The Change Needed to Protect Consumer Privacy from "Always On" Devices

JESSICA CHAN*

I. INTRODUCTION

The growing number of "always on" devices that surreptitiously record the communications of consumers creates the need for federal legislation to protect consumer privacy interests affected. The risk posed to a user's privacy rights stemming from the use of always on devices in the home has already begun to increase. The government has already gained access to the data collected by always on devices without the consent of the user. In an Arkansas murder case, the prosecutor sought recordings of the defendant's Amazon Echo smart speaker as evidence in the case.[1] Amazon partially complied with a warrant, turning over information from the always on device.[2] Amazon's compliance is just one example of the government's ability to gain access to a user's personal data without their consent.

I propose that Congress first investigate the techniques used for data collection, the amount and type of data collected, the extent to which this data is stored, the ways that this data is used, and the current safeguards and security measures being implemented by companies. Second, I propose that Congress pass a new law requiring all providers of always on devices to publically disclose their practices. Congress' comprehensive investigation and new law will create transparency in this developing industry and reduce abuses of personal data, such as unlawful surveillance and unauthorized access and use by third parties, which includes data being sold and sensitive data being accessed by hackers due to insufficient security measures. It could also spur more legislation at the federal and state levels, inform consumer lawsuits and agency actions, promote healthy consumer choice, and motivate industry standards for protecting consumers' personal data.

Part II of this article provides an overview of the most prominent always on devices currently on the market and their functionality. Part III describes how limited the current laws are in regulating these devices to the protect consumer privacy. Part IV describes my proposal for a comprehensive investigation by Congress and a new law that are both needed to regulate this new market of always on devices. It explains how the proposal will better

*Jessica Chan earned her J.D. from the University of San Francisco in December 2017. She is currently pursuing a LL.M. in Intellectual Property and Privacy Law from the University of Houston Law Center, expecting to complete the program in December 2018. In 2011, Jessica graduated from the University of Houston, C.T. Bauer College of Business with a Bachelors in Business Administration, *Cum Laude*.

1. Brian Heater, *After pushing back, Amazon hands over Echo data in Arkansas murder case*, TECHCRUNCH (Mar. 7, 2017), https://techcrunch.com/2017/03/07/amazon-echo-murder/.

2. *Id.*

protect consumer privacy than the current framework. Lastly, Part V will discuss issues that would Congress would still need to address even if it adopted my proposals.

II. BACKGROUND: ALWAYS ON DEVICES AND THEIR THREAT TO PRIVACY

Questions regarding the vulnerability of consumer privacy have arisen due to the quickly expanding market of always on devices.[3] The increase in privacy concerns stems from the incorporation of speech recognition technology, which allows device providers to collect, store, analyze, and share abundant amounts of personal data. The unknown risk to a user's privacy and possible government surveillance place a chilling effect cast over otherwise freewheeling private conversations. For example, users having a private dinner conversations within their home discussing possible political disasters may become fearful that their discussions could be recorded and used out of context against them. The following describes a few of the most popular always on devices currently on the market.

1. HOME PERSONAL ASSISTANTS

Home personal assistants use Wi-Fi to sync with other devices and answer everyday inquiries and automate simple tasks, such as turning on the living room lights or locking the front door.[4] Once configured, personal assistant devices sit dormant—listening for trigger words—also known as wake words, to activate.[5] For example, the Amazon Echo sits dormant until it hears the trigger word, "Alexa."[6] Only then will the device listen for a voice command and execute the request.[7] The device uploads the audio, including the fraction of a second before the trigger word ("Alexa"), to the cloud, where Amazon's software identifies the command and responds accordingly.[8] The Amazon Echo also includes a manual switch that allows the microphone in the device to be turned off, but it will still respond to commands made with the device's remote microphone control.[9]

---

3. Stacy Gray, *Always On: Implication of Microphone-Enable Devices*, FUTURE OF PRIVACY FORUM (Apr. 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

4. Eliott C. McLaughlin, *Alexa, What Other Devices Are Listening to Me?*, CNN (Jan. 12, 2017, 5:45 PM),
http://www.cnn.com/2017/01/12/tech/voice-technology-internet-of-things-privacy/.

5. Jay Stanley, *The Privacy Threat From Always-On Microphones Like the Amazon Echo*, AMERICAN CIVIL LIBERTIES UNION (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/free-future/privacy-threat-always-microphones-amazon-echo.

6. *What is Amazon Echo*, AMAZON, http://www.amazon.com/dp/B00X4WHP5E (last visited July 18, 2017).

7. *See, e.g.*, *id.*

8. *Alexa and Amazon Echo FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (last visited July 16, 2017).

9. *Id.*

2. PHONES, TABLETS, LAPTOPS

Many phones, tablets, and laptops incorporate software that allow consumers to query information. These types of always on devices provide an array of functions, including translating spoken word to text and initiating Internet searches.[10] Their software includes Apple's Siri, Microsoft Cortana, and Motorola X, which all use voice recognition.[11]

3. SMART TVS

Internet-enabled Smart TVs provide various functions, such as allowing users to stream Netflix or update Facebook on the same screen as they view their favorite shows.[12] Many of these televisions are equipped with a voice-controlled search function.[13] The most popular Smart TVs currently on the market are LG, Panasonic, Samsung, Sharp, Sony, and Vizio.[14] The leading provider of Smart TVs is Samsung.[15] Samsung's Smart TV software responds to commands in two different ways.[16] In one way of voice processing, users may use their voices to make simple predetermined TV commands (e.g. changing the channel and volume), which are processed locally at the TV rather than in the cloud.[17] Privacy concerns arise from the second type of voice processing, which involves more complex voice commands (e.g. asking for movie recommendations).[18] These complex voice commands require data to be sent offsite to a third party for processing (currently, Nuance Communications, Inc.).[19] When this voice recognition feature is enabled, all spoken words said within the location of the Samsung SmartTV are recorded and transmitted over the Internet.[20] Consumers should be concerned about this transmission of data because the communications recorded and transmitted include sensitive personal data, such as the commands themselves, information about the user's device (e.g. device identifiers and IP address), associated text, videos watched, applications and content accessed, any requested transactions (e.g. renting or buying videos), and any additional spoken words, including personal and sensitive information.[21] By using always on devices like the Samsung SmartTV,

10. *See, e.g.,* McLaughlin, *supra* note 4.
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.*
15. Samsung "SmartTV" Complaint, Electronic Privacy Information Center, https://epic.org/privacy/internet/ftc/samsung/ (last visited July 16, 2017).
16. Natasha Lomas, *Samsung Edits Orwellian Clause Out Of TV Privacy Policy*, TechCrunch (Feb. 10, 2015), https://techcrunch.com/2015/02/10/smarttv-privacy/#.puzvmzo:yfMB.
17. *Id.*
18. *Id.*
19. *Id.*
20. Electronic Privacy Information Center, *supra* note 15.
21. *Id.*

consumers place their privacy rights at risk by allowing third party access to their personal data.

4. TOYS

Interactive always on toys include Hello Barbie, My Friend Cayla, and I-Que Intelligent Robot, all of which pose privacy implications for the users of these devices who are generally children.[22] A widely known interactive toy on the market is Hello Barbie. When a user (child) presses the button on her belt buckle, Barbie records what is said and transmits the data to the cloud.[23] The data is then saved allowing Barbie to continuously learn about the user and tailor her responses.[24] The Wifi connected doll imposes implications on the privacy of children by allowing providers access to a user's (child's) personal information, including their preferences and spoken words to the doll.[25]

When using always on devices, users and parents' of users need to be concerned with the risks posed to children's privacy rights because "[p]arents cannot reasonably review all the information that these 'always on' devices are collecting from children," or know how the information is being used by device providers.[26] Insufficient security safeguards provide hackers with potential interactive access to any child or adult who is in proximity to the toy. The data collected and stored can be compromised to allow unauthorized access to sensitive information leading to identify theft, fraud and hackers finding out the location of a user's house or business. "As the 2015 data breach of Vtech's InnoTab Max uncovered, hackers specifically target kids because they offer clean credit histories and unused Social Security numbers . . . [are good] for identity theft."[27] These toys also collect a lot of information about users' children, and it is unclear what the companies do with the extraneous "noise" they pick up.[28] The users' information is subpoenaed; the user might have to hand it over.[29] For example, if a user jokes about terrorism or illegal activity and an investigation is conducted into these activities, always on device providers could hand over any information collected by these devices.[30]

22. McLaughlin, *supra* note 4.

23. Katie Lobosco, *Talking Barbie is too 'creepy' for some parents*, CNN (Mar. 12, 2015, 4:11 PM), http://money.cnn.com/2015/03/11/news/companies/creepy-hello-barbie/.

24. *Id.*

25. Gray, *supra* note 3.

26. Kate Cox, *All Those Smart Devices That Listen To Your House May Be Unlawfully Violating Kids' Privacy*, CONSUMERIST (May 26, 2016, 11:20 AM), https://consumerist.com/2016/05/26/all-those-smart-devices-that-listen-to-your-house-may-be-unlawfully-violating-kids-privacy/.

27. Caroline Knorr, *Why you should protect your child's online privacy*, CNN (June 7, 2017, 5:29 AM), http://www.cnn.com/2017/06/07/health/parents-children-online-privacy-partner/index.html.

28. *Id.*

29. *Id.*

30. *Id.*

III. CURRENT LAWS AND THEIR LIMITATIONS

The increasing popularity of always on devices has raised the legal question of whether the collection and use personal data by these devices should be regulated or even permitted altogether. The following describes how current laws regulating this developing market do not adequately protect consumer privacy interests.

A. FOURTH AMENDMENT

1. Protections Regarding Always On Devices

The Fourth Amendment protects against unreasonable searches and seizures of "persons, houses, papers, and effects by the government or private parties acting as an agent for the government."[31] Fourth Amendment protection covers intangible media, such as oral communications, which includes digital data of conversations collected by always on devices.[32]

Protection extends only to those areas where an individual has a legitimate expectation of privacy. *Katz v. United States* establishes the standard for reasonable expectation of privacy, which has two components: (1) the person must have an actual subjective expectation of privacy; and (2) the person's subjective expectation must be one that society deems reasonable.[33] When the Fourth Amendment applies, the government must obtain a warrant or be subject to an exception to that requirement prior to any search or seizure.[34]

Users of always on devices satisfy the two-part test to warrant a reasonable expectation of privacy as set forth in *Katz*. "What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection."[35] "But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[36] Users of always on devices have a subjective expectation of privacy in their spoken words because they do not expect the government to use their home devices to listen to their conversations at home. If a person knows he will be searched, he cannot claim that he expected privacy. Subjective expectation of privacy may be eliminated if a user agrees to terms of service or a privacy policy that discloses collection practices and distribution practices to third parties, including government entities.

Additionally, users' expectation of privacy is also objectively reasonable because of the prevalent idea that people are free from the uninvited ears of the government within their own homes.[37] Therefore, the

31. U.S. CONST. amend. IV.
32. Katz v. United States, 389 U.S. 347, 353 (1967).
33. *Id*. at 361.
34. *Id.*
35. *Id*. at 351.
36. *Id.*
37. Kyllo v. United States, 533 U.S. 27, 31 (2001).

Fourth Amendment protects personal data transmitted and stored by always on devices.

The Supreme Court has treated privacy within the home as protected under the Fourth Amendment.[38] In *Kyllo v. United States*, the Court stated that, "'[a]t the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[39] Justice Scalia emphasized that the scan from the thermal imaging device constituted a search under the Fourth Amendment.[40] The scan showed that Kyllo's garage roof and side wall were relatively hot, compared to the rest of his home and the neighboring units, and thus, could inform the police "at what hour each night the lady of the house takes her daily sauna and bath . . . ."[41] Similarly, always on devices can overhear intimate and private communications and activities within the home. Therefore, the interception of data transmitted and stored by these devices should similarly constitute a search and warrant protection under the Fourth Amendment.

However, the Supreme Court has yet to address the application of the Fourth Amendment to the use of always on devices. *United States v. Warshak*, does however, provide guidance on the Sixth Circuit Court's application of *Katz's* reasonable expectation of privacy test to government demands for personal data collected and stored by internet services.[42] In *Warshak*, the government used a court order, instead of a warrant, under the Stored Communications Act (SCA)[43] to compel an Internet service provider (ISP) to turnover emails containing information regarding Warshak's business and personal life.[44]

The court held that users have a reasonable expectation of privacy in their emails and extended Fourth Amendment protection to stored e-mails.[45] The *Katz* court found that e-mail serves a similar and as important role in modern communication as the telephone.[46] The court reasoned that e-mail has substituted for other forms of communications, including telephone calls, face-to-face conversations and mailed letters, which "society clearly views as private."[47] Because society expects privacy in these more traditional forms of communication, users should be entitled to expect the same level of protection regarding their privacy in e-mail.[48] The court found that the defendant manifested a subjective expectation that his emails would not be

38. *Id.* (quoting Silverman v. United States, 365 U.S. 505, 511 (1961).

39. *Id.*

40. *Id.* at 38.

41. Kyllo*,* 533 U.S. at 38.

42. U.S. v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).

43. 18 U.S.C. §§ 2701-2712 (2015); *Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

44. Warshak, 631 F.3d at 282-83.

45. *Id.* at 288.

46. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEG. F. 121, 138 (2008).

47. Bellia & Freiwald, *supra* note 46, at 138.

48. *Id.*

scrutinized due to the "sensitive and sometimes damning substance of emails."[49] Since e-mails contain sensitive and private information, government surveillance of e-mails is as intrusive as surveillance of other forms of communication.

Similar to the information contained in e-mails and scans conducted by thermal imaging devices, the data collected from always on devices should not be accessible by law enforcement agents without a warrant under the Fourth Amendment because of the intimate and possibly "damning" information contained in the data.[50] Always on devices have the ability to record, transmit, and store private communications and activities within the home, despite users' subjective and objectively reasonable expectation that this data will remain private and not be subject to warrantless government surveillance. Denying this protection would be destructive of society's ability to communicate, and it would create a disincentive to use new communications technologies.

2. Legal Limits of Protection

a. Third-Party Doctrine

Protection provided by the Fourth Amendment is limited due to the availability of the third-party doctrine. The third party doctrine gives the government a right to compel the disclosure of a user's data when third parties hold it in the ordinary course of their business, and the information has been voluntarily shared with third party businesses.[51] In *United States v. Miller*, the Court held that the government's use of a subpoena to obtain the defendant's bank records did not violate the Fourth Amendment because "[a]ll of the documents obtained, including financial statements and deposit slips, contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[52]

In recent cases, federal appellate courts have held that the defendants lacked a reasonable expectation of privacy in cell phone location data because of the third-party doctrine.[53] The most recent Sixth Circuit case, *U.S. v. Carpenter*, held that the government did not conduct a "search" for Fourth Amendment purposes when it obtained business records from defendants' wireless carriers for cell phone service, in which contained cell tower locational data.[54] The court reasoned that these records do not fall under the Fourth Amendment because they say nothing about the content of any calls and only include routing information, which the wireless providers gathered in the ordinary course of business.[55] Tracking their customers' phones across different cell-site sectors is necessary to connect their customers' calls, and

49. Warshak, 631 F.3d at 284.
50. *Id.*
51. United States v. Miller, 425 U.S. 435, 442-43 (1976).
52. *Id.* at 437-442.
53. United States v. Graham, 824 F.3d 421, 424-425 (4th Cir. 2016).
54. United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016).
55. *Id.* at 887.

the maintenance of those records are necessary to identify weak spots in their networks and to determine whether certain charges apply.[56] Thus, the cell-site data are information that facilitate personal communications, rather than part of the content of the communications themselves.[57]

Thus, the holdings in *Miller*, *Davis*, *Graham,* and *Carpenter* articulate that the third-party doctrine eliminates a person's reasonable expectation of privacy when (1) information is voluntarily disclosed (2) for use by a third party (3) in its normal course of business.[58] The third-party doctrine may limit Fourth Amendment protection in allowing government compulsion of personal data collected by always on devices. The devices obtain data when a user voluntarily shares the data with the third-party provider through the use of device, which the courts may find as part of the normal course of business, and thus within the exception.

However, the information collected by always on devices may not fall within the third-party doctrine because the data collected more closely resembles the e-mails in *Warshak.*[59] The data collected exposes the contents of the communications and activities recorded within the home and are not merely numbers or metadata (e.g. cell-site data, mailing addresses, phone numbers, or IP addresses) which are collected in the ordinary course of business.

B. ELECTRONIC PRIVACY COMMUNICATION ACT

The Electronic Communications Privacy Act (ECPA) of 1986 incorporates two acts that regulate the data collection practices used by always on devices: (1) the Wiretap Act, which prohibits some inceptions of data,[60] and (2) the SCA, which regulates the government seizure of stored data.[61]

1. Wiretap Act

a. Private Cause of Action for Violation of ECPA

The Wiretap Act prohibits persons from "intentionally intercept[ing] . . . any wire, oral, or electronic communication" unless either the person intercepting the communication is also a party to the communication or if one party to the communication consented prior to the recording.[62] To make out a prima facie case, the plaintiff must show that the defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device."[63] ECPA defines "electronic

56. *Id.*
57. *Id.*
58. Graham, 824 F.3d at 426, 427.
59. Warshak, 631 F.3d at 282.
60. 18 U.S.C. § 2510 (2002).
61. 18 U.S.C. §§ 2701-12 (2015).
62. 18 U.S.C. § 2511(1)(a)–(2)(d) (2012).
63. *Id*. at § 2511(1)(a).

communication services" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[64]

Interception is the "aural or other acquisition of the contents of wire, electronic or oral communication by electronic or mechanical or other device."[65] Law enforcement may intercept communications collected by always on devices by gaining access to the microphones within these devices through compelling providers for permission to access their networks or by wiring the devices themselves. By gaining access to always on devices, law enforcement would have the ability to intercept the communications recorded by these devices as they are being transmitted to providers' servers. Interception of data collected from always on devices would violate the Wiretap Act if providers do not obtain consent from users, possess a warrant, or fall within another exception. However, protection provided by the Wiretap Act is weak because exceptions under this act provide strong defenses always on device providers.

b. Legal Limits of Protection

i. Ordinary Course of Business Exception

The Wiretap Act contains an exception often referred to as the ordinary course of business exception for the monitoring of communications carried out by certain types of telephone equipment or providers of electronic communication and done in the ordinary course of business.[66] Providers of always on devices may fall within the business exception if they can provide evidence that the communications collected are required for the functionality of the device and that the storage of the data is necessary for quality control checks or improving upon their services. However, it remains unknown if providers of always on devices fall within the exception because they have yet to disclose the reasons their use of communications collected and stored from these devices. If the data collected and stored are not necessary for the ordinary course of business, e.g. like in Google's course of business, providers will not fall within the scope of this exception and could be in violation of the Wiretap Act.

ii. The Consent Exception

Companies facing suits have a strong defense under ECPA's single party consent exception by arguing that the company itself consented to the recording as a party to the communication.[67] If either party to the communication consents to its interception, then there is no violation of the Wiretap Act.[68] *In re Doubleclick Inc. Privacy Litigation* was one of the first cases brought by private plaintiffs for a violation of ECPA.[69] The plaintiff class claimed DoubleClick, a targeted advertising company, violated ECPA

64. 18 U.S.C. § 2510(15).
65. 18 U.S.C. § 2510(4) (2002).
66. *Id.* at § 2510(5).
67. *See* 18 U.S.C.A. § 2701(c)(2) (Westlaw 2015).
68. 18 U.S.C. § 2511(2)(d) (2012).
69. *See* In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 510-12 (S.D.N.Y. 2001).

when it placed its users' cookies, which were designed to collect and return information about the users, on hard drives of internet users.[70] The court held that Doubleclick did not violate ECPA because Doubleclick tracked consumers only when they visited sites affiliated with Doubleclick.[71] The court reasoned that one of the parties of the tracked communication, the affiliated website, consented to the use of cookies when it chose to utilize Doubleclick's services.[72] Therefore, the actions by Doubleclick fell within the consent exception to the Wiretap Act, which applies when one party to a communication consents to a third-party's access.[73] Accordingly, the exception under ECPA would allow providers of always on devices to consent to the collection of data recorded from these devices without the consent from their users. Therefore, the federally provided protection is greatly limited and provides little protection for users of always on devices to the extent that what is intercepted is considered a communication with the provider.

iii. Consent by Contract

The Wiretap Act protection remains weak because providers of always on devices can likely establish that the user consented to the interception of data by consenting to the privacy policy or terms of service before using the product. In most recent cases brought under the Wiretap Act, the courts dismissed claims where defendants were able to show that the user consented to the wiretapping or that the interception is required to provide the service.[74]

Recently, courts have recently placed stricter standards for establishing explicit consent. For example, in a lawsuit against Google, the plaintiff alleged that the scanning and analysis of the contents of their emails for the purpose of building user profiles and selling advertisements was a violation of the Wiretap Act.[75] The court held that the terms of service "did not explicitly notify plaintiffs that Google would intercept users' emails for the purposes of creating user profiles or providing targeted advertising."[76] Section 8 of the Terms of Service suggests that content may be intercepted for a different purpose, to exclude objectionable content, such as sexual material.[77] Therefore, the court held that the Terms of Service establishes consent to interceptions only for the purpose of eliminating objectionable content.[78] Similar to Google, providers of always on devices may be failing to collect explicit consent from users by not clearly disclosing their data collection practices in their terms of service and privacy policies.

---

70. *Id.* at 500, 507.

71. In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d at 504, 513.

72. *Id.* at 510.

73. *See* 18 U.S.C.A. § 2701(c)(2) (Westlaw 2015).

74. *See* In re Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *17 (N.D. Cal. Sept. 26, 2013).

75. In re Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *12.

76. *Id.* at *13.

77. *Id.*

78. *Id.*

Privacy policies for always on devices remain broad and allow providers to distribute data collected and stored to third parties, including law enforcement agencies and their affiliates. For example, Google's privacy policy explains that a user's personal information may be provided "to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures."[79] In another example, Amazon's Alexa policy says voice recordings and other information is used to "answer your questions, fulfill your requests, and improve your experience and our services."[80] In addition, Amazon warns it may turn over data if requested by a legal entity or to protect the rights, property, or safety of Amazon.com, Amazon's users, or others.[81] Users of always on devices need to be concerned with the authority granted to providers through these policies. Users should be concerned with whether their data can be stored and where such information may be distributed.

iv. State Consent Statutes

Users of always on devices have stronger privacy protection in California and eleven other states as they require both parties to consent to the interception of confidential communications. The California Invasion of Privacy Act ("CIPA"), for example, prohibits the interception of any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation.[82] The statute defines confidential communications as conversations in which one of the parties has an objectively reasonable expectation that no one is eavesdropping.[83]

In addition, "CalECPA requires warrants for more investigations; its warrants impose more restrictive requirements; it provides more notice to targets; and it furnishes more significant remedies" than federal ECPA.[84] CalECPA requires the government to obtain a warrant prior to the seizure of metadata, examples of which might be telephone numbers dialed and address information, in real time. ECPA, by contrast, only requires a court order based on the relevance of the investigation, which has a lower threshold requirement to satisfy than acquiring a warrant.[85] CalECPA also requires specific consent, which must be "provided directly to the government entity seeking information."[86] Therefore, in California, the government cannot compel providers of always on devices to disclose information by relying on

79. *Google's Privacy* Policy, GOOGLE, https://www.google.com/policies/privacy/.

80. *Alexa Terms of Use*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740.

81. *Id.*

82. CAL. PENAL CODE § 632.7 (West 2015).

83. Coulter v. Bank of America, 28 Cal. App. 4th 923, 928-29 (1994).

84. Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA),* 31 BERKELEY TECH. L. J. 1, 30 (2018); *see also* U.S.F. Law Research Paper No. 2017-01 *available at* https://ssrn.com/abstract=2939412.

85. 18 U.S.C. § 2511(2)(a) (2012).

86. Freiwald, *supra* note 84, at 26.

consent stemming from terms of service or privacy policies because the government entity is not a party that is authorized to establish consent to search.

C. FEDERAL TRADE COMMISSION ENFORCEMENT

The Federal Trade Commission (FTC) has regulated the collection of personal data under the authority given by the Federal Trade Commission Act (hereinafter "FTCA") to include: (1) when information is collected from children online[87] and (2) when companies engage in unfair and deceptive acts in or affecting commerce.[88]

1. COPPA

The federal government enacted the Children's Online Privacy Protection Act (COPPA) to protect the online privacy of children.[89] The Federal Trade Commission is responsible for the enforcement of COPPA, which restricts how and what owners and operators of websites, social media plug-ins, mobile applications, advertising networks, and other "Online Service Providers" can collect from children under the age of 13.[90] Mattel is currently facing a class action in California alleging that its new Hello Barbie doll records conversations without parental consent, in violation of COPPA.[91] The plaintiffs allege that the recording of the owner's friend's voice by the doll, without the permission of the friend's mother, violates COPPA. Thus, Mattel and ToyTalk's advertisement of Hello Barbie in compliance with COPPA is false and misleading.[92] The plaintiffs are currently unprotected by the process used by these providers, which only notifies the parents of the users when information is collected via microphone.[93] The courts will likely find in favor of the plaintiff due to the impact on children and will require providers of these interactive toys to develop a process for recognizing when third parties talk to the doll and to obtain permission to use their comments.

The protection provided by COPPA is limited because the statute regulates only always on devices that collect information from children and it cannot be used by adult consumers as the basis for a claim.[94] Therefore,

87. 15 U.S.C. §§ 6501–6506 (2015).

88. 15 U.S.C.A. at § 45(a)(2) (West 2012).

89. 15 U.S.C. § 6501 (2015).

90. Julia Jacobson & Heather Egan Sussman, *Protecting Children Online: New Compliance Obligations for Digital Marketing of Children*, 57 BOSTON B.J. 17 (Summer 2013).

91. Andrew Blake, *Class-action suit takes aim at 'Hello Barbie' after security researcher says doll can be hacked*, THE WASHINGTON TIMES (Dec. 9, 2015), http://www.washingtontimes.com/news/2015/dec/9/hello-barbie-makers-sued-after-security-researcher/.

92. *Id.*

93. Martha Neil, *Moms sue Mattel, saying 'Hello Barbie' doll violates privacy*, ABA JOURNAL (Dec. 8, 2015, 11:25 AM), http://www.abajournal.com/news/article/hello_barbie_violates_privacy_of_doll_owners_playmates_moms_say_in_lawsuit/.

94. 15 U.S.C. § 6502 (1998).

violations of privacy rights from the majority of always on devices are not regulated by COPPA.

2. Federal Trade Commission Act, Section 5

The FTCA states, "Unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful."[95] A deceptive act or practice is a material representation, omission, or practice, which is likely to mislead consumers acting reasonably in the circumstances.[96] Deceptive practices include misrepresentation by a company regarding the sharing of information with third parties without notification or illegally collecting personal information from users.[97] "An unfair act or practice causes or is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[98] Unfair practices include changing a privacy policy without notification or providing the choice to opt out, collecting user data without notice, or implementing substandard security procedures.[99] The FTC may consider established public policies, but may not serve as a primary basis for determining whether the act or practice is unfair.[100]

a. Misrepresentation

Misrepresentation occurs when a company makes a statement that is false regarding its data sharing practices.[101] In *United States v. Path*, the FTC filed a complaint against Path, Inc., a social network, for making false and misleading disclosures regarding its automatic collection of users' mobile device contact information.[102] The Path App gave users the ability to find friends through their contacts.[103] The app automatically collected contacts stored on a user's mobile device even if the user had never selected the option.[104] The court held that the automatic collection of information without regard to selection of the option amounted to a deceptive act or practice.[105] Similar to the Path App, always on devices may engage in the automatic collection of data without providing the proper disclosure to their users.

---

95. 15 U.S.C.A. § 45(a)(1) (1994).

96. Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce on FTC Policy Statement on Deception (Oct. 14, 1983) *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

97. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628 (2014).

98. 15 U.S.C.A. § 45(a)(4)(A)(i)–(ii), 45(n) (1994).

99. Solove & Hartzog, *supra* note 97, at 628-30.

100. 15 U.S.C.A. § 45(n) (1994).

101. Solove & Hartzog, *supra* note 97, at 640-42.

102. Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶ 15, United States v. Path, Inc., (N.D. Cal. 2013) No. 3:13-cv-0448, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf.

103. *Id.* ¶ 12.

104. *Id.* ¶ 15.

105. Complaint for Civil Penalties, Permanent Injunction, and Other Relief, *supra* note 103, at ¶ 31.

Currently, it is difficult for users and courts to determine whether providers of always on devices are engaging in these deceptive practice without first knowing of their data collection processes. Providers of always on devices should "periodically review statements they make to consumers make sure their practices line up with those statements."[106] There is limited protection, however, since if providers are not making false statements regarding their data collection practices, there can be no liability for misrepresentation.

b. Selling Data

The FTC has also taken action against companies for selling data to third parties. In 2005, the FTC settled with Vision I Properties, LLC d/b/a CartManager International ("CartManager").[107] CartManager licensed software to online merchants who incorporated the software into their own websites.[108] Merchants using CartManager's shopping cart software published privacy policies stating that they would not rent or sell personal information collected from consumers to third parties,[109] even though CartManager sold personal information it collected through the checkout process to third party marketers.[110] The commission found that CartManager's actions constituted an unfair practice in violation of the FTC Act (FTCA).[111]

Currently, third party access to data collected by always on devices is unclear. However, several sources have reported the selling of users' personal data by providers of always on devices.[112] For example, Electronic Privacy Information Center has filed complaints against Genesis Toys alleging that the data collected from their devices were sold to Nuance, who work on law enforcement and military intelligence products, to use at their discretion.[113] The risk of personal data being sold to third parties is a real threat currently on the rise, which is a major reason for the need to require the disclosure of the data collection practice from providers of always on devices to ensure that companies are held liable for the violation of privacy rights.

c. Data Security Enforcement

The holding in *FTC v. Wyndham Worldwide Corp.* granted the FTC the authority to regulate insufficient cyber security practices.[114] In *Wyndham*, the

106. *Nomi Tech., Inc.*, No. 1323251 (Aug. 28, 2015), *available at* https://www.ftc.gov/public-statements/2015/08/statement-commissioner-julie-brill-matter-nomi-technologies-inc (statement of Comm'r Julie Brill).

107. *In the Matter of Vision I Properties, LLC, Doing Bus. As Cartmanager Int'l,* 139 F.T.C. 296, 309 (2005).

108. *Id.* at 297.

109. *Id.* at 297–98.

110. *In the Matter of Vision I Properties, LLC, Doing Bus. As Cartmanager Int'l,* 139 F.T.C at 298.

111. 15 U.S.C.A. § 45(a)(1) (1994).

112. *See* Kat Sieniuc, *FTC To Look Into Toys That Spy*, LAW360 (Jan. 12, 2017, 4:36 PM), https://www.law360.com/articles/880365/ftc-to-look-into-toys-that-spy.

113. *Id.*

114. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 237 (3d Cir. 2015).

FTC alleged that the defendant's "fail[ure] to maintain reasonable and appropriate data security for consumers' sensitive personal information" was a deceptive and unfair practice.[115] The hospitality chain failed to remedy known security vulnerabilities and did not employ "'reasonable measures to detect and prevent unauthorized access' to its company's network."[116] The court found that avoiding data breach of consumers' financial information led to $10.6 million of fraudulent charges,[117] which outweighed the cost of providing a stronger security system.[118] The court held that a foreseeable data breach leading to substantial injury is a deceptive and unfair practice under the FTCA and can be penalized by the FTC.[119]

The current security measures implemented by providers of always on devices are unknown, which creates a need for the mandated disclosure of data collection and security practices. Mandated disclosure will ensure that providers meet the minimum requirements to prevent foreseeable data breaches, similar to the practices discussed in the *Wyndham* case.[120] If providers are currently implementing insufficient security safeguards then mandated disclosure will allow these providers to be held liable for engaging in unfair and deceptive practices under the FTCA.

d. Legal Limits of Protection

The protection by the FTCA is limited due to the FTC's limited resources against privacy violations. [121] The FTC lacks the authority to issue civil penalties and rarely fines companies for privacy-related violations under privacy-related statutes or rules that provide for civil penalties.[122] The FTC is limited to seeking equitable monetary relief under Section 13(b) of the FTCA, which constitute a majority of the FTC's complaints for privacy-related violations. [123] Currently, the FTC "must be strategic in bringing its cases, since it doesn't have the resources to pursue more than a relatively small fraction of law violators."[124]

IV. PROPOSAL FOR FEDERAL ACTION

My proposal recommends two actions by Congress. First, Congress must investigate the data collection, sharing, and security practices of all producers of always on devices. Second, Congress must pass a new law requiring the disclosure of these practices. These two actions by Congress

115. Wyndham Worldwide Corp., 799 F.3d at 236.

116. *Id.* at 241 (quoting Complaint at ¶ 24(h), Federal Trade Commission v. Wyndham Worldwide Corporation, 799 F.3d. 236 (2015) (No. CV 12-1365-PHX-PGR), 2012 WL 12372027).

117. *Id.* at 240.

118. *Id.* at 255–56.

119. *Id.* at 248.

120. *See,* e.g., *id.*

121. Solove & Hartzog, *supra* note 97, at 600.

122. *Id.* at 605.

123. *Id.* at 612.

124. *Id.* at 624.

will be an important step in protecting consumer privacy interests threatened by always on devices.

1. INVESTIGATION

The FTC or an assigned commission needs to investigate problems arising from the developing market of always on devices. An investigation will help Congress identify current illegal practices, define the scope of the consumer privacy rights problem, and find the best approach for regulating this market.

Congress must investigate data collection practices and learn how always on consumer devices operate. It must publish a report clarifying the type of information collected and determining when voice capture occurs. The clarification of data collection practices will discourage over collection and disclosure of data by giving users, the FTC, and courts notice of when data collection practices are violating a user's privacy interest. It will also allow providers of always on devices the ability to compare and develop industry standards for protecting their customers' personal data. Congress must also discover if communications and other data are stored and the period of storage. If data is stored, Congress must discover if the storage occurs on the device under the control of the consumer, at the service provider's server, or on a third party's server. Investigation of storage practices will help unearth insufficient security measures. Congress must investigate under what circumstances users' communications are obtained to understand and determine if they are intercepted under applicable law. Investigating unknown practices will define the scope of any intrusions into a consumer's privacy interests.

A comprehensive investigation is only a stepping-stone in providing adequate protection for users' of always on devices. The investigation will allow Congress and the public to gain knowledge of data collection processes, but it will not prevent the violation of privacy interest. Knowledge of current practices in this developing industry will foster the creation of sufficient industry standards for protecting a user's privacy interest. Providers falling short of these standards may be held liable under tort lawsuits and eventually under statutes that satisfy best practices. A Congress-implemented investigation is also needed because providers of always on devices will not want to disclose information regarding their data collection and security practices to Congress and the public without the enforcement of a mandated disclosure.

2. PROPOSED FEDERAL LEGISLATION FOR MANDATORY DISCLOSURE

Congress must create a new federal privacy law that will require always on device providers to publically disclose their practices. Mandatory disclosure will require similar information acquired in Congress' investigation, which includes how a user's information is being collected, when the recording of data actually begins, the type of information collected,

and how providers are using, storing, and safeguarding this personal information from transmission to storage to disposal.

3. THE EFFECTS OF CONGRESS' INVESTIGATION AND NEW LAW

Congress' comprehensive investigation and mandatory disclosure law will spur more legislation on the federal and state level, and increase consumer lawsuits and agency actions by helping the government determine which providers are engaging in problematic practices and implementing insufficient security measures. Disclosure will simultaneously create healthy consumer competition, and encourage the creation of industry standards for protecting consumer's personal data. The following will discuss the positive effects of Congress' investigation and the proposed law.

A. Educating Consumers

Transparency will allow consumers to become informed about their privacy risks when engaging with always on devices, which will, in turn, allow companies to collect meaningful informed consent. Consumers will understand devices' different practices and choose the device that provides their preferred level of protection of their personal information. For example, consumers will be able to buy products that guarantee the deletion of data instead of its storage by providers. An example of similar transparency is the Electronic Frontier Foundation's (EFF) website.[125] "Who's got your back?" compares service providers' compliance with government requests for a user's personal data.[126] Consumers can use this information to select a provider that fits their needs for privacy protection against government seizures of personal information.[127]

B. Best Practice

Transparency will inspire device companies to create a standard of best practices. Similar to other technological industries, the information disclosed allows the FTC to better understand the process of data collection used by these devices, and may assist the FTC in setting forth guidelines for the best practices in the always on device industry.[128]

VI. CONCLUSION

Providers of always on devices, who are profiting from the collection of personally identifiable information, should be tasked with the proper use,

125. *See generally Who Has Your Back? Protecting Your Data From Government Data Requests 2015,* ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/who-has-your-back-government-data-requests-2015 (last visited July 19, 2017).

126. *Id.*

127. *Id.*

128. *Mobile Privacy Disclosures: Building Trust Through Transparency*, FEDERAL TRADE COMMISSION (Feb. 2013),
https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also* Start With Security: A Guide for Business, FEDERAL TRADE COMMISSION (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

storage, and disposal of that information. Congress' investigation and proposed law requiring mandatory disclosure will be the first steps to holding providers accountable for abusing users' privacy rights. These two actions by Congress will allow the government and users to identify the providers who are currently violating privacy laws and allow pursuit of legal steps to remedy these violations. Transparency in this developing industry will lead to the creation of new federal and state privacy laws that strengthen the privacy rights of the modern user.