Loyola Consumer Law Review

Volume 29 | Issue 2 Article 2

2017

Always-Listening Technologies: Who Is Listening and What Can Be Done About It?

Arielle M. Rediger

ALWAYS-LISTENING TECHNOLOGIES: WHO IS LISTENING AND WHAT CAN BE DONE ABOUT IT?

*Arielle M. Rediger**

I. INTRODUCTION

People love the ability to control their phones by a simple voice command of "OK Google" or "Siri," but often do not realize that it necessarily requires the phone to be always listening for those trigger words. This voice command technology spread into consumers' homes via products like the Samsung Smart TV, Amazon Echo, and Microsoft's Xbox. Just like with Google's OK Google or Apple's Siri, these products take voice commands and are always listening for the trigger words. The advent of these always-listening technologies presents multiple new problems. After discussing exactly how the Amazon Echo, the Samsung Smart TV, and Microsoft's Xbox function, this paper investigates the problems presented in two areas: government listening and corporate listening.

The Government Listening section begins a discussion of the Federal Bureau of Investigation's (FBI) and the National Security Agency's (NSA) abilities to remotely access microphones in citizens' cell phones. This serves as the situational analogy for the possibility that arises from these in-home always-listening technologies that are also heavily reliant on microphones. Following that is an analysis of Fourth Amendment law, beginning with a discussion of the evils the Fourth Amendment sought to eliminate – general warrants and writs of assistance.. *Olmstead v. United States*, *Katz v. United States*, and *Berger v. State of New York* lead the discussion on how the United States Supreme Court addresses privacy concerns in the face of new-at-the-time technologies and what exactly can be protected by the Fourth Amendment. The ultimate question posed in this section is whether the fact that these technologies are almost exclusively used within one's home – a classic Fourth Amendment area of protection – changes the legality of any potential government surveillance, and how a court might view these technologies.

In the Corporate Listening section, the recent Samsung Smart TV scandal serves as an example of what privacy concerns arise from these technologies even absent government eavesdropping. By virtue of being able to respond to voice command, these devices are necessarily always waiting to hear certain trigger words. Samsung's privacy policy informed customers to be cognizant when discussing "sensitive information" around the device, as anything discussed around the device may be collected among the data reported to third-party companies. After outrage ensued from its users, Samsung amended its policy. This speaks to the paradox created between consumers' desire to have hyper-convenient technology in every aspect of life, and their unwill-

ingness to accept that these desired technologies may necessarily require companies to be listening to them. The other problem presented by corporate listening stems from the Fourth Amendment and the third-party doctrine. This section will discuss what the third-party doctrine means for always-listening technologies and the uncertain future of the doctrine itself.

II. THE ALWAYS-LISTENING TECHNOLOGIES

A. How Does the Technology Work?

Each of these three technologies – Amazon Echo, Samsung Smart TV, and Xbox – works in a fairly similar manner. All of the devices rely on microphones that are always waiting to hear a command from its owners, as each requires the user to employ a trigger word to activate the device. Only upon hearing the trigger word will the device respond to the request. For instance, an owner cannot just ask aloud whether the Sacramento Kings won the latest game, but must preface the question with "Alexa" when using the Amazon Echo.[1]

Amazon Echo is built to be one's very own personal assistant. Once the owner employs the trigger word, the device will follow a litany of commands. Amazon's website has a non-exhaustive list of various commands one could give it, including questions it can answer for the owner. For example, an owner can ask the device for the weather in any given city, or for the statistics for a favorite sports team.[2] The product page boasts that it is "hands-free and always on" and can hear commands from the other side of the room even when music is playing, all thanks to its seven microphones.[3] When the device hears the trigger word, it streams the audio to the cloud where Amazon's software identifies the command and responds accordingly.[4] Also streamed to the cloud is the "fraction of a second of audio before" the trigger word.[5] The seven microphones can be turned off using a button on the device itself, but it will still respond to commands made with the device's

---

[1] *What is Amazon Echo*, AMAZON, http://www.amazon.com/dp/B00X4WHP5E (last visited Mar. 31, 2017). Each of these three devices responds to its own trigger word.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Alexa and Amazon Echo FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (last visited Mar. 31, 2017).

remote.[6] The microphones will only turn on again once the button is pushed another time.[7]

Samsung's Smart TV responds to commands in two different ways. The distinction lies in whether the command can be processed locally, or whether it must go through a server. The first situation relies on the microphone within the television itself, which can process "predetermined" commands.[8] These commands include things like changing the volume or the channel. The second situation relies on the microphone inside the television's remote.[9] The command is one that was not "predetermined" but instead involves a search requiring the server.[10] For example, someone could use the microphone in the remote to make a more specific command like recommending a good romantic comedy.[11] Samsung asserts this kind of search is akin to one done by any other device using voice recognition software.[12]

The Xbox Kinect is an addition to the Xbox gaming console that allows users to use the device's camera and microphone to log in with facial recognition, control their televisions, change the channel or the game they are playing, and many other personalized features.[13] The device responds to the trigger word "Xbox" followed by a command.[14] The universe of commands it responds to is more geared toward video games and television controls, but it can also run an internet search if the commands "Xbox Bing" or "Browse to" are used, followed by the website.[15] Some of the commands given to the device are processed locally and the command does not get transmitted outside of the device.[16] Microsoft captures the voice command given to the Xbox,

---

[6] *Id.*

[7] *Id.*

[8] Natasha Lomas, *Samsung Edits Orwellian Clause Out of TV Privacy Policy*, TECH CRUNCH (Feb. 10, 2015), http://techcrunch.com/2015/02/10/smarttv-privacy/#.puzvmzo:yfMB.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Kinect for Xbox One*, XBOX, http://www.xbox.com/en-US/xbox-one/accessories/kinect-for-xbox-one (last visited Mar. 15, 2017).

[14] *Id.*

[15] Xbox Wire Staff, *The Complete List of Kinect Gesture and Voice Commands For Your Referencing Pleasure*, XBOX (Nov. 26, 2013, 12:02 AM), http://news.xbox.com/2013/11/26/xbox-one-kinect-gesture-and-voice-guide/.

[16] *Kinect Xbox One Privacy FAQ*, XBOX, http://news.xbox.com/2013/11/26/xbox-one-kinect-gesture-and-voice-guide/ (last visited Mar. 31, 2017).

"along with any ambient background noise."[17] Additionally, the user can decide to deactivate the microphones for the purposes of voice commands, but still opt to use the microphones to chat with other gamers.[18]

B. Why These Technologies Can be Analogized to Cell Phones

The relevant underlying technology of both cell phones and the in-home, always-listening devices are microphones. As will be discussed below, reports of the United States government spying on its own citizens via citizens' cell phones explained that it was done by remotely turning on the microphones within the cell phone. Even if the cell phone was turned off, the government was still able to remotely access the phone, turn on the microphone without alerting the phone's owner, and listen to whatever was occurring around it.

Accordingly, these in-home, always-listening devices may be just as susceptible to government intrusion by virtue of their heavy reliance on microphones. The key difference between the cell phones already known to be accessible by the government and the in-home, always-listening technologies that are gaining popularity today is that the latter are predominantly used in one's home. This difference will be discussed in more detail below, but insofar as the underlying technology is concerned, however, the two groups are substantially similar.

III. GOVERNMENT LISTENING

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*[19]

The Fourth Amendment has been held to protect or prohibit many different things. In *Olmstead v. United* States, the Supreme Court held the Fourth Amendment did not extend so far as to protect government surveillance absent physical trespass on one's property.[20] In *Katz v. United States*, the Supreme Court overruled *Olmstead* and

---

[17] *Id.*
[18] *Id.*
[19] U.S. Const. amend. IV.
[20] Olmstead v. U.S., 277 U.S. 438, 466 (1928).

instead held the Fourth Amendment to protect people, not places.[21] As technology advances, the Supreme Court must continue to update what is protected by the Fourth Amendment as to allow the Constitution to adapt to modern times.

A. Reports of NSA and FBI Remote Hacking of Cell Phones

Reports of the government eavesdropping via microphones are not new. In 2006, CNET reported that the FBI used the "novel form of electronic surveillance" during a criminal investigation by remotely activating the microphone of a suspect's cell phone to listen in on conversations.[22] The report stated that the eavesdropping could occur regardless of whether the phone was on; the phone's microphone would only be inaccessible if the battery was removed.[23] Verizon Wireless did not directly comment on the remote eavesdropping for CNET's article, but said that the company "works closely with law enforcement" and complies with legal orders.[24]

Seven years later, reports of the government remotely accessing microphones were still in the headlines. The Wall Street Journal reported the FBI had the ability to remotely activate the microphone on laptops and Android devices without the user knowing that it is happening.[25] The FBI reportedly uses such a technique when investigating organized crime, child pornography, or terrorism, but refrains from doing so when investigating hackers due to fear that the technique would be discovered and subsequently publicized.[26] In cases where the microphones on laptops or Android devices are remotely accessed, the FBI attempts to ensure that only relevant information is collected.[27] In doing so, however, an FBI "screening team" must go through all of the collected data to determine what is relevant.[28] While the Wall Street Journal's report was specific to laptops and Android devices, other websites reported that the NSA has been able to, *inter alia*, remotely

---

[21] Katz v. U.S., 389 U.S. 347, 351 (1967).

[22] Declan McCullagh, *FBI taps cell phone mic as eavesdropping tool*, CNET (Dec. 4, 2006, 6:56 AM), http://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool.

[23] *Id.*

[24] *Id.*

[25] Jennifer Valentino-Devries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J. (Aug. 3, 2013, 3:17 PM), http://www.wsj.com/articles/SB10001424127887323997004578641993388259674.

[26] *Id.*

[27] *Id.*

[28] *Id.*

access the microphone on the iPhone since 2008.[29]

In 2014, CNN reported on the NSA's hacking of cell phones after Edward Snowden spoke about it in an interview on NBC with Brian Williams.[30] CNN's article included an explanation on how this technology works, courtesy of former members of the Central Intelligence Agency, Navy SEALs, and consultants to the military's cyber warfare team:

Government spies can set up their own miniature cell network tower. Your phone automatically connects to it. Now, that tower's radio waves send a command to your phone's antennae: the baseband chip. That tells your phone to fake any shutdown and stay on. A smart hack won't keep your phone running at 100%, though. Spies could keep your phone on standby and just use the microphone – or send pings announcing your location.[31]

The article reported that the NSA relies on these tactics on a "specified list of terrorists and foreign fighters" rather than on the average person.[32] However, it noted that the FBI uses these surveillance techniques domestically for investigations of many various crimes.[33]

B. Government Surveillance and The Fourth Amendment

The United States Supreme Court has an inconsistent past in deciding what is and what is not protected under the Fourth Amendment.[34] The confusion stems from the very obvious problem that when the Constitution was drafted, the Founding Fathers could not have possibly imagined the future of technology. When the Fourth Amendment was drafted, the threat of government intrusion came from general warrants and writs of assistance.[35] General warrants were used by the King before the American Revolution and allowed officers to search

---

[29] Chris Smith, *Yikes: NSA can turn on your iPhone's camera, mic without you knowing*, BRG (Dec. 31, 2013, 7:45 AM), http://bgr.com/2013/12/31/nsa-iphone-hack/; *The NSA's Spy Catalog*, SPIEGEL (Dec. 30, 2013, 3:18 PM), http://www.spiegel.de/international/world/a-941262.html.

[30] Jose Pagliery, *How the NSA can 'turn on' your phone remotely*, CNN (June 6, 2014, 8:03 AM), http://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *See, e.g.*, Olmstead v. U.S., 277 U.S. 438 (1928); *see contra* Katz v. U.S., 389 U.S. 347 (1967).

[35] *Olmstead*, 277 U.S. at 463.

unspecific places and seize unspecified persons.[36] Such were often used by the King to silence dissenters.[37] Writs of assistance allowed officers to search any place based merely on his own suspicion.[38] Especially concerning was that writs of assistance lasted the duration of the King or Queen's life.[39] General warrants and writs of assistance were the predominant concerns for the drafters of the Fourth Amendment, but as stated by Justice Brandeis in his dissent in *Olmstead v. United States*, general warrants and writs of assistance "are but puny instruments of tyranny and oppression when compared with wire tapping."[40]

The problem of an unknown future plagues the Supreme Court just as it plagued the Founding Fathers. It is impossible to plan for something that has not yet been conceptualized. For that reason, Fourth Amendment case law is akin to a patchwork quilt; the Supreme Court fixes one problem created by technology at a time, largely without considering what will come next or how one decision will affect privacy implications presented by later technologies. For example, when dealing with the question of whether police can use GPS trackers on suspects, Justice Sotomayor criticized the majority's opinion in her concurrence for being short-sighted, stating that "[i]n cases of electronic or other novel means of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[41]

In 1928, the Supreme Court decided *Olmstead v. United States*, in which the defendants challenged the constitutionality of evidence obtained by the government through the wiretapping of several properties[42] over the course of almost five months.[43] The defendants and seventy-two other people were indicted after the wiretapping evidence revealed a large-scale operation of unlawfully importing, possessing, and selling liquor within the United States.[44] Olmstead was in charge of the operation and received half of the profits gained.[45] Federal agents placed wiretaps along the telephone wires from four of the de-

---

[36] The Honorable M. Blane Michael, *Reading the Fourth Amendment: Guidance From the Mischief that Gave It Birth*, 85 N.Y.U. L. REV. 905, 909 (2010).

[37] *Id.*

[38] *Id.* at 907.

[39] *Id.*

[40] *Olmstead*, 277 U.S. at 476 (Brandeis, J. dissenting).

[41] U.S. v. Jones, 132 S.Ct. 945, 955 (2012) (Sotomayor, J. concurring).

[42] *Olmstead*, 277 U.S. at 455-57.

[43] *Id.* at 471 (Brandeis, J., dissenting).

[44] *Id.* at 455 (majority opinion).

[45] *Id.* at 456.

fendants' residences and from the operation's main office without trespassing upon the defendants' respective properties.[46] The Supreme Court opined that the "well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to *prevent the use of governmental force to search* a man's house, his person, his papers, and his effects, and to prevent their seizure against his will."[47] The Court ultimately determined that the wiretapping used against Olmstead was not prohibited by the Fourth Amendment because there was no searching or seizing, and was obtained only by hearing, without entering the defendants' offices or houses.[48] The Court opined that holding otherwise would give an "enlarged and unusual meaning to the Fourth Amendment."[49]

Almost forty years later, *Olmstead* was overruled by *Katz v. United States*, but Justice Brandeis's dissent in *Olmstead* went on to become one of the most influential opinions regarding privacy and the Fourth Amendment. In his dissent, Justice Brandeis admitted that when the Fourth and Fifth Amendments were adopted, their purposes were obvious because the government "could secure possession of [man's] papers and other articles incident to his private life-a seizure effect, if need be, by breaking and entry."[50] Because that was the government's only option, the Fourth and Fifth Amendments' specific language protected against "such invasion of 'the sanctities of a man's home and privacies of life'..."[51] Justice Brandeis then noted that as time progressed, inventions made it possible for the government to obtain "what is whispered in the closet" and that progress is unlikely to stop with wiretapping.[52] He further explained that when the government uses a wiretap on someone's telephone, it is also "tapping the telephone of every other person whom he may call, or who may call him."[53] He opined that people are quick to notice when their liberties are infringed by "evil-minded rulers;" thus, the greatest danger to liberty comes from the "insidious encroachment by men of zeal, well-meaning but without understanding."[54]

---

[46] *Id.* at 457.
[47] *Id.* at 463 (emphasis added).
[48] *Id.* at 464.
[49] *Id.* at 466.
[50] *Id.* at 473 (Brandeis, J. dissent).
[51] *Id.*
[52] *Id.*
[53] *Id.* at 476.
[54] *Id.* at 479.

Katz again presented the Supreme Court with the issue of governmental wiretapping.[55] Federal agents placed a wiretap on a public phone booth where they believed the defendant was making phone calls.[56] The primary debate was whether the phone booth qualified as a "constitutionally protected area."[57] Rejecting the premise of the debate, the Supreme Court instead held that the Fourth Amendment protects people, not places.[58] The Court overruled *Olmstead* by holding that there was no constitutional significance given to the fact that the wiretap did not physically go inside the phone booth.[59] The Court further explained that what someone knowingly exposes to the public is not protected by the Fourth Amendment, but that what someone "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[60] As applied to *Katz*, the Court found that even though he used a public phone booth, he had entered the booth in an attempt to exclude the "uninvited ear."[61] Justice Harlan wrote an influential concurrence in which he delivered a test for protection: an actual, subjective expectation of privacy, and an objective, reasonable expectation of privacy.[62]

In *Berger v. State of New York*, the Supreme Court considered the constitutionality of a New York statute permitting electronic eavesdropping.[63] The statute in question allowed a court to issue an *ex parte* order to eavesdrop based on the word of a district attorney, the attorney-general, or "an officer above the rank of sergeant of any police department of the state or of any political subdivision thereof."[64] The statute required that the oath stated a reasonable ground to believe evidence of a crime would be obtained, that it particularly described the person(s) who would be eavesdropped upon, the purpose of doing so, and the particular phone number or telegraph line involved.[65] Although the statute required the identification of the person subject to the warrant, the Court opined that said requirement "does no more than identify the person who constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations,

---

[55] Katz v. U.S., 389 U.S. 347, 348 (1967).
[56] *Id.* at 349.
[57] *Id.* at 351.
[58] *Id.*
[59] *Id.* at 353.
[60] *Id.* at 351.
[61] *Id.*
[62] *Id.* at 361.
[63] Berger v. State of New York, 388 U.S. 41, 44 (1967).
[64] *Id.* at 54.
[65] *Id.*

or discussions to be seized."[66] Additionally, the statute allowed eavesdropping for two months, and the possibility of an extension thereafter, based on the single, original showing of cause.[67] The statute also did not provide a termination procedure in the event that the information sought was obtained within the two month time period, which the court opined left too much to the sole discretion of the officer.[68] Lastly, the Court took issue with a warrant being issued without any notice being given to the suspect because of the necessity for secrecy, but no requirement for a showing of exigency, as would be required of a traditional warrant.[69]

C. The Significance of Being "In-Home" Technologies

As noted above, the always-listening technologies can be analogized to cell phones for the purposes of discussing exactly how the government may use them as surveillance tools in the future. However, the always-listening technologies discussed in this paper have one crucial difference from cell phones that may change how they are treated under the Fourth Amendment: they almost exclusively reside in one's home. That means that these devices do not travel with their owners into public spaces. Traditionally, homes and what occurs therein have been treated as sacred with regard to the Fourth Amendment. Such was illustrated in the Supreme Court's analysis in *Kyllo v. United States*.

In *Kyllo*, the Supreme Court decided whether the use of a thermal imager on a person's home was considered a search under the Fourth Amendment.[70] Justice Scalia wrote the opinion and heavily emphasized both the nature of the home under the Fourth Amendment and the intimate nature of the information obtained by using the device.[71] The Court noted 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."[72] It referred to the interior of the home as the prototypical area of protection.[73] Allowing this tech-

---

[66] *Id.* at 59.
[67] *Id.*
[68] *Id.* at 59-60.
[69] *Id.* at 60.
[70] Kyllo v. U.S., 533 U.S. 27, 29 (2001).
[71] *Id.* at 31-39.
[72] *Id.* at 31 (citations omitted) (quotations omitted).
[73] *Id.* at 34.

nology to fall outside of a "search" would be to permit police technology to lessen the privacy guaranteed by the Fourth Amendment.[74] Justice Scalia also emphasized that the information obtained was intimate as the thermal imager might inform the police "at what hour each night the lady of the house takes her daily sauna and bath."[75] The Court also noted that thermal imaging technology is largely used only by police rather than being in general public use.[76] Considering all of these points, the Court reversed the Court of Appeals decision and held that using the thermal imager constituted a "search" and was unreasonable without a warrant.[77]

The Supreme Court's logic in *Kyllo* would likely vary a bit if applied to the always-listening technologies. The biggest difference between the two technologies is that the thermal imager was largely used only by police, whereas the always-listening technologies are specifically marketed for general public use. The devices are bought by consumers and voluntarily placed in the owners' homes. However, the Court would likely find protection under the Fourth Amendment for these devices because of the emphasis on the interior of the home being protected and intimate details being discovered. If a thermal imager's ability to discover the time of a daily bath is too intimate, the fact that use of these devices' microphones can lead to overhearing much more private details than just bath time would likely necessitate a finding that it is too intimate as well.

Consequently, the history of the Supreme Court's Fourth Amendment decisions indicate that these technologies will be covered by the Fourth Amendment and require the government to obtain a warrant before using them for surveillance purposes. Under *Katz*, the Fourth Amendment can protect what someone seeks to maintain private by excluding the "uninvited ear."[78] These technologies would also satisfy Justice Harlan's test described in his *Katz* concurrence, which has since been heavily relied upon.[79] There would almost undoubtedly be a subjective expectation of privacy in these devices as one does not expect the government to listen in on conversations through their televisions or gaming consoles. Likewise, the expectation of privacy is objectively reasonable because of the prevalent and pervasive idea that people are free from government eyes and ears while in their own homes. Lastly, as mentioned above, *Kyllo* could be relied upon to grant

---

[74] *Id.* at 35.
[75] *Id.* at 38.
[76] *Id.* at 34.
[77] *Id.* at 40-41.
[78] *Katz*, 389 U.S. at 351.
[79] Kyllo v. U.S., 533 U.S. 27, 33 (2001).

protection given the intimate nature of details that may be discovered by listening in on conversations taking place in the home. Should states attempt to legislate electronic eavesdropping regarding these devices, *Berger* gives good guidance on what will be considered unconstitutional.

IV. CORPORATE LISTENING

A. The Problem of Corporate Listening: The Samsung Smart TV Scandal and the State of Privacy Policies

When people buy a new gadget, most rush home to install and start using it; they are not running home to tear open the privacy policy and start reading. People's tendency to (at most) skim over these policies is especially worrisome in the technological context because people are almost always opting to give up data about themselves and their usage of that service or device.[80]

In 2015, Samsung made headlines not just for its latest cell phones, but for its privacy policy regarding the Samsung Smart TV.[81] Samsung's policy warned Smart TV owners to: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."[82] News outlets quickly began comparing that portion of the privacy policy to the telescreens featured in George Orwell's *1984*.[83] It only took a few days for Samsung to amend its policy's terms.[84] Samsung amended the policy to the following:

If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some interactive voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service provider (currently, Nuance Communications, Inc.)

---

[80] Devin W. Ness, *Information Overload: Why Omnipresent Technology and The Rise of Big Data Shouldn't Spell the End For Privacy As We Know It*, 31 Cardozo Arts & Ent. L. J. 925, 930 (2013).

[81] *See, e.g.*, Andrew Griffin, *Samsung smart TV policy allows company to listen in on users*, THE INDEPENDENT (Feb. 9, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/samsungs-new-smart-tv-policy-allows-company-to-listen-in-on-users-10033012.html.

[82] Lomas, *supra* note 8.

[83] *See, e.g.*, Griffin, *supra* note 81.

[84] *See* Chris Matyszczyk, *Samsung changes Smart TV privacy policy in wake of spying fears*, CNET (Feb. 10, 2015, 12:35 PM), http://www.cnet.com/news/samsung-changes-smarttv-privacy-policy-in-wake-of-spying-fears/.

that converts your interactive voice commands to text and to the extent necessary to provide the Voice Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Samsung will collect your interactive voice commands only when you make a specific search request to the Smart TV by clicking the activation button either on the remote control or on your screen and speaking into the microphone on the remote control.[85]

Additionally, Samsung alerted its users that they could opt out of Voice Recognition if any privacy concerns remained.[86] The irony, of course, is that people likely bought Samsung's Smart TV because they *wanted* the ability to control their televisions by voice recognition commands, they just failed to consider that the television's microphones may capture anything said around it.

Samsung's scandal is but one instance of new technologies creating privacy concerns for users who likely never considered the potential downside of convenience. As one writer put it, "[t]he technology industry is increasingly asking consumers to make a choice that treads the line between cool and creepy, as companies prompt us to trade our personal information in exchange for convenience and services."[87] People love the technological convenience of being able to control electronics by voice commands, but are far less keen on the prospect of companies overhearing them do so. This paradox puts companies like Samsung in a tough spot; how are they supposed to contribute to the future of the Internet of Things, where things are so easily controlled by voice commands, and still assuage people's fears that the companies are listening? By virtue of being voice-controlled, the device must necessarily be listening and be able to transmit that data back to the company to decipher the request and respond accordingly. This makes sense, but is often not considered and understood by the users of these devices.

---

[85] *Samsung Privacy Policy—SmartTV Supplement*, SAMSUNG, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited Feb. 22, 2017).

[86] *Id.*

[87] Donna Tam, *Our devices are listening to us all the time—but do we care?*, CNET (Nov. 16, 2014, 4:00 AM), http://www.cnet.com/news/our-devices-are-listening-to-us-all-the-time-but-do-we-care/.

1. Privacy Policies for Samsung, Amazon, and Microsoft

Microsoft's privacy policy explains what features can be enabled by the camera and microphones in the Xbox Kinect device.[88] With regard to the microphones, the policy states that it can be used to chat with other players during games, give commands for the console, games or apps, and run searches.[89] The only section dealing with the voice data is surprisingly short given the length of the entire document. Microsoft simply states, "[w]e collect, and use for service improvement, voice search requests or samples of voice commands occurring while using Kinect. These data are stored separately from your Xbox profile."[90]

The privacy policy for Amazon Echo is fairly concise, but adds quite a bit through the incorporation of Amazon's general Conditions of Use and Privacy Notice.[91] With regard to the voice commands a user can give to Amazon Echo, the statement informs users that the device streams the audio to the cloud, processes it, then retains "voice input and other information, such as music playlists..." in the cloud.[92] The frequently asked questions section of Amazon Echo's product page informs users that they have the option of turning off the microphones, but such information is left out of the privacy statement.[93] Amazon's general privacy policy states that the company does not sell information about customers to others and shares it only in six outlined situations.[94] These situations were generally applicable to the regular use

---

[88] *Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last updated Oct. 2015).

[89] *Id.*

[90] *Id.*

[91] *Alexa Terms of Use*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 (last updated: Aug. 19, 2015); *Conditions of Use*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=508088 (last updated June 22, 2015); *Amazon.com Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-A2C397AB-68FE-4592-B4A2-7550D73EEFD2__SECTION_3F77537F901B4157B0CBD26834827652 (last updated: Mar. 3, 2014).

[92] *Alexa Terms of Use*, *supra* note 91.

[93] *See id.; see also Alexa and Amazon Echo FAQs*, *supra* note 5. In Amazon's frequently asked questions section, it informs owners that they can turn off the voice command feature, but is quick to also inform owners that doing so may "degrade your Alexa experience."

[94] *Amazon.com Privacy Notice*, *supra* note 91.

of Amazon – ordering items, for example – rather than the use of Amazon Echo.[95]

Samsung's privacy policy for its Smart TV was discussed above in regard to the scandal that surrounded it. The quoted section was only in regard to the voice recognition feature of the television, but made an important distinction for users. It clarified that Samsung only collects the voice commands when a specific request is made *by clicking the activation button.*[96] This means that the predetermined phrases one can make to the device are not collected by Samsung.[97] So if a user decides to deactivate the voice recognition feature, he will not lose the functionality of the voice commands all together. The policy for the Smart TV also incorporates by reference the general Samsung Privacy Policy.[98] The general privacy policy was especially helpful as it largely employed a clear, bullet-point format and as a bonus for Californians, included a special "Your California Privacy Rights" section.[99]

2. *Privacy Policies: The Best Practice*

Despite making headlines for its suspect privacy policy, Samsung's policy is the best practice. First, its readability was far superior to Amazon's privacy policy. Amazon incorporated a lot by reference, which required the user to click through several links to eventually gather all of the information. Trying to track down all of Amazon's policy pages made it hard to make sure everything was accounted for and get a clear idea of what the policy was. In contrast, both Microsoft and Samsung had one, concise page with all of the relevant information. The policies for their many products (i.e., Microsoft Word, Cortana, etc.) were clearly separated and easy to navigate through.

Second, even before Samsung amended its policy post-scandal, its policy was not bad. Each of the devices' policies largely had the same method of dealing with voice commands. In fact, the warning Samsung gave that led to the scandal is true of all always-listening devices; Samsung was just the only one to point it out. By virtue of being voice-controlled devices, these technologies will overhear conversations around them. Additionally, the Samsung Smart TV was the only

---

[95] *Id.*

[96] *Samsung Privacy Policy—SmartTV Supplement*, *supra* note 85.

[97] *Id.*

[98] *Id.*

[99] *Samsung Privacy Policy*, SAMSUNG (Feb. 10, 2015), http://www.samsung.com/us/common/privacy.html.

one that allowed for continued use of the voice recognition feature after opting to disable it; users could still use a more limited range of predetermined commands. The downside for Samsung was that it used a third-party service provider, Nuance Communications, Inc., to respond to the voice command. While this is not a huge deal, it might matter to those who are already concerned with one company overhearing the various commands they give to their devices.

B. Government Seizing Data From Corporations

1. The Fourth Amendment and the Third-Party Doctrine

In 1979, the Supreme Court decided *Smith v. Maryland* wherein a pen register was at issue.[100] The police were investigating a series of harassing phone calls made to a victim and installed a pen register on a suspect's phone.[101] A pen register records all of the phone numbers dialed on a phone without overhearing any of the content of the phone calls by measuring electrical impulses caused by dialing phone numbers.[102] The resulting phone records indicated that the suspect was responsible for the phone calls, which was used as a basis for a warrant to search his home and later used as evidence at trial.[103] The defendant argued that the evidence yielded from the pen register should be excluded because its use constituted a warrantless search.[104] The Supreme Court held that the use of a pen register did not qualify as a search for Fourth Amendment purposes.[105] The Court opined that the entire set of privacy interests at stake in the case were held by the phone company.[106] People could not claim a privacy interest in the phone numbers they dialed because they know that when they dial a phone number, that number is conveyed to the phone company – a third party.[107] Because someone else is getting that information, people cannot expect that police will be prevented from obtaining those records.[108]

The *Smith* decision created a clear, bright-line rule that phone numbers being dialed out have no Fourth Amendment protection.

---

[100] Smith v. Maryland, 442 U.S. 735, 737 (1979).
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.* at 745.
[106] *Id.* at 741.
[107] *Id.* at 742.
[108] *Id.*

When read in conjunction with *United States v. White*, *Smith* suggests that the Supreme Court intended to create a very robust third-party doctrine. In *White*, the defendant was found guilty of various drug charges after the prosecution introduced evidence of conversations the defendant had with a government informant which had been overheard using a radio receiver.[109] The Court opined that the Fourth Amendment should not protect a defendant whose conversation has been recorded or transmitted by an informant when the Fourth Amendment does not protect a defendant who confides in a "trusted accomplice [who] is or becomes a police agent."[110] The Court reasoned that someone thinking about or engaging in illegal activities must certainly realize that people he speaks with might be reporting to the police.[111]

Justice Sotomayor's concurrence in *United States v. Jones* strongly suggests there is potential for the Supreme Court to amend the third-party doctrine in the future. Much like Justice Brandeis's dissent in *Olmstead*, Justice Sotomayor's concurrence touches on how changing technology creates problems for existing Supreme Court case law. Justice Sotomayor noted:

[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 of information about themselves to third parties in the course of carrying out mundane tasks."[112]

She also opined that people likely would not accept a world in which companies gave the government a list of every website visited in the last week, month, or year, without a warrant.[113] To support this proposition, Justice Sotomayor cited to *Katz*, where the Supreme Court held that even if in a publicly accessible area, what a person intends to keep private may be constitutionally protected.[114]

As it stands today, such an expansive third-party doctrine suggests that users of always-listening technologies may not have much of an argument to make when objecting to companies using information yielded by these technologies. This does not bode well for the future given that people are increasingly giving their information away

---

[109] U.S. v. White, 401 U.S. 745, 747 (1971).

[110] *Id.* at 752.

[111] *Id.*

[112] U.S. v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J. concurring) (citations omitted).

[113] *Id.*

[114] *Id.*

to third parties at an alarming rate.[115] As applied to the Amazon Echo, this particular issue was poised to have its day in court. In December 2016, it was reported that police in Arkansas were trying to obtain the recordings on a suspect's Amazon Echo.[116] The man was charged with murder after a friend was found dead in the suspect's hot tub following a gathering at his house.[117] The police used a search warrant to obtain the Echo's data covering two days around the incident, which Amazon reportedly only partially complied with by providing the account holder's information and purchase history.[118] Amazon's statement was that: "'Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course.'"[119] As of February 2017, Amazon was refusing to provide the account holder's Echo voice recordings based on First Amendment protections.[120] However, the issue became moot in March 2017 when the defendant agreed to allow the police to have access to the recordings.[121] Amazon provided the requested data later that same day.[122]

2. *The Uncertain Future of the Third-Party Doctrine*

Circuit courts' discussions of the third-party doctrine evidences reluctance at best and unhappiness at worst. Several circuits express uneasiness about applying a relatively antiquated doctrine in modern times. Recently, two circuits have changed stances on the third-party doctrine when rehearing cases en banc.

---

[115] *See, e.g.*, Saul Hansell, *Zuckerberg's Law of Information Sharing*, N.Y. TIMES (Nov. 6, 2008, 7:03PM), http://bits.blogs.nytimes.com/2008/11/06/zuckerbergs-law-of-information-sharing/?_r=0. In 2008, Mark Zuckerberg predicted that people will continue to share twice as much information about themselves as they did the year before.

[116] *See, e.g.*, Alina Selyukh, *As We Leave More Digital Tracks, Amazon Echo Factors in Murder Investigation*, NPR (Dec. 28, 2016), http://www.npr.org/sections/alltechconsidered/2016/12/28/507230487/as-we-leave-more-digital-tracks-amazon-echo-factors-in-murder-investigation.

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] Jeff John Roberts, *Amazon Argues Free Speech in Alexa Murder Case*, FORTUNE (Feb. 23, 2017), http://fortune.com/2017/02/23/amazon-free-speech-alexa-murder/.

[121] Eliott C. McLaughlin, *Suspect OKs Amazon to hand over Echo recordings in murder case*, CNN (Mar. 7, 2017), http://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/.

[122] *Id.*

In 2014, the Eleventh Circuit decided *United States v. Davis* and held that there is a reasonable expectation of privacy in cell-site location information despite the third-party doctrine.[123] Consequently, it held that obtaining such information without a warrant violates the Fourth Amendment.[124] However, rehearing the case en banc one year later, the Eleventh Circuit reversed course and held that the defendant expressly did not have a reasonable expectation of privacy in such data because of the third-party doctrine.[125] In Circuit Judge Rosenbaum's concurrence, he opined that the dissent was right to be concerned because, "[i]n our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life."[126] However, he noted that, "[s]ince we are not the Supreme Court and the third-party doctrine continues to exist and to be good law at this time, though, we must apply the third-party doctrine where appropriate."[127]

In 2015, the Fourth Circuit decided *United States v. Graham* in which it also considered the issues of cell-site location information and the third-party doctrine.[128] The court held that the third-party doctrine could not be applied to the cell-site location information because it is not something that a phone user conveys to its provider, voluntarily or involuntarily.[129] Consequently, the user does not assume the risk of disclosing that information as it is generated regardless of the user's participation.[130] However, just as the Eleventh Circuit in *Davis*, the Fourth Circuit reversed course when rehearing the case en banc and held that the Fourth Amendment cannot protect the cell-site location information due to the third-party doctrine.[131] Also just as the *Davis* court, the *Graham* court expressed a sentiment of resignation by saying, "unless and until the Supreme Court so holds, we are bound by the contours of the third-party doctrine as articulated by the Court."[132] It went so far as to say that the third-party doctrine "increasingly feels like an exception," as "[a] per se rule that it is unreasonable to expect

---

[123] U.S. v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014), *reh'g granted*, 2014 WL 4358411 (11th Cir. 2014).

[124] *Id.*

[125] U.S. v. Davis, 785 F.3d 498, 511 (11th Cir. 2015).

[126] *Id.* at 525 (Rosenbaum, J. concurring).

[127] *Id.*

[128] U.S. v. Graham, 796 F.3d 332 (4th Cir. 2015), *reh'g granted*, 624 Fed.Appx. 75 (4th Cir. 2015).

[129] *Id.* at 354.

[130] *Id.*

[131] U.S. v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc).

[132] *Id.* at 437.

privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy."[133]

In 2016, the Seventh Circuit heard *United States v. Caira* wherein it applied the third-party doctrine to I.P. addresses.[134] The defendant argued, inter alia, that the government should not have been able to obtain his I.P. addresses from Microsoft.[135] The court rejected the argument and found that the defendant had no reasonable expectation of privacy in the addresses because he had shared them with Microsoft – a third party.[136] It acknowledged that an attack on the third-party doctrine was not new, but such arguments had not won the day because "it is also true that '[t]he Supreme Court ... has twice rejected [Caira's critique]. Until the Court says otherwise, these holdings bind us.'"[137] As of November 2016, there is petition for certiorari docketed with the Supreme Court for *Caira*.[138]

Whether it is *Caira* or a different case, the Supreme Court will likely choose to hear a case dealing with the third-party doctrine relatively soon. As technology continues to advance and even more information is shared with corporations on a regular basis, dissatisfaction with the third-party doctrine will continue. Given the previous doubt cast upon the third-party doctrine by Justice Sotomayor in her concurrence in *Jones* and the begrudging way in which circuit courts apply it, the Supreme Court may use a new case as an opportunity to at least modernize the doctrine.

C. The Possibility of Protection: California Assembly Bill 1116

California recently enacted legislation dealing with the use of voice recognition software in the home. On October 6, 2015, Governor Jerry Brown approved Assembly Bill No. 1116, which became section 22948.20 of the California Business and Professions Code. The law primarily accomplished three things: (1) requiring manufacturers of connected televisions with voice recognition features to prominently inform the user of such feature upon initial set up; (2) prohibiting such manufacturers from selling or using for advertising purposes the collected recordings of voice commands; and (3) prohibiting the compelling of these manufacturers to incorporate specific features that would

---

[133] *Id.*
[134] *U.S. v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016).
[135] *Id.* at 807.
[136] *Id.* at 809.
[137] *Id.* (citation omitted).
[138] See *Id.* at 803; United States Supreme Court Case Number: 16-6761.

allow law enforcement to monitor conversations through the feature.[139] The bill also prohibited a waiver of these provisions, limited the manufacturers' liability to functionalities they provide at the time of the original sale, and limited the scope of the protected voice recognition data to that which is not processed locally.[140]

The requirement that manufacturers inform users of the voice recognition feature is a worthwhile provision, but likely does not do much in terms of practical effects. Most consumers are aware of the fact that their new smart television can be voice-controlled; it might have even been the reason they bought it in the first place. The real danger for this group is that they are so overjoyed with the voice command technology that they do not consider what the company or the government might be doing with their recorded commands and resulting data. Even if people are unaware of the feature, the likelihood that the consumers will read through all of the disclaimers, privacy agreements, and litany of other warnings provided to them is slim to none. Consequently, the two other main provisions are bigger accomplishments with regard to privacy.

The first of these two provisions, as noted above, prohibits companies from selling or using for any other advertising purposes the recorded voice commands. The second prohibits manufacturers from being compelled to include extra features that would allow for the monitoring of conversations for law enforcement purposes. These are more heavy-hitting than the first because they potentially assuage the two problems with corporate listening that this paper sets forth: that the corporations may abuse the data they collect and that the government may use these devices to collect data on citizens. However, this legislation is limited to "connected televisions" and while that covers the problem presented here with regard to the Samsung Smart TV, it does not account for the Xbox Kinect or Amazon Echo. Given that there are many always-listening technologies other than smart televisions already, and that many more will likely flood the market in the coming years, this type of legislation needs to be more expansive in its scope.

V. CONCLUSION

It seems clear that none of the privacy concerns addressed here will prevent the public from using these always-listening technologies

[139] Cal. Bus. & Prof. Code §22948.20.
[140] *Id.*

today or in the future, though concerns may persist. The Samsung Smart TV scandal was likely blown out of proportion as the possibility of private conversations being overheard is a risk that comes with the territory of owning always-listening technologies. Additionally, its privacy policy was the most coherent and upfront out of the three policies applicable to the Samsung Smart TV, Amazon Echo, and Xbox Kinect. Further, the Fourth Amendment would likely protect always-listening technologies in the home if such a case presented itself to the Supreme Court. Users have both a subjective and objectively reasonable expectation of privacy in using the device. They are almost exclusively used in the home and would consequently divulge intimate details to the government similar to the situation in *Kyllo*. Whether the government can seize information from the corporations is less certain. Justice Sotomayor explicitly stated the third-party doctrine is ill-equipped to deal with today's technologies, correctly opining that it may not remain applicable as more and more information is regularly disclosed to third parties. Her concurrence in *Jones* seems to have planted to the seeds of change, so to speak, at least for circuit courts. The Supreme Court has changed its mind on Fourth Amendment privacy issues before, so it is not farfetched to think that the Court may be willing to rethink the third-party doctrine going forward.