuse.[264] So, a device could listen for not only its wake word, but words that are related to unlawful activity. It could also potentially be configured to listen for a kidnapped person's voice.

II. ADEQUATE PRIVACY PROTECTION FOR USERS OF IN-HOME, CONNECTED DEVICES REQUIRES A TWO-PRONGED APPROACH: ONE FOR COMPANIES, ONE FOR THE GOVERNMENT

Against the backdrop of repeated law enforcement and technology company clashes, devices like the Echo starkly highlight the blurring between two different prongs of privacy: the sanctity of the home[265] and the third-party doctrine.[266] Emails and files like those at issue in Microsoft's recent challenge[267] already muddy the privacy waters, but voice-activated devices throw the inadequacies of existing doctrine into sharp relief. Voice-activated devices are both in the home—a place with the highest expectation of privacy—and share data with third parties—the place with the least expectation of privacy.[268] Some experts suggest

262. *Id.*

263. *Id.*

264. *Google "Reveals User" Over Gmail Child Abuse Images*, *supra* note 255; *Google Terms of Service*, GOOGLE (Apr. 14, 2014), https://www.google.com/intl/en/policies/terms/archive/20131111-20140414/ [https://perma.cc/9P6C-5BHL] ("Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.").

265. Kyllo v. United States, 533 U.S. 27, 40 (2001).

266. *See* California v. Greenwood, 486 U.S. 35, 39–42 (1988); Smith v. Maryland, 442 U.S. 735 (1979) (holding that installing a pen register at the telephone company and using it to learn the telephone numbers called from a private telephone was not a search because the numbers were revealed to a third party).

267. First Amended Complaint, Microsoft Corp. v. U.S. Dep't of Justice, 2016 WL 3381727 (W.D. Wash. June 17, 2016) (No. 2:16-cv-00538-JLR).

268. *See Kyllo*, 533 U.S. at 40; *Greenwood*, 486 U.S. at 39–42; *Smith*, 442 U.S. 735; *Talk to Your Alexa Device*, *supra* note 196.

that bringing devices that transmit data to third parties into the home will normalize privacy intrusions.[269]

Regardless, these devices' dual nature shows the outdated nature of the third-party doctrine—especially when there is a valid warrant, as was the case in Bentonville. Focusing solely on judicial revision of the third-party doctrine ignores cases like Bentonville, where there is a warrant. That warrant could reach vast amounts of data—data generated from the most intimate reaches of the home and shared instantaneously, and perhaps accidentally,[270] with third parties.[271] Accordingly, more than revision of the third-party doctrine is needed. Both the law and technology companies will need to change to best protect user privacy. This Part will recommend technological solutions and legal solutions to give users certainty in their privacy protections and companies guidance.

A. Neither Technical Solutions nor Legal Solutions Alone Are Enough to Ensure Privacy Protections

Technical solutions are needed in addition to legal solutions, because when the hurdle is technical, not legal, privacy protections for users are stronger, and the government is often less able to compel disclosure. A well-known example involves a dispute between Apple and the FBI following the 2015 San Bernardino, California shooting.[276] On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik shot and killed fourteen people and wounded twenty-two others in an attack in San Bernardino, California.[273] The FBI investigated the attack as an act of terrorism because Malik had posted a pledge of allegiance to the Islamic State on his Facebook page.[274] Questions remained whether

---

269. Apeksha Vora, *Amazon's Alexa: Convenience, for the Price of Privacy*, GEO. L.: INST. FOR L. & POL'Y (May 23, 2017), http://www.georgetowntech.org/blogfulltext/2017/5/23/amazons-alexa-convenience-for-the-price-of-privacy [https://perma.cc/9PWY-P64L].

270. Hackett, *supra* note 4.

271. Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU: FREE FUTURE (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/free-future/privacy-threat-always-microphones-amazon-echo [https://perma.cc/X5H3-5YQ2].

272. Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html [https://perma.cc/KH2Z-2TNS].

273. Mark Berman, *One Year After the San Bernardino Attack, Police Offer a Possible Motive as Questions Still Linger*, WASH. POST (Dec. 2, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/12/02/one-year-after-san-bernardino-police-offer-a-possible-motive-as-questions-still-linger/?utm_term=.f9ce483e8b6b [https://perma.cc/6ZD3-5Y2W].

274. *Id.*

anyone else was involved in or knew about the attack, leading to a dispute between the FBI and Apple over Farook's iPhone.[275]

The FBI asked Apple to help it gain access to the shooter's iPhone.[276] The FBI wanted Apple to change the iPhone's software to gain access.[277] This change would circumvent the phone's encryption, allowing the FBI to attempt to guess the password.[278] Normally, after someone tries to guess an iPhone's password ten times, the phone will automatically erase all its data.[279] The FBI wanted Apple to remove the limit on the number of guesses so that the FBI could use brute force to break the phone's password—guessing millions of passwords in an attempt to unlock it—without losing the data.[280] Apple opposed this, calling the FBI's request "an unprecedented step which threatens the security of our customers."[281] Apple's CEO, Tim Cook, reiterated that Apple would comply with warrants and subpoenas, but that changing software would be "too dangerous."[282] Though the Department of Justice received an order from a magistrate judge to unlock the phone, Apple continued to resist.[283] The FBI ultimately hired a hacker to access the phone, so Apple engineers were not needed to revise the software.[284]

The FBI dropped the case, so the question remains open as to whether a technology company can be compelled to create access.[285] The question continues to come up, however; in at least two subsequent cases, the FBI has considered returning to court to force Apple to help unlock an iPhone that belonged to a suspect.[286] Though uncertain, the law could compel companies like Apple or Amazon to modify existing

---

275. *Id.*

276. Nakashima, *supra* note 272.

277. *Id.*

278. *Id.*

279. *Id.*

280. *Id.*

281. du Lac & Nakashima, *supra* note 256 (quoting Apple CEO, Tim Cook).

282. *Id.*

283. Nakashima, *supra* note 272.

284. *See* Don Reisinger, *Apple and the FBI Could Be Headed for Another Locked iPhone Battle*, FORTUNE (Apr. 20, 2016, 10:49 AM), http://fortune.com/2016/10/07/apple-iphone-dahir-adan/ [https://perma.cc/7BT3-NR5S].

285. *Id.* (seeking to unlock the iPhone owned by Dahir Adan, the attacker who stabbed ten people in a Minnesota mall in September 2016); Matt Drange, *Apple Fires Back in New York iPhone Case, Urges Judge to Deny Feds' Appeal For Help*, FORTUNE (Apr. 15, 2016, 06:09 PM), https://www.forbes.com/sites/mattdrange/2016/04/15/apple-fires-back-in-new-york-iphone-case-urges-judge-to-deny-feds-appeal-for-help/#7a493bcd62f9 [https://perma.cc/ZE73-8CD2] (seeking to unlock a phone involved in a New York City drug ring).

286. Reisinger, *supra* note 284.

software, but so far, technical solutions have allowed companies to resist changing their products in response to law enforcement requests. Thus, technical solutions that provide users with a backdrop of protection, coupled with legal protections that recognize the pervasiveness and importance of electronic communications, would give users confidence to bring tools like Alexa into their home.

B. Companies Should "Bake In" Privacy Protections from the Very Conception of Consumer Technologies

Companies could avoid the on-going friction with law enforcement and protect users' privacy by ensuring their devices are technologically incapable of giving law enforcement too much insight into users' data. Because the law can be slow to change, privacy advocates recommend that tech companies advocate on their users' behalf, even if the law frustrates companies' good intentions.[287] Moreover, as the passage of CalECPA shows, many companies want to support strong privacy measures.[288] Therefore, the private sector is likely an effective tool to drive change because it is ready and willing to protect users' privacy.

Some experts see the failure to protect privacy not just as a legal failing, but as technology companies' failure.[289] Investigators are inventive; they have used, and will use, new technologies for recording and tracking,[290] so experts note Amazon's failure to "bake in" privacy to the same extent as other devices.[291] Though Apple has been criticized for privacy issues as well,[292] it occasionally takes a different approach from Amazon. As just one example of a different approach to privacy in

---

287. Andrew Crocker, *When the Law Stands in the Way of Tech Companies Standing Up for Their Users*, ELEC. FRONTIER FOUND. (Jan. 23, 2017), https://www.eff.org/deeplinks/2017/01/when-law-stands-way-tech-companies-standing-their-users [https://perma.cc/R9EZ-KKJ8]; *supra* notes 97–105 (describing Microsoft's case challenging the ECPA).

288. Shahid Buttar, *California Leads the Way in Digital Privacy*, ELEC. FRONTIER FOUND. (Oct. 21, 2015), https://www.eff.org/deeplinks/2015/10/california-leads-way-digital-privacy [https://perma.cc/CHR6-FY3U] ("Companies from Apple, Facebook and Google to Twitter, Adobe and Mozilla all backed the new law.").

289. Daniel R. Stoller, *Amazon Echo Murder Case Is No Apple-FBI Encryption Battle*, BLOOMBERG BNA (Jan. 17, 2017), https://www.bna.com/amazon-echo-murder-n73014449867 [https://perma.cc/TLX2-NUMT].

290. *See supra* notes 246–54 (discussing the use of cartapping, Fitbits, and pacemakers by law enforcement).

291. Stanley, *supra* note 271.

292. *E.g.*, Dave Gershgorn, *Five Privacy and Security Concerns About Apple's New FaceID Facial Recognition*, QUARTZ (Sept. 12, 2017), https://qz.com/1075874/five-privacy-and-security-concerns-about-apples-new-faceid-facial-recognition/ [https://perma.cc/8MPH-88VU] (describing concerns regarding some Apple technology).

action, Siri—Apple's voice assistant—both anonymizes and encrypts voice data.[293] Amazon's Alexa does not anonymize data.[294]

Experts point to both Amazon's storage of conversations and the linking of those conversations to customers as privacy concerns that Amazon should have thought through before releasing Alexa to the public.[295] A second concern noted by experts is technology companies' lack of transparency. Companies should tell users about the requirements for, and disclosure of, their data.[296] But other privacy advocates note that this lack of transparency is not companies' fault;[297] federal law often prevents technology companies from disclosing to users when their data is requested.[298] As discussed in section I.B.2, Microsoft has challenged this provision of the law because it wants to disclose to users when law enforcement requests this data.[299] So, lack of notice to users remains an issue, not only from the technology company but from the government as well.[300] In short, experts have faulted companies for not imagining the ways that users' privacy could be impacted by their new products.

Similarly, experts have criticized Amazon for failing to think through the implications of the Echo and other Alexa-enabled devices from the very beginning of the devices' creation.[301] Amazon could have avoided its recent fight with the Bentonville Police Department from the outset by making technological changes to its product, like anonymizing data.[302] In contrast to the Apple cases, the Bentonville case presents a legal question, not a technical one.[303] The Bentonville Police Department did not need Amazon's help unlocking data stored inside a specific Echo (the data were on its servers the entire time), but the FBI did need

293. *See* Stoller, *supra* note 289.

294. *Id.*

295. Stanley, *supra* note 271.

296. *Id.*

297. *See, e.g.*, Alex Abdo, *Why We're Supporting Microsoft's Challenge to Secret Surveillance*, ACLU: FREE FUTURE (May 26, 2016 10:45 AM), https://www.aclu.org/blog/free-future/why-were-supporting-microsofts-challenge-secret-surveillance [https://perma.cc/L5YL-EYAV] (describing the government's limits on notice to users); Crocker, *supra* note 287 (describing "gag orders" which limit notice to users).

298. 18 U.S.C. § 2705(b) (2012).

299. First Amended Complaint, Microsoft Corp. v. U.S. Dep't of Justice, 2016 WL 3381727 (W.D. Wash. June 17, 2016) (No. 2:16-cv-00538-JLR).

300. *See* Abdo, *supra* note 297.

301. *See* Stanley, *supra* note 271.

302. *See* Stoller, *supra* note 289.

303. *Id.*

Apple's help to unlock an iPhone.[304] In other words, the barrier to Apple's compliance was both legal and technical, while the barrier to Amazon's compliance was solely legal. Thus, at least some of the privacy concerns can be alleviated by technical changes to the Echo device.

Technical changes would help to ensure stronger privacy protections for users. In addition, technical changes would give users more control over and transparency regarding what is done with their data. These changes could include the following: (1) shortening data retention periods; (2) providing notice to consumers when law enforcement requests their data; (3) establishing obvious cues that devices are recording; (4) engineering protections against turning in-home recording devices into bugs; (5) storing as much data as possible on the device, not in the cloud; and (6) enshrining the company's commitment to never scanning for offensive keywords and concepts, or terms related to illegal activity, in its terms of service.

First, technology companies should shorten the period they retain recordings. Shortening retention would decrease the amount of data available to law enforcement.[305] For example, Amazon retains recordings until users delete them.[306] In contrast, Apple retains data from its voice assistant for up to two years, and most of that time the data is anonymized.[307] Amazon could do something similar and retain recordings of Alexa requests for a limited time.[308] If Amazon wanted to use the recordings to improve Alexa's performance, it could also anonymize the data after six months, or a similar period of time.[309]

Second, companies, whenever possible, could give users clear notice regarding what is happening with their recordings. Users could be clearly notified about what happens to their data and recordings when they buy the device, in the way that California mandates for smart

304. *Id.*

305. Donohue, *supra* note 164, at 663.

306. *See* Stanley, *supra* note 271.

307. Robert McMillan, *Apple Finally Reveals How Long Siri Keeps Your Data*, WIRED (Apr. 19, 2013, 6:30 AM), https://www.wired.com/2013/04/siri-two-years/ [https://perma.cc/P6YM-73F4] ("Once the voice recording is six months old, Apple 'disassociates' your user number from the clip, deleting the number from the voice file. But it keeps these disassociated files for up to 18 more months for testing and product improvement purposes."); *Our Approach to Privacy*, APPLE, https://www.apple.com/privacy/approach-to-privacy/ [https://perma.cc/DBR9-CC53].

308. *Our Approach to Privacy*, *supra* note 307.

309. *E.g.*, McMillan, *supra* note 307 (describing how Apple anonymizes data after a period of time, then deletes the data).

TVs.[310] Users could again be notified when they first use the device and when law enforcement requests users' data.[311] As Microsoft's recent litigation regarding secrecy orders demonstrates, the ability to notify users is not assured.[312] But in cases where technology companies are not under a secrecy order, they could notify users of requests for their data to maintain transparency.

Third, devices could have obvious visual indicators regarding collection and transmission of data. Similar to giving users notice, indicators that the device is activated gives users more control over their privacy. The device's hardware could clearly indicate when the device is recording.[313] For example the Echo device lights up when it is recording.[314] Then, a separate cue, such as a different colored light, would show that the device is transmitting that recording.[315] And when a user wants the device to stop recording, there could be a way on the hardware to do that—not just a software switch.[316] The goal of including hardware indicators and switches is to give users certainty and control over the device's recordings, in the way that a user might put a sticker over a laptop's camera,[317] unplug a smart TV, or mute an Echo.[318]

Fourth, companies should make remote conversion of devices technically impossible—or as close to that as possible.[319] For example, experts worry that the Echo could be "switched on" to become a remote-accessed recording device without the user's consent.[320] Just as iPhones do not come enabled with software to circumvent their encryption,[321] other devices should be similarly protected. Thus, Amazon might restrict the use of their Alexa technology to devices that can not be "back-doored" or turned into truly always-on devices. Accordingly, both the

---

310. CAL. BUS. & PROF. CODE § 22948.20 (West 2016).

311. Stanley, *supra* note 271.

312. First Amended Complaint, Microsoft Corp. v. U.S. Dep't of Justice, 2016 WL 3381727 (W.D. Wash. June 17, 2016) (No. 2:16-cv-00538-JLR); Smith, *supra* note 101.

313. Stanley, *supra* note 271.

314. *See, e.g.*, *About the Light Ring*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201601790 [https://perma.cc/JT8U-Q8T3] (describing the light that appears when Alexa is "listening").

315. Stanley, *supra* note 271.

316. *Id.*

317. *Id.*

318. *Hardware Basics: Echo (1st Generation)*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201549580 [https://perma.cc/WY56-5VF3].

319. *See* Stanley, *supra* note 271.

320. González, *supra* note 258.

321. *See* Nakashima, *supra* note 272.

device itself should be secure and the transmissions should be secured with strong encryption.

Fifth, as much processing as possible should be done on the device itself—not in the cloud.[322] As long as the third-party doctrine is still in place, sending data to companies who store it on the cloud erodes users' privacy.[323] Additionally, tech companies should encrypt data on the device as well.[324] For example, Apple avoided creating software for the FBI to access locally stored information.[325] If that information was stored on the cloud, then it would have been accessible under the third-party doctrine. Because the law has struggled to keep pace with technology's changes, companies have a heightened responsibility to protect users' privacy themselves.

Lastly, companies should modify the terms of service to protect users' privacy. By committing to never perform constant monitoring for keywords—whether offensive or related to illegal activity—in the terms of service, companies would give users more certainty regarding their information and more clarity about what happens to that information.[326]

In sum, while no company is a completely perfect example of privacy protections, the steps each company has taken so far demonstrates that privacy and business goals are not at odds.

C. CalECPA Is a Step in the Right Direction, and Other States Should Follow Suit

Given the disputes between law enforcement and technology companies, lawmakers should provide citizens, living in an increasingly digital world, with more clarity regarding their legal privacy protections. State legislators have started responding to concerns about privacy for electronic communications more quickly and comprehensively than

---

322. Stanley, *supra* note 271; STACEY GRAY, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/9UZV-MB7K].

323. GRAY, *supra* note 322.

324. Aaron Allsbrook, *Five Easy Ways to Build Security Into the Internet of Things*, FORBES TECH. COUNCIL (Nov. 23, 2016, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2016/11/23/five-easy-ways-to-build-security-into-the-internet-of-things/#25b89f1e6aff [https://perma.cc/4CFX-QBCD].

325. Nakashima, *supra* note 272.

326. There is of course value in law enforcement being able to listen in on conversations, especially when the target and duration of the listening are appropriately described in a warrant. This suggestion deals with long-term, undifferentiated monitoring that is not limited in duration or to a specific target.

federal lawmakers.[327] For example, California enacted its law on smart TVs before CalECPA.[328] But state legislatures are reacting to headlines: California passed the law on smart TVs in response to headlines regarding eavesdropping TVs,[329] while other states moved to protect users' private information from being sold after Congress repealed FCC's ban on selling users' data without consent.[330] But instead of reacting to the news cycle, states should look forward.

Experts have celebrated California and CalECPA as the pinnacle of this forward-looking response. Other state legislatures should follow suit, and adopt flexible, forward-looking, CalECPA-like schemes. CalECPA stops overly broad warrants, thereby preventing "fishing expeditions that violate the spirit, if not the letter, of the Fourth Amendment."[331] Importantly, CalECPA also uses "technologically neutral language,"[332] which ensures that users who adopt any new technologies are protected.[333] In short, the momentum generated by attention-grabbing headlines can be used by state legislatures to enact CalECPA-like statutes. The public's support for privacy protection exists,[334] and states should use that support to draft forward-looking statutes that anticipate new technologies.

Experts suggest that eavesdropping statutes could serve as a framework for new privacy protections.[335] As discussed above, a problem with current eavesdropping statutes is that they turn on consent.[336] When a person consents to a recording, they no longer have a privacy interest in that recording, and it can be shared widely.[337] But most devices owners are considered to have consented to the device's

---

327. *See, e.g.*, Conor Dougherty, *Push for Internet Privacy Rules Moves to State Houses*, N.Y. TIMES (Mar. 26, 2017), https://www.nytimes.com/2017/03/26/technology/internet-privacy-state-legislation-illinois.html [https://perma.cc/YMM8-VBCT] (noting that many state legislatures have introduced privacy legislation).

328. *See supra* section I.A.3.

329. Lazarus, *supra* note 117 ("[W]e should look next to a ban on data from all in-home smart appliances being used for advertising purposes.").

330. *See supra* notes 153–57.

331. Freiwald, *supra* note 124, at 21.

332. *Id.* at 17.

333. *See* CAL. PENAL CODE § 1546 (West 2017).

334. Joseph O'Sullivan, *Washington State Lawmakers Move to Secure Internet Privacy After Changes to Federal Law*, SEATTLE TIMES (Apr. 5, 2017, 7:52 PM), http://www.seattletimes.com/seattle-news/politics/state-lawmakers-move-to-secure-internet-privacy-after-changes-to-federal-law/ [https://perma.cc/2K49-QJYG].

335. DeNisco, *supra* note 175.

336. *See supra* section I.B.3.

337. *See supra* notes 173–78.

listening, meaning that they have little protection for their privacy interests in the recordings.[338] Experts fear that many users do not understand that using the device means they consent to the recordings.[339] Accordingly, legislators should step in to protect users' privacy. Under CalECPA, Amazon would be a service provider, and the recordings, electronic communications.[340] Thus, the recordings would receive privacy protections, including requiring a warrant to access.[341] Similarly, CalECPA requires notice to users when law enforcement requests their data, giving users more transparency regarding their data.[342]

Though the Supreme Court may seem like the most effective venue for change to the third-party doctrine,[343] the Court is necessarily reactive, and not forward-looking as is required to address these problems.[344] First, Supreme Court holdings tend to be narrow in the Fourth Amendment context,[345] unlike the broad protection provided by CalECPA.[346] Second, upcoming cases regarding cell-site location data are tempting vehicles for third-party doctrine reform,[347] but those holdings will likely rest on narrower grounds.[348]

In sum, lawmakers should recognize that sharing digital information with third parties is a near-necessity of modern life, and new laws should ensure that this sharing does not erode users' expectations of privacy. Moreover, laws should anticipate that technology will change, and not simply react to the latest device that makes headlines. Providing background rules will benefit both companies and users: users will feel comfortable knowing their recordings are protected by heightened

338. *See supra* notes 173–78.

339. DeNisco, *supra* note 175.

340. *See supra* notes 124–41.

341. *Id.*

342. *See supra* section I.A.3.

343. *See* Note, *supra* 169, at 1942.

344. *See id.* at 1943 ("It is interesting to note that *Katz*, and by extension *Smith*, came out of a needed response to shifting technology and social norms.").

345. City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Prudence counsels caution before the facts in the instant case are used to establish far-reaching . . . privacy expectations . . . .").

346. CalECPA, CAL. PENAL CODE § 1546 (West 2017).

347. *See* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, __ U.S. __, 137 S. Ct. 221 (2017).

348. *E.g.*, United States v. Jones, 565 U.S. 400, 412–13 (2012) (holding that placing a GPS device on a Jeep is a trespass and thus a search under the Fourth Amendment but leaving "vexing problems" of non-trespassing searches for a later time).

warrant standards, and companies will then benefit from increased consumer confidence.

CONCLUSION

Federal laws and jurisprudence regarding digital privacy have not responded fast enough to changing technologies.[349] And though state legislatures have moved faster than either courts or Congress, they tend not to be proactive.[350] Thus, a two-pronged approach is needed: companies should engineer privacy into their devices,[351] while legislatures should legislate to ensure electronic communications stored with technology companies are properly protected.[352] CalECPA provides a model for the type of flexible, forward-looking statute needed.[353] Building on the momentum of support for privacy legislation prompted by recent congressional action, other states should adopt their own CalECPA-like statutes, taking into account CalECPA's (few) failings.[354] Tech users should look to their states to protect privacy, as many states have already-heightened protections and could continue to take the lead in this area.

---

349. *See id.* at 417 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited 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." (citations omitted)); Vesalga, *supra* note 102, at 460 ("[The ECPA] fail[s] to consistently protect the geolocational data associated with electronic communications").

350. *E.g.*, CAL. BUS. & PROF. CODE §§ 22,948.20–22,948.25 (West 2016) (California's connected TV law).

351. Stanley, *supra* note 271.

352. *See supra* section II.B.

353. *See supra* section I.A.3.

354. *See supra* section II.B.