THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XIX STLR.ORG FALL 2017

ARTICLE

PRIVACY AND LIBERTY IN AN ALWAYS-ON, ALWAYS-LISTENING WORLD†

Allison S. Bohm,* Edward J. George,** Bennett Cyphers,*** and Shirley Lu****

The home is often considered the last bastion of privacy and the Fourth Amendment guarantees people the right to be secure in their houses against unreasonable searches and seizures. But today, the government is not the only entity seeking to invade homes to obtain information—technology companies like Amazon and Google are making an aggressive push into homes with devices like Amazon Echo, Google Home, and Apple HomePod. We are entering an always-on, always-connected world. A generation of always-on devices, capable of watching and listening to everything we do, is entering the consumer electronics market. These devices promise to make daily lives easier, safer, and more enjoyable, but they also bring powerful surveillance tools into our most private spaces.

Privacy and security issues associated with always-on, always-listening, and always-watching devices are demanding increased attention. After examining the current state of government regulation and the rapid technological development of always-on devices, this Article argues that existing legal regimes

* J.D. 2017, Georgetown University Law Center.

** J.D. 2017, Georgetown University Law Center.

*** M.Eng. Computer Science, 2017, MIT.

**** M.Eng. Computer Science, 2017, MIT. The authors would like to thank Professors David Vladeck and Alvaro Bedoya of Georgetown Law, and Professors Danny Weitzner and Ilaria Liccardi of MIT for their extensive guidance in the development of this Article. All errors remain those of the authors alone.

are not sufficient to protect consumers. The Federal Trade Commission (FTC), for example, can only protect consumer privacy through sector-specific privacy laws that give the FTC oversight authority or by invoking its Section 5 "unfairness and deception" authority. Moreover, existing laws like the federal Wiretap Act or state one- and two-party consent laws do little to protect consumers from always-on device privacy intrusions. While sector-specific legislation like the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA) offer stronger protection in certain situations, these laws are not comprehensive solutions to the challenges posed by always-on devices.

This Article, developed as part of a collaborative effort between lawyers and data scientists, identifies three major gaps in the current law. First, when and how law enforcement agencies may access sensitive always-on device data is not clearly defined, giving always-on technology the potential to erode Fourth Amendment privacy rights. Second, consumers often lack control over what data always-on devices may collect and what happens to that data once it is collected. Finally, there is insufficient recourse for holding always-on service providers legally accountable for refusing to take data security seriously. This Article proposes model legislation to address these gaps. This proposal enhances consumer control and transparency, regulates law enforcement access to information captured by always-on devices, and requires service providers to adhere to industry security standards or higher security standards set by the FTC. The Article provides a new analytical context to view policies that will increase consumer confidence, protect privacy, and prevent disastrous, costly data breaches as we move towards an always-on, always-connected world.

I. INTRODUCTION

Robin, while away at college, looks down at her phone and notices an email with the subject line "Information Based on Your Questions." The email is advertising oncologists and immunotherapy treatment in her hometown. While email advertisements are nothing new, what is odd is that this ad is specific to cancer treatment, and Robin had not searched for anything online that would result in such a targeted ad. However, Robin does not know that her father, James, was diagnosed a few days earlier with non-Hodgkin's lymphoma. Robin's parents, who are waiting to tell Robin in person, have been having intimate conversations about doctors, treatments, and various medications in their kitchen. Unfortunately, Robin's parents were unaware that their voice-activated smart device, an always-on device, was recording their conversation, singling out key words, and generating targeted ads to every email address linked to the device. In effect, the smart device informed Robin of her father's medical condition.[1]

While Robin's story may seem egregious, companies have been collecting personal data for years through both the Internet and smart devices in order to sell targeted ads. The data collected can reveal the most intimate secrets about an individual—about you.[2]

As biometrically-enhanced smart devices become an even more essential part of daily life, the data collected has never been more personal. The first digital assistants on mobile phones, like Siri and Google Now, required a physical prompt, typically pressing a button, before the device would capture information about the user. Following the success of Siri and Google Now,

---

1. While this scenario is imagined, it is based on the real-life capabilities of behavior-based advertising. *See, e.g.*, Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did,* FORBES (Feb. 16, 2012, 11:02 AM). https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#6d4e87906668. Always-on devices are theoretically capable of gathering the information required to inform behavior-based advertising.

2. *See*, *e.g.*, *id.*

there are devices like Amazon Echo and Google Home, which are always listening for oral prompts like "Okay, Google." By incrementally advancing always-on devices from a physical prompt to always listening, people, like Robin's parents, now interact with always-on devices that record their intimate conversations and potentially sell them to advertisers.[3]

And while this technology brings about a world of new possibilities—hands-free control for people with physical disabilities[4] or voice dictation to improve efficiency in healthcare[5]—there must be reasonable regulation of the collection and use of voice and other intimate data by companies. While the eyes may be the window to the soul, the human voice can be used to detect gender, race, age, and even emotions.[6] As poet Frederick Turner has noted, our personal history is reflected in our voice.[7]

The human voice is an intimate medium. Many of the most private thoughts are expressed first, or only, during face-to-face conversation: coming out about your sexuality, proposing to your loved one, or announcing that you are terminally ill. Most of these conversations occur in the home, often considered the last bastion of privacy.[8] That is why it is not surprising that always-on devices feel more intrusive than older technologies—because they are.

---

3. *See* Gary Robbins, *Tips on Protecting Your Privacy on Amazon Echo and Google Home*, SAN DIEGO UNION-TRIB., (Jan. 5, 2017, 4:00 PM), http://www.sandiegouniontribune.com/news/science/sd-me-echo-home-20170105-story.html.

4. Allen St. John, *Amazon Echo Voice Commands Offer Big Benefits to Users with Disabilities*, CONSUMER REP. (Jan. 20, 2017), http://www.consumerreports.org/amazon/amazon-echo-voice-commands-offer-big-benefits-to-users-with-disabilities/.

5. Joseph Conn, *Nurses Turn to Speech-Recognition Software to Speed Documentation*, MODERN HEALTHCARE (Dec. 12, 2015), http://www.modernhealthcare.com/article/20151212/MAGAZINE/312129980.

6. *See* Susan M. Hughes & Bradley C. Rhodes, *Making Age Assessments Based on Voice: The Impact of the Reproductive Viability of the Speaker*, 4 J. SOC., EVOLUTIONARY, & CULTURAL PSYCHOL. 290, 290 (2011), http://psycnet.apa.org/fulltext/2011-14971-007.pdf (using voice to identify gender, race, age); Harriet M. J. Smith et al., *Concordant Cues in Faces and Voices: Testing the Backup Signal Hypothesis*, EVOLUTIONARY PSYCHOL. (Feb. 10, 2016), http://journals.sagepub.com/doi/full/10.1177/1474704916630317 (using voice to identify emotions).

7. Frederick Turner, *The Human Voice*, 27 AM. ARTS Q. (Spring 2010), http://www.nccsc.net/essays/human-voice.

8. Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 84 (2008).

These devices have the capability to record, share, and even predict our most intimate conversations in the home.[9]

In 2015, Samsung sparked the ire of privacy advocates with an "unsettling" privacy policy for their Smart TVs: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data capture [sic] and transmitted to a third party through your use of Voice Recognition."[10] This language is chilling because it is so vague. It seems to imply that Samsung is able to collect and sell every word spoken in the TV's vicinity—but would the company actually do that? After purchasing the TV, can a consumer ever have a private conversation in his or her living room again? Unfortunately, this kind of policy is not unique. Companies selling always-on devices are able to collect, store, analyze, and share increasing amounts of personal data. But it is often unclear to consumers what kinds of data these devices are collecting, when they are collecting that data, and what companies are really doing with the data.

This lack of transparency, combined with always-on devices' ability to collect massive amounts of data without the user's knowledge, exacerbates the risk of data breaches. Imagine that you purchase the new, voice-activated Hello Barbie toy, which is intended for children six to fifteen, for your child.[11] She plays with it, in private, for months, and the information the Barbie collects about your daughter is saved in the cloud. You are vaguely aware that her information is stored on corporate servers, but you are not sure what information is stored, and you trust the company not to abuse it. Then, even though Mattel (Barbie's manufacturer) follows commonly-accepted security practices, their data center suffers a massive breach. Hours and hours of your child's conversations with her friends and her toy, as well as recordings of ambient sound, are now available for anyone in the world to hear, possibly forever. Her private conversations are no longer private.

This Article examines the technical and legal development of always-on devices and their integration into society. Part II establishes the technical background for this policy proposal,

---

9. *Cf.* Mike Elgan, *Does Google Listen in on Your Life?*, COMPUTERWORLD (Dec. 10, 2016, 4:00 AM), https://www.computerworld.com/article/3149085/search/does-google-listen-in-on-your-life.html.

10. Brian Barrett, *Tech That's Always Listening Isn't Always Creepy*, WIRED (Mar. 17, 2015, 7:00 AM), https://www.wired.com/2015/03/always-listening-tech-isnt-always-creepy/.

11. Barbie - Hello Barbie Doll, AMAZON, https://www.amazon.com/Barbie-DKF74-Hello-Doll/dp/B012BIBAA2 (last visited Jan. 6, 2018).

including a definition for always-on devices and the devices' costs and benefits. Part III discusses real-world incidences of security breaches and the personal and financial damages these breaches have caused. Part IV examines the existing legal framework that may apply to always-on devices and assesses how it fails to protect consumers' privacy. Lastly, Part V presents a multi-part solution to this problem. The goal of this framework is to enable the smooth transition of always-on devices into everyday life while protecting the privacy and intimacy of the consumer.

II. CURRENT TECHNOLOGY

Always-on devices are the result of a natural technological evolution rather than a single innovation. Over the past three decades, electronics and sensors have gotten smaller and cheaper as the Internet has grown exponentially in speed and breadth. Ten years ago, powerful pocket-sized computers merged with phones, cameras, and constant Internet connectivity as "smartphones," devices that collect and stream data about their owners wherever they go. Since then, Internet bandwidth has become faster and cheaper, software for voice recognition and data analysis has improved and matured, and consumers have warmed up to the idea of always-on, always-connected devices. As a result, it is now feasible to build a computer powerful enough to understand voice commands, sell it for under $100, and expect it to maintain a consistent, fast Internet connection on the average American family's coffee table.

An always-on device is a consumer product with one or more electronic sensors capable of collecting and responding to audio, video, and other information-dense data. Always-on devices usually stream portions of that data to a remote party via the Internet, either intermittently or continuously. Always-on devices may be single purpose, such as voice-activated light bulbs, or general purpose, like the Amazon Echo and Google Home. In addition to in-home appliances, products like cell phones and Internet-connected cars can be considered always-on devices. Today, a majority of Americans own smartphones, equipped with GPS and mobile Internet connection, which are capable of streaming continuous location data to remote parties.[12] Always-on devices are not just the future: they are the present.

---

12. Aaron Smith, PEW RES. CTR., *U.S. Smartphone Use in 2015* (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

Smartphones led the first wave of always-on device adoption. Thanks to their popularity, many people already stream data about their activity, their communication, and their location to a private corporation every time they leave home. Today, voice-activated devices are leading the next wave of always-on technology. Many single-purpose household devices, from TV remotes to vacuum cleaners to light bulbs, have recently become available in models with voice-recognition technology.[13] In 2016, 6.5 million voice-activated, always-on devices like the Amazon Echo were sold, and that number was estimated to surpass 24 million in 2017.[14] Soon, it may be difficult to find an American household without some kind of always-recording electronic listening device.

Voice recognition is not the only technological advance driving always-on monitoring. Developments in image processing have made video monitoring more useful and potentially more lucrative.[15] In 2009, MIT alumni launched Affectiva, a company which uses live video feeds to measure emotional reactions to media content in real-time.[16] Around the same time, a startup called Dropcam began developing its eponymous device, which is an always-on video camera for home use that stores video in the cloud. The company was bought by Nest, a subsidiary of Alphabet, Inc., which now markets the device as Nest Cam, an always-recording camera that can automatically detect and report events such as a human entering the frame.[17] Furthermore, recent research has shown that unconventional forms of monitoring, such as sensors that measure low-frequency radio waves, can be used to estimate biometrics, human location, gestures, and emotion.[18] In

---

13. Nancy Young, *15 Voice-Controlled Gadgets*, HONGKIAT, http://www.hongkiat.com/blog/innovative-voice-activated-gadgets/ (last visited Nov. 5, 2017).

14. *See* Adam Marchick, *The 2017 Voice Report*, VOICELABS (Jan. 15, 2017), http://voicelabs.co/2017/01/15/the-2017-voice-report/.

15. Ying Yin & Randall Davis, *Real Time Continuous Gesture Recognition for Natural Human-Computer Interaction*, 2014 IEEE SYMP. ON VISUAL LANGUAGE AND HUM.-CENTRIC COMPUTING, https://groups.csail.mit.edu/mug/pubs/Yin2014Realtime.pdf.

16. *Media and Advertising*, AFFECTIVA, http://www.affectiva.com/what/uses/media/ (last visited Nov. 5, 2017).

17. *See* Katherine Boehret, *Always-On Dropcam Proves Helpful, However Creepy*, RECODE (Mar. 19, 2014, 7:00 AM), https://www.recode.net/2014/3/19/11624704/always-on-dropcam-proves-helpful-however-creepy; *Meet the Nest Cam Indoor Security Camera*, NEST, https://nest.com/cameras/nest-cam-indoor/overview/ (last visited Nov. 9, 2017).

18. *See* Mingmin Zhao et al., *Emotion Recognition Using Wireless Signals*, PROC. 22ND ANN. CONF. MOBILE COMPUTING & NETWORKING 95 (2016); Fadel

2015, an MIT professor and two graduate students presented Emerald, a method for predicting falls among senior citizens using always-on WiFi-spectrum sensors, at the White House's "Demo Day."[19] These developments suggest that always-on devices with even more advanced monitoring capabilities will be deployed in the near future.

Always-on devices promise tremendous benefits to consumers. Several companies have already built multi-million-dollar businesses with novel applications for in-home sensors and computers.[20] Medical devices, such as pacemakers and diabetic sensors, can be enhanced with always-on Internet connectivity, making it easier for doctors to monitor patients and administer care remotely. Car companies like Tesla, which provide software-enhanced driving experiences, are able to develop and remotely activate new features for customers of older car models.[21] Products like the Amazon Echo and Google Home are early steps toward general in-home automation, a futurist consumer dream since the days of animated sitcom *The Jetsons*.[22]

Unfortunately, always-on devices expose consumers to new privacy risks. By their nature, these devices have the ability to collect video, audio, location data, and more. They can stream that data to remote servers, where companies can use it to derive powerful insights. In particular, the authors of this Article are concerned about the trend towards constant collection of audio and video data. Currently, Amazon and other large voice-activated product manufacturers claim their devices stream audio to the

---

Adib et al., *Smart Homes that Monitor Breathing and Heart Rate*, PROC. 33RD ANN. ACM CONF. ON HUM. FACTORS COMPUTING SYS. (2015), http://dl.acm.org/citation.cfm?id=2702200.

19. Adam Conner-Simons, *President Obama Invites MIT Entrepreneurs to Give Demo at the White House*, MIT NEWS (Aug. 6, 2015), http://news.mit.edu/2015/president-obama-meets-mit-entrepreneurs-white-house-demo-day-0806.

20. *See*, *e.g.*, *Breaking Down the Valuation for Nest's $3.2 Billion Purchase Price*, NEXT MARKET BLOG (Jan. 14, 2014, 12:59 PM), http://blog.nextmarket.co/post/73320622998/breaking-down-the-valuation-for-nests-32; *Samsara Company Profile*, CRUNCHBASE, https://www.crunchbase.com/organization/samsara-2 (last visited Nov. 12, 2017); *SmartThings Company Profile*, CRUNCHBASE, https://www.crunchbase.com/organization/smartthings (last visited Nov. 10, 2017).

21. Alex Brisbourne, *Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things?*, WIRED, *https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/* (last visited Nov. 12, 2017).

22. In the show, the titular family owns several devices for automating simple tasks around the house, including Rosie the Robot, a mechanical maid who responds to voice commands.

cloud only when activated by a "wake word" like "Alexa."[23] While there is no reason to disbelieve them yet, there is little stopping these vendors from collecting greater amounts of data in the future.

Many consumers may not realize the full scope of data being collected by their devices. It is often difficult for consumers to tell what sensing capabilities an always-on device actually has. Some of these concerns have already been borne out.[24] In 2014, Vizio began selling TVs with hidden cameras installed behind the screen in order to monitor what their users were watching.[25] The company discretely collected users' viewing habits and sold individualized viewing histories to advertisers. The tracking functionality could technically be turned off by users under a setting called "Smart Interactivity," but the company failed to adequately explain how this "feature" actually worked. After the Federal Trade Commission (FTC) filed a formal complaint early in 2017, Vizio was ordered to halt the program and pay a $2.2 million penalty—less than one tenth of one percent of its annual revenue.[26] More examples of concerning corporate behavior are detailed in Part III.

In terms of both intimacy and sheer volume, the personal data collected by always-on devices is unprecedented. Consumers have become accustomed to corporate monitoring of certain aspects of their lives—emails, web browsing habits, and, more recently, location data via GPS-enabled smartphones. But always-on devices will be able to provide corporations with constant streams of audio and video from consumers' most intimate spaces. A complicating

---

23. A "wake word" is a particular word or phrase which activates a device's higher-level audio processing functions. Many voice-activated always-on devices remain in a semi-inactive state and process audio data locally until they recognize a wake word; then, they stream whatever audio follows to a remote datacenter for more complex processing. For example, Amazon's Alexa FAQs state: "When [Amazon Echo and Dot] detect the wake word, they stream audio to the Cloud, including a fraction of a second of audio before the wake word." *Help & Customer Care: Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (last visited Mar. 8, 2017).

24. This practice occurred without giving consumers proper notice or acquiring consent, and resulted in FTC action against Vizio. Lesley Fair, *What Vizio was Doing Behind the TV screen*, FED. TRADE COMM'N, (Feb. 6, 2017, 11:05 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen.

25. *Id.*

26. In 2016, the company's total revenue was $3.5 billion. *America's Largest Private Companies: Vizio*, FORBES, https://www.forbes.com/companies/vizio/ (last visited Nov. 12, 2017).

issue is data security. Even if consumers are willing to trust service providers with such data, what if that data is stolen? Always-on device manufacturers and service providers take on an awesome responsibility when they monitor so much of a person's life. If private conversation records leak, careers may be lost, reputations may be ruined, or relationships may be destroyed. Data breaches are already a serious problem for even the largest, wealthiest companies.[27] As always-on data makes its way into more hands, breaches will only become more costly and more dangerous.[28] Without improved security standards, they may become more numerous as well.

III. INCIDENTS AND DAMAGES

Privacy concerns over microphone-enabled always-on devices had begun to emerge by 2014. That year, the Google Chrome web browser drew criticism for its built-in ability to passively listen for the words "Okay, Google" to launch a voice-activated search function. Low rates of user adoption eventually led Google to remove the feature.[29] In 2015, the FTC received numerous complaints about Samsung's microphone-enabled SmartTV always being on.[30] Privacy advocates claim that Samsung violated the federal Wiretap Act,[31] as users noticed that Samsung's privacy policy warned that sensitive conversations might be swept up and transmitted to third parties as part of the TV's voice-controlled search function.[32] Despite Samsung's assertion that the TV only recorded and transmitted information when the user pushed a

---

27. In 2013, Yahoo lost more than one billion user credentials, many of which were not strongly encrypted. Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html. *See also* more examples, *infra* Part III.

28. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

29. *See* Matt Elliott, *Chrome drops 'OK Google' voice search*, CNET (Oct. 19, 2015), https://www.cnet.com/how-to/chrome-46-drops-ok-google-voice-search/.

30. *E.g.*, *In re. Samsung, Compl., Req. for Investigation, Inj., and Other Relief*, ELEC. PRIVACY INFO. CTR. (Feb. 24, 2015), https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

31. The Wiretap Act prohibits intentionally intercepting "any wire, oral, or electronic communication" of someone who does not have an "expectation" that it will be intercepted. 18 U.S.C. § 2511 (2012).

32. *Letter to Attorney General Loretta Lynch and FTC Chairwoman Edith Ramirez*, ELEC. PRIVACY INFO. CTR. (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf [hereinafter *EPIC Letter*].

button on the remote control to activate voice searching,[33] many advocates remained skeptical.

Early in 2017, Spiral Toys left two million messages recorded by its digital teddy bear brand Cloudpets exposed in a vulnerable online database.[34] Due to the vulnerability, anyone could find the messages parents recorded for their children with the Internet of Things ("IoT")[35] search engine Shodan and listen to those messages. The breach included 800,000 sets of credentials, including email addresses and passwords, not all of which were strongly encrypted.[36]

Then, in October, tech journalist Artem Russakovskii reported that an early-access version of Google's new Home Mini device had been acting strangely.[37] While the device was only supposed to record audio in response to a wake word or touch event, due to a hardware bug, the device was registering "phantom" activation signals every few seconds. As a result, near-constant audio from Russakovskii's home was being streamed to Google and saved remotely.[38]

The IoT has developed a reputation for poor security, and many security researchers have published articles demonstrating how to hack into common IoT devices. Wes Wineberg, an Internet security researcher, published on Synack an explanation of how to

---

33. Samsung's Privacy Policy was modified to state: "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." Press Release, *Samsung Smart TVs Do Not Monitor Living Room Conversations*, SAMSUNG (Feb. 10, 2015), https://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations; *see also* Alex Hern, *Samsung Rejects Concern over 'Orwellian' Privacy Policy*, THE GUARDIAN (Feb. 9, 2015), http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy.

34. *Security News This Week: An IoT Teddy Bear Leaked Millions of Parent and Child Voice Recordings*, WIRED (Mar. 4, 2017), https://www.wired.com/2017/03/security-news-week-iot-teddy-bear-leaked-millions-parent-child-voice-recordings/ [hereinafter *Security News*].

35. In this Article, the Internet of Things refers generally to physical devices and objects not traditionally identified as computers which have been embedded with electronic sensors, computing processors, and network connectivity.

36. *Security News*, *supra* note 34.

37. *See* Artem Russakovskii, *Google is Permanently Nerfing Home Minis Because Mine Spied on Everything I Said 24/7*, ANDROID POLICE (Oct. 10, 2017), http://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/.

38. *Id.*

hack fourteen IoT devices, including hardware, PC apps, mobile apps, and cloud communities.[39] Synack is a website that "leverages the best combination of humans and technology to discover security vulnerabilities in [their] customers' web apps, mobile apps, and infrastructure endpoints."[40] Numerous sites like Synack exist on the Internet to teach readers how to exploit vulnerabilities in IoT devices. A GitHub[41] user under the name of nebgnaz has created a repository called "Awesome IoT Hacks," which is a lengthy curated list of vulnerability exploits in the IoT space.[42] This information could easily be used for malicious actions.

With respect to law enforcement, civil liberties organizations like the American Civil Liberties Union (ACLU) are wary of government requests for access to always-on device data for investigative purposes.[43] In Bentonville, Arkansas, police obtained a warrant to access audio records of a suspect's Amazon Echo,[44] sparking a debate over the privacy implications of surveillance devices in homes.[45] Unfortunately, existing statutes governing the interception of voice communications do not address the situation now at hand. It is unclear whether or how existing law regulates collection of or access to such data.[46]

Consumers need a legal framework to address these risks. The framework should provide security guidelines for manufacturers and developers of always-on devices. Additionally, it should protect consumer privacy by providing law enforcement agencies with clear rules governing when and under what rubric they can

---

39. *See* Wes Wineberg, *Hacking 14 IoT Devices,* IOT Village, https://www.iotvillage.org/slides_DC23/IoT11-slides.pdf (last visited Nov. 12, 2017).

40. *Id.*

41. Github.com is a website which primarily hosts open-source software projects, in units called "repositories," and related discussion. GITHUB, https://github.com (last visited Jan. 6, 2018).

42. *A Collection of Hacks in IoT Space*, GITHUB, https://github.com/nebgnahz/awesome-iot-hacks (last visited Mar. 7, 2017).

43. *See* Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/free-future/privacy-threat-always-microphones-amazon-echo.

44. *See* Tom Dotan & Reed Albergotti, *Amazon Echo and the Hot Tub Murder*, THE INFO. (Dec. 27, 2016), https://www.theinformation.com/amazon-echo-and-the-hot-tub-murder?eu=JnmYMZlQZHz7uehZk0Lvtg.

45. *See* Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. TIMES (Dec. 28 2016), https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html.

46. *See* Barrett, *supra*, note 10.

access always-on device information for investigative purposes. That legal framework is largely missing today.

IV. LEGAL FRAMEWORK

The Fourth Amendment guarantees people the right to be secure in their houses against unreasonable searches and seizures.[47] And courts have applied the Fourth Amendment vigorously to bar governmental intrusions into homes.[48] But today, the government is not the only entity seeking to invade homes to obtain information—technology companies are making an aggressive push. Amazon Echo, Google Home, and Hello Barbie are just a few examples of always-on devices that have the ability to record intimate conversations in the home. Although always-on technology raises consumer privacy and electronic surveillance issues, it remains largely unregulated.

While there are commercial privacy laws, like the Video Privacy Protection Act[49] and the Electronic Communications Privacy Act,[50] none of them fully address the information collected by always-on devices.[51] Therefore, any breach or misuse of the information collected by the devices will be left to the regulatory purview of the FTC. The FTC, under its Section 5 authority, can pursue companies for "unfair or deceptive acts or practices in or affecting commerce."[52] The FTC has used this authority to bring enforcement actions against companies for alleged privacy violations in products they develop and market for public use—but

47. U.S. CONST. amend. IV.

48. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (holding thermal imaging of a personal home constitutes a search under the Fourth Amendment); Wilson v. Layne, 526 U.S. 603 (1999) (holding media ride-alongs with police into private residences violate the Fourth Amendment); Silverman v. United States, 365 U.S. 505 (1961) (holding eavesdropping devices touching a residence were unauthorized physical penetrations under the Fourth Amendment); Weeks v. United States, 232 U.S. 383 (1914) (holding that taking letters from the defendant's house was a violation of his Fourth Amendment rights).

49. Video Privacy Protection Act, 18 U.S.C. § 2710 *et seq.* (2012).

50. Electronic Communications Privacy Act, Pub. L. 99–508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C).

51. However, it is likely that the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq.* (2012), would apply if the user of an always-on device were twelve years old or younger. COPPA imposes certain privacy requirements on operators of online services directed toward children under thirteen years of age. *See* FTC Children's Online Privacy Protection Rule, 16 C.F.R § 312 (2013).

52. 15 U.S.C. § 45(a)(2) (2012).

the FTC can only use this authority in limited circumstances—when a company has acted deceptively or unfairly.[53] Unless a company triggers a Section 5 violation, the FTC cannot get involved, and because the information always-on devices capture is extremely sensitive, Section 5 alone is an insufficient protection for consumers. For the most part, companies are legally protected as long as they disclose the extent of their data collection. Consumers have been bound to the long, legalistic Terms of Service and Privacy Policies with which they must agree to use most digital products and services; few read them and fewer challenge them.[54]

With respect to government surveillance, for over forty years America's electronic surveillance law has drawn a distinction between the protections afforded to communications content and non-content (also known as metadata).[55] In 1967, the Supreme Court in *United States v. Katz* first recognized Fourth Amendment protections for the content of telephone conversations, holding that the interception of conversations is a search and that a warrant is required.[56] Twelve years later, in 1979, the Court in *Smith v. Maryland* addressed the constitutional question about non-content information stored by telephone companies, finding that dialed telephone numbers are not communications content and therefore are not given Fourth Amendment protection.[57] Moreover, the Court held that a person does not have Fourth Amendment protections for information disclosed to a third party.[58]

---

53. *See, e.g.*, *Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk*, FED. TRADE COMM'N (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

54. *See* Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services,* 44TH RES. CONF. ON COMM., INFO. & INTERNET POL'Y (Aug. 24, 2016).

55. *See* Steven M. Bellovin, et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 HARV. J. L. TECH. 1, 4 (2016).

56. *Id.* at 5.

57. *Id.*

58. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976) (holding that bank records do not have Fourth Amendment protections because they are financial documents used in the ordinary course of business); Couch v. United States, 409 U.S. 322 (1973) (holding that there are no Fourth Amendment protections in records handed to an accountant); On Lee v. United States, 343 U.S. 747 (1952) (holding that there are no Fourth Amendment protections in making voluntary, incriminating statements to an undercover informant).

Katz and *Smith* established two major precedents in electronic surveillance law: the content/non-content distinction and the third-party doctrine.[59] But since that time, communications technology has rapidly become more complex, and the distinctions between content and non-content have blurred. This raises a series of legal questions for manufacturers of always-on devices, including whether always-on devices are subject to federal surveillance laws.

A. The Wiretap Act

Because always-on devices record conversations in the home, questions arise about whether the devices may constitute unlawful surveillance under federal wiretap law.[60] Following the Supreme Court's decisions in *Berger v. New York*[61] and *Katz*,[62] Congress enacted the Wiretap Act,[63] creating a uniform set of rules that comply with the Fourth Amendment while allowing the government to intercept wire and oral communications in criminal investigations.[64]

The Wiretap Act prohibits any person from intentionally intercepting "any wire, oral, or electronic communication" without a warrant.[65] Whether this prohibition applies to companies like Amazon and Google seems to depend on whether the user expects the always-on device to record the conversation. "Oral communication" is defined as "any oral communication uttered by a person exhibiting *an expectation* that such communication is not subject to interception under circumstances justifying such expectation,"[66] and "intercept" is defined as the "aural or other acquisition of the contents of any . . . oral communication through the use of any [device]."[67] Therefore, an argument can be made

---

59. *See* Part IV.B, *infra*.

60. *See EPIC Letter*, *supra* note 32.

61. Berger v. New York, 388 U.S. 41, 51 (1967) (holding that "a court order does not purify an otherwise unconstitutional physical invasion and electronic search where the enabling statute is invalid due to its allowance of eavesdropping for general purposes and without the belief that a crime is being committed for a protracted period of time."); *see* Kenneth Ira Solomon, *The Short Happy Life of Berger v. New York*, 45 CHI.-KENT. L. REV. 123, 123-24 (1968).

62. Katz v. United States, 389 U.S. 347, 348 (1967).

63. 18 U.S.C. § 2510 *et seq.* (2012).

64. *See* Bellovin, *supra* note 55.

65. 18 U.S.C. § 2511(1)(a) (2012).

66. *Id.* § 2510(2) (emphasis added).

67. *Id.* § 2510(4).

that as long as the user expects the communication to be intercepted, the device's manufacturer would not be in violation of the Act.

But relying on user expectation may cause legal headaches for companies. What if the user is not aware that the always-on device records his or her conversations? Or what if the user believes that the device only records the interaction with the device when in fact the device records the sixty seconds after the interaction as well? Or what if the user is unaware that the device records any and all conversations the device picks up? Will these be considered violations under the Wiretap Act? Companies may argue that the owner of the always-on device expresses his or her expectation to be recorded the moment he or she purchases the device and that the owner's expectation resolves any Wiretap Act concerns. But this result is hardly a given and relies on the customer's understanding of how the device functions. As the foregoing questions indicate, many of the devices available today simply are not marketed with sufficient information to enable consumers to understand and develop reasonable expectations about how the devices function—and when they are listening. As a result, this could be a litigation nightmare for the makers of always-on devices.[68]

Any conversation captured by an always-on device is protected "content" as defined under the Wiretap Act. Content is defined as "any information concerning the substance, purport, or meaning of that communication."[69] Therefore, any attempt by law enforcement to wiretap an always-on device to collect conversations in real-time would be subject to the Act's warrant standards.[70] But what if a law enforcement agency wants to access the audio stored on the server? Would the stored audio be afforded Fourth Amendment protections?

B. The Third-Party Doctrine

In late November 2015, James Andrew Bates was charged with murder after his friend, Victor Collins, was found floating face-up

---

68. For a discussion of so-called "shrink-wrap licenses" (or agreements consumers purportedly consent to by purchasing and using a product), *see generally* 27A WEST'S LEGAL FORMS, SPECIALIZED FORMS § 10:33. For a discussion of what constitutes meaningful consent, *see generally* Orit Gan, *The Many Faces of Contractual Consent*, 65 DRAKE L. REV. 615 (2017).

69. 18 U.S.C. § 2510(8) *et seq.* (2012).

70. *Id.* §§ 2516, 2518.

in Bates's hot tub.[71] The police found an Amazon Echo when searching Bates's home and obtained a search warrant to access the data collected by the Echo. But Amazon refused the warrant twice.[72] Eventually, Bates himself agreed to hand over the recordings, and Amazon complied.[73] In this case, law enforcement established probable cause and acquired a search warrant. Amazon challenged the court's request for voice data on First Amendment grounds, and the issue of whether law enforcement needed to obtain a warrant was avoided.[74] However, in light of the third-party doctrine, it is worth stepping back to consider whether information obtained by an always-on device—and therefore shared with a third-party service provider—is protected by the Fourth Amendment at all.

Under the third-party doctrine, "a person cannot have a reasonable expectation of privacy in information disclosed to a third party" like Amazon, and, therefore, the Fourth Amendment does not apply to data shared with third parties.[75] For example, in *United States v. Miller*,[76] Miller had been convicted of various crimes having to do with the unlicensed production of whiskey and the failure to pay taxes. In furtherance of its case against Miller, the government issued subpoenas to two of Miller's banks, and the banks complied with the subpoenas.[77] The government used the evidence collected from the banks to convict Miller at trial. On appeal, Miller argued that his Fourth Amendment rights were violated when the government failed to obtain a warrant to access the bank records. Justice Powell, for the majority, held that "in revealing [Miller's] affairs to another," Miller had assumed the risk

---

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

72. *See* Elliot C. McLaughlin & Keith Allen, *Alexa, Can You Help with this Murder Case?*, CNN (Dec. 28, 2016), http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/.

73.. *See* Amy B. Wang, *Can Amazon Echo Help Solve a Murder? Police Will Soon Find Out*, WASH. POST (Mar. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/09/can-amazon-echo-help-solve-a-murder-police-will-soon-find-out/.

74. *See* Brian Heater, *Amazon Hands Over Echo Data in Arkansas Murder Trial*, TECHCRUNCH (Mar. 7, 2017), https://techcrunch.com/2017/03/07/amazon-echo-murder/.

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

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

77. *Id.* at 436-37.

"that the information [would] be conveyed by that person to the Government."[78] It follows that a court could conclude that any conversation recorded and stored by an always-on device should not receive Fourth Amendment protection. An always-on device owner "reveal[s] his affairs to another"—in fact, his affairs are transmitted to the cloud—and assumes the risk that "the information [will] be conveyed . . . to the government." Under this rationale, law enforcement could access the always-on device information without needing to first obtain a warrant. While it is promising to see law enforcement seek a warrant and Amazon fight to protect consumers' information in the Bates case, Amazon is just one company, and the Bentonville Police Department is only one law enforcement agency. Legally, companies are not required to fight to protect the information shared with them and law enforcement may not be required to seek warrants under the third-party doctrine.[79]

As a result, this Article takes the view of Justice Marshall's dissent in *Smith v, Maryland*.[80] Specifically, Marshall argued that just because consumers share information with a business, "it does not follow that they expect this information to be made available to . . . the government in particular."[81] Further, while one may argue, as the majority did in *Smith*, that individuals who convey information to third parties have "assumed the risk" of disclosure to the government, the Article agrees with Marshall that "[i]mplicit in the concept of assumption of risk is the notion of choice."[82] As society becomes more dependent upon technology that readily shares information with third parties, implicit notions of choice change as consumers will not forgo their technological products due to lengthy terms of service agreements. Consumers should be afforded the highest Fourth Amendment protections possible, and those protections should not turn on the whim of a corporation that could voluntarily hand over information to the government. Therefore, this proposed legislation (discussed in the next section)

---

78. *Id.* at 443; it is worth mentioning that Congress overturned *Miller's* narrow holding with respect to items given to financial institutions by passing the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq.* (2012), though the Third Party Doctrine remains good law as of publication.

79. It is likely that Amazon fought to protect Bates's information, because the company recognized that consumers will be less likely to share information with Amazon and to purchase Amazon devices if they believe information shared with Amazon could be shared with the government.

80. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979).

81. *Id.*

82. *Id.*

abolishes the third-party doctrine for always-on device data and requires law enforcement to obtain a warrant before accessing data held by a third party.

C. One- and Two-Party Consent

Consent law is another area where always-on devices implicate existing legal regimes. As discussed earlier, the Wiretap Act prohibits the intentional interception of oral communications without the prior consent of at least one of the parties. And most states have similar statutes that require at least one party to consent before recording a private conversation.[83] In fact, in twelve states, one can only record a private conversation if all parties to the conversation have given their prior consent, an approach known as two-party consent.[84]

Consent is tricky for always-on devices. Legally, companies have to get the owner's consent before the owner can operate the device, which companies often do by asking the customer to agree to a terms of service agreement or by printing a disclaimer on the product's box or including such a disclaimer in the packaging. But, always-on devices present unique problems for companies seeking to obtain user consent. What if the owner's friend comes over and asks the device a question? Does the company have to get the friend's consent before processing the question? Suppose Person A is asking the device a question while Person B is having a conversation in the background and is unaware the device is also recording what she is saying. How does consent law apply there? Or assume the Echo purchaser lives in one of the two-party consent states, and she throws a Super Bowl party. How does Amazon, or any company for that matter, obtain the consent of

---

83. *See generally State Law: Recording*, DIG. MEDIA L. PROJECT (Mar. 4, 2017), http://www.dmlp.org/legal-guide/state-law-recording.

84. *See* STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 7 n.26 (Apr. 2016), https://www.ftc.gov/system/files/documents/public_comments/2016/08/00003-128652.pdf (citing CAL. PENAL CODE § 632 (2016); CONN GEN. STAT. § 52-570d (2016) (applying only to telephonic conversations); FLA. STAT. § 934.03 (2016); 720 ILL. COMP. STAT. 14/1 *et seq.* (2008); MD. CODE, CTS & JUD. PROC. § 10-402 (West 2016); MASS. GEN LAWS ch. 272, § 99 (2016); MICH. COMP. LAWS § 750.539c (2016); MONT. CODE ANN. § 45-8-213 (2016); NEV. REV. STAT. ANN. § 200.620 (2015) (applying only to "wire" or telephonic conversations); N.H. REV. STAT. ANN. § 570-A:2 (2016); 18 PA. CONS. STAT. § 5703 (2016); WASH. REV. CODE § 9.73.030 (2015)).

every party guest? Because always-on devices do not fit neatly into current consent regimes, they require a retooling of consent.

V. PROPOSED SOLUTION

This Article proposes a multi-part privacy intervention for always-on devices. The proposal addresses (a) law enforcement access to information captured by always-on devices, (b) individual consumer control and transparency, (c) data retention, (d) the rights of third parties, and (e) security.

A. Law Enforcement Access to Information Captured by Always-On Devices

Law enforcement agents should be required to obtain a probable cause warrant in order to access information captured by an always-on device. The warrant requirement should take into account whether data is acquired from the service provider or manufacturer of the device by means of physical or electronic interaction with the device, or from any third party who may have access to data captured by the device. However, law enforcement agents should be permitted to obtain a warrant after the fact in exigent circumstances. The government should be permitted to access always-on device data only with consumer consent or in order to react to a life or limb-threatening emergency where no criminal wrongdoing is suspected. But where law enforcement agents access information from an always-on device absent a probable cause warrant or consumer consent, the information obtained should be barred by the Fourth Amendment's exclusionary rule.

In addition, when law enforcement agents access always-on device data from a service provider pursuant to a warrant, they should be required to notify the individual whose information is being accessed in order to satisfy the warrant's notice requirement. The consumer, not the service provider, is in the best position to vindicate his or her rights. Courts should be permitted to delay notification under exigent circumstances: when immediate notice would endanger the safety of an individual, seriously jeopardize an investigation, unduly delay a trial, engender flight from prosecution, lead to destruction of or tampering with evidence, or lead to the intimidation of potential witnesses.

Obtaining always-on device data grants the government access to information from within the boundaries of the home, a space

that has always been sacred under the Fourth Amendment.[85] The Supreme Court has been reluctant to withdraw the Fourth Amendment's protection of the home, even in the face of cutting-edge technology that is capable of rendering private details public. In *Kyllo v. United States*, a case pertaining to the government's warrantless use of heat sensors to determine whether the defendant was growing marijuana inside his home, the Supreme Court observed that:

> To withdraw protection of this minimum expectation would be to permit . . . technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search.[86]

Similarly, always-on devices capture their users' faces and voices—unique biometric identifiers. Biometrics are particularly sensitive because they are both revealing and permanent: one cannot simply change one's face if it becomes inconvenient to wear. Studies have shown that consumers are much less likely to agree to share biometric data than other personal identifiers, such as birth date, address, age, and marital status.[87] In recent years, several states have passed laws granting heightened privacy protections to biometrics.[88]

Since the Wiretap Act,[89] U.S. law has recognized the sensitivity of voice data and oral communications, prohibiting the interception and disclosure of wire, oral, or electronic

---

85. *E.g.*, United States v. Jones, 565 U.S. 400, 405-07 (2012) ("The text of the Fourth Amendment reflects its close connection to property . . . [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding.").

86. Kyllo v. United States, 533 U.S. 27, 34 (2001) (internal citation omitted).

87. Fifty-six percent of consumers surveyed were willing to share date of birth and address, 53% age, gender and marital status, but only 11% would share biometrics such as facial recognition and fingerprints. *Microsoft Research Reveals Understanding Gap in the Brand-Consumer Data Exchange*, MICROSOFT APAC NEWS CTR. (June 3, 2015), https://news.microsoft.com/apac/2015/06/03/microsoft-research-reveals-understanding-gap-in-the-brand-consumer data-exchange/.

88. *See* 740 ILL. COMP. STAT. 14/1 *et seq.* (2008); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017); H.R. 299, 2017 Leg., 65th Reg. Sess. (Wash. 2017).

89. 18 U.S.C. § 2510 *et seq.* (2012).

communications except in select, enumerated circumstances.[90] Under the Act, real-time communications receive even greater protection than other forms of information or property. Law enforcement is permitted to intercept wire, oral, or electronic communications only where a judge has found probable cause, only during investigations of certain enumerated, more serious crimes,[91] and only when normal investigative procedures appear unlikely to succeed, have already failed, or are too dangerous to attempt.[92]

Always-on devices implicate two sensitivities: they capture unique biometric identifiers about their users, and they penetrate the home and capture information that previously could only be obtained by "physical intrusion into a constitutionally protected area."[93] For this reason, the warrant and probable cause standard is the appropriate standard for law enforcement access to always-on device information.

Law enforcement agencies will likely resist the warrant and probable cause standard on the basis that always-on devices convey information to third parties, stripping users of their reasonable expectation of privacy and rendering the information more easily available to law enforcement under the third-party doctrine. However, the third-party doctrine has never been an absolute. For example, "[t]he government may not freely search a rented apartment or tap a telephone wire the caller does not own."[94] Moreover, life in the digital age requires individuals to turn over massive amounts of information to third-parties that heretofore were physically stored in the home or simply destroyed. Therefore, it is time to re-think or eliminate the third-party doctrine. However, lawmakers can address the risks posed by always-on technology more narrowly. Because of the sensitivity of voice data and information collected by cutting-edge technology from within the boundaries of private homes, lawmakers should clarify that the third-party doctrine simply does not apply to always-on devices.

---

90. *Id.* § 2511.

91. *Id.* § 2516.

92. *Id.* § 2518.

93. Kyllo v. United States, 533 U.S. 27, 34 (2001).

94. Elizabeth Goitein, *United States v. Davis – Wrestling with the Third Party Doctrine*, JUST SEC. (May 13, 2015), https://www.justsecurity.org/22989/united-states-v-davis-wrestling-party-doctrine/.

Law enforcement will likely also invoke a "parade of horribles" argument[95] and insist that information from always-on devices is necessary for solving crimes. First, a warrant will almost invariably issue when law enforcement has a sufficiently compelling case that access to always-on device data is needed to solve a crime. Second, this proposed solution includes emergency and exigent circumstances exceptions to permit law enforcement access to always-on device information in a life or limb-threatening situation when there is not time to first obtain a warrant. Third, law enforcement has been solving crimes for centuries without always-on device information, and this proposed legislation would not foreclose the use of any longstanding investigative techniques or practices.

Law enforcement's probable objections provide good reason to legislate protections for always-on devices immediately. It will be much easier to put reasonable protections in place before law enforcement access to the technology is widespread. Otherwise, in the future, the government could plausibly argue that it is losing a tool it is accustomed to using.

B. Individual Control and Transparency

Always-on device manufacturers and service providers should provide the consumer with an easy-to-use dashboard that permits her to access the information about herself that her device has transmitted to the service provider's servers. The consumer should also be permitted to delete any information that she wishes not to be retained. Always-on device service providers and manufacturers should also obtain separate, informed consent for any information shared with third parties. This Article recommends that each separate type of use be agreed to with a separate screen or voice prompt, as appropriate for a given device. Furthermore, prior to purchasing the always-on device, the consumer should be informed whether the failure to consent to a particular type of data disclosure would jeopardize the functionality of the device. Importantly, third parties, such as advertisers, should be treated as service providers for the purposes of the consent provisions in order to stem unfettered, secret tertiary data sharing. Both the dashboard and informed consent provisions would be enforceable

95. *See generally* Ben Zimmer, *Where Did the Supreme Court Get its 'Parade of Horribles'?*, BOS. GLOBE (July 1, 2012), https://www.bostonglobe.com/ideas/2012/06/30/where-did-supreme-court-get-its-parade-horribles/Y0jnIscamtgPEzO0PdtL9N/story.html.

by the FTC and by a private right of action. These solutions apply the Fair Information Practice Principles (FIPPs) and the Consumer Privacy Bill of Rights to always-on devices. They may also be good for business.

This Article refers to the FIPPs because for decades they have articulated widely agreed-upon best practices. A version of the FIPPs was first adopted by the Health Education and Welfare Advisory Committee in 1973 as the Code of Fair Information Practices.[96] The FTC, after consulting with industry groups, subsequently updated the Code for the digital age and released the current version of the FIPPs.[97] The FIPPs, which reflect longstanding American values, insist that a:

> . . . widely-accepted core principle of fair information practice is consumer choice or consent . . . . Specifically, choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction . . . .
>
> . . . Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.[98]

The FIPPs also advise that "[a]ccess is . . . [a] core principle. It refers to an individual's ability . . . to . . . access data about him or herself—*i.e.*, to view the data in an entity's files . . . ."[99]

In addition, the Individual Control section of the Consumer Privacy Bill of Rights stipulates that "[c]onsumers have a right to exercise control over what personal data companies collect from them and how they use it . . . . Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure."[100] Similarly, the Consumer Privacy Bill of Rights calls for "easily understandable and

---

96. *The Code of Fair Information Practices*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/consumer/code_fair_info.html (last visited May 4, 2017).

97. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (June 1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter PRIVACY ONLINE].

98. *Id.* at 8-9.

99. *Id.* at 9.

100. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 4 J. PRIVACY & CONFIDENTIALITY 95, 104 (2012).

accessible information about privacy and security practices."[101] Finally, the Consumer Privacy Bill of Rights stipulates that "[c]onsumers have a right to access . . . personal data."[102] Although the Consumer Privacy Bill of Rights was never adopted, the White House's big data and privacy working group called for the advancement of the Consumer Privacy Bill of Rights based on input from "academic researchers and privacy advocates, regulators and the technology industry, and advertisers and civil rights groups," as well as the general public.[103] This suggests that the Consumer Privacy Bill of Rights has earned the support of at least some consumers, advocates, regulators, and technology industry leaders.

There is also reason to believe that the user dashboard and informed consent requirements could be good for business:

> Users want to be in control of how their information is used or shared. Failing to obtain explicit consent to use or share personal information . . . risks alienating existing users and discourages others from joining . . . .
>
> . . . .
>
> . . . [G]iving users the ability to choose how and whether . . . information is collected, used, or shared can increase [consumer] trust.[104]

Furthermore, consumers may be more likely to share information with always-on devices if they know they will have the ability to delete it later. "Negative publicity from denying users the right to [delete information] may far outweigh any marginal benefit from retaining their information."[105] The two largest companies in the always-on space, Amazon and Google, already provide rich dashboards allowing users to control their own data. This demonstrates that such features are hardly a competitive disadvantage.

---

101. *Id.* at 108.

102. *Id.* at 114.

103. The White House, *Big Data: Seizing Opportunities, Preserving Values, Interim Progress Report* (Feb. 2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.

104. NICOLE A. OZER & CHRIS CONLEY, PRIVACY & FREE SPEECH: IT'S GOOD FOR BUSINESS 18-16 (ACLU of Cal., 3rd ed. 2016).

105. *Id.* at 19.

Nonetheless, device manufacturers and service providers will still likely argue that these solutions will stymie innovation or inhibit effective marketing and advertising, driving down their profits. As for innovation, many consumers will choose to share their data to improve the product. Under this proposal, manufacturers and service providers are free to incentivize this selection by making clear that the device will not work as intended if information is not shared.[106] In addition, service providers should not charge consumers more for withholding consent for data sharing or discounting consumers for consenting to disclosure.

Law enforcement may also resist this provision, arguing that criminal suspects will delete incriminating information. While there is a risk that this will occur, there are several counterarguments. First, many criminals simply will not be sufficiently savvy or thoughtful. Second, law enforcement does not have carte blanche to access information on consumers' electronic devices now. For example, Apple encrypts iPhone data, making law enforcement access more challenging.[107] Third, this proposal builds in an exception prohibiting the deletion of data that is subject to a warrant or preservation request pending issuance of a warrant in a criminal investigation. Fourth, law enforcement has been solving crimes for centuries without always-on device information; this proposal would not foreclose any longstanding law enforcement investigative techniques or practices. While law enforcement may be able to solve more crimes with increased access to individuals' data, American values have always militated in favor of individual privacy and against unfettered law enforcement ability to solve crimes. This is why this proposal requires a warrant before police search a home and at least reasonable suspicion before they stop an individual in the public way.[108]

C. Data Retention Limits

Always-on device manufacturers and service providers should be required to proactively delete consumers' always-on device data

---

106. Although, if, as described *infra*, the refusal to share information would impinge advertised device functionality, notice must be provided prior to purchase.

107. *E.g.*, Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We On Encryption?*, NPR (Dec. 3, 2016, 1:00 PM), http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.

108. Terry v. Ohio, 392 U.S. 1, 20 (1968).

no later than two years after the information is no longer necessary for the purpose for which it was collected.[109] Data deletion should be the default unless the consumer has requested that the information be saved or the information is the subject of a warrant or a preservation request pending the issuance of a warrant in a criminal investigation. This requirement should be enforceable by the FTC and by a private right of action.

This proposal would apply the Consumer Privacy Bill of Rights provision on Focused Collection to always-on devices. Specifically, the Consumer Privacy Bill of Rights stipulates that "[c]onsumers have a right to reasonable limits on the personal data that companies collect and retain . . . . Companies should securely dispose of . . . personal data once they no longer need it, unless they are under a legal obligation to do otherwise."[110]

This proposal should also help build consumer trust. "[R]etaining large amounts of user data . . . can lead to user mistrust and make [the always-on device service provider] a target for hackers and legal demands alike."[111] Regularly deleting data once it is no longer necessary for the purpose for which it was collected can reduce "the potential harm of data breach and other privacy hazards."[112]

Moreover, the two-year limit on data retention should provide service providers with ample time to use the collected always-on device data to improve their products and to innovate. This requirement thus balances companies' desire to innovate with individual consumers' interest in the privacy of their data.

D. The Rights of Third Parties

Always-on devices should be programmed to recognize authorized users. Always-on device manufacturers and service providers should then only be permitted to retain the personally identifiable information[113] of the individuals who have provided their consent. The personally identifiable information of third

---

109. *See* Part V.B, *infra*.

110. The White House, *supra* note 100, at 115.

111. OZER & CONLEY, *supra* note 104, at 3.

112. *Id.* at 4.

113. "Personally identifiable information" is defined here to include data captured by an always-on device that uniquely identifies an individual. This definition excludes from that definition address book, calendar, or other similar information programed into an always-on device or service by the device's owner or user.

parties who have not consented should be immediately deleted, or, at a minimum, stripped of identifying characteristics.[114] This solution provides a carve-out or white list for devices that cannot serve their intended purpose without capturing third party communications, such as devices to aid the deaf or hard of hearing or devices to monitor the elderly in order to respond quickly in emergency situations. The requirement would be enforceable by the FTC and a private right of action.

U.S. law has always been solicitous of third parties who cannot consent to the interception of private information. This is why twelve states require two-party consent before recording private conversations.[115] It is also why the FTC has repeatedly taken action against companies who have collected data without explicit consent. These include technology companies who surreptitiously installed apps on users' phones without their consent,[116] who failed to secure their software,[117] or who bundled secret audio monitoring software in their smartphone apps.[118] The FTC has also filed charges against a rent-to-own computer company who installed secret monitoring and photo-taking software on the computers it rented out[119] and has gone after the software

---

114. For always-on data, this can be accomplished with techniques like pixelation for images and voice anonymization for audio recordings. Pixelation changes the resolution of an image by changing the number of pixels used to represent an image area; by representing certain portions of an image with fewer pixels, it is possible to retain the general structure of the image while destroying information that would allow specific re-identification of individuals in the image. A voiceprint is a set of attributes, or "features," which uniquely identifies one person's voice with respect to others. Voiceprints can be constructed with mathematical transforms of raw audio waveforms. Voice anonymization can be accomplished by removing or obfuscating enough features of a voiceprint so that it can no longer be uniquely linked to an individual. *See* David Talbot, *Wiping Away Your Siri "Fingerprint,"* MIT TECH. REV. (June 28, 2012), https://www.technologyreview.com/s/428053/wiping-away-your-siri-fingerprint/.

115. *See* GRAY, *supra* note 84.

116. *Tech Company Settles FTC Charges it Unfairly Installed Apps on Android Mobile Devices Without Users' Permission*, FED. TRADE COMM'N (Feb. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/tech-company-settles-ftc-charges-it-unfairly-installed-apps.

117. *HTC America Settles FTC Charges it Failed to Secure Millions of Mobile Devices Shipped to Consumers*, FED. TRADE COMM'N (Feb. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile.

118. Grant Gross, *FTC Warns App Developers Against Using Audio Monitoring Software*, CIO (Mar. 18, 2016), http://www.cio.in/news/ftc-warns-app-developers-against-using-audio-monitoring-software.

119. *Aaron's Rent-To-Own Chain Settles FTC Charges that it Enabled Computer Spying by Franchises*, FED. TRADE COMM'N (Oct. 22, 2013),

developer who enabled employers to secretly record their employees' computer activity without warning.[120] It is also why search warrants[121] and the Foreign Intelligence Surveillance Act require "minimization" of information collected about third parties.[122]

Always-on devices collect information about third parties who visit someone with an always-on device. These third parties will not have the opportunity to consent to their information being collected and, indeed, may not even be aware that their information is being collected. Because obtaining informed consent from these individuals would be burdensome and impractical (imagine a TV sensing a new person entering the room, stopping a program, and asking for informed consent), it is imperative that their information be permanently deleted to protect their privacy rights.[123]

Notably, recognizing that always-on device manufacturers and service providers have some interest in third party information—for example, it may be useful for training devices to differentiate between foreground commands to the device and background noise—this proposal only requires the deletion of a smaller-subset of data about third parties—personally identifiable information—and allows the retention of transcripts and anonymized information.

The greatest pushback on this proposal will be from always-on device manufacturers and service providers, who will decry the expense and the technical difficulties associated with this mandate.

---

https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

120. *Spyware Seller Settles FTC Charges; Order Bars Marketing of Keylogger Software for Illegal Uses*, FED. TRADE COMM'N (June 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/spyware-seller-settles-ftc-charges-order-bars-marketing-keylogger.

121. 18 U.S.C. § 2518(5) (2010).

122. Marc Ambinder, *Minimization: A Term You Need to Know*, THE ATLANTIC (Feb. 5, 2010), https://www.theatlantic.com/politics/archive/2010/02/minimization-a-term-you-need-to-know/35403/.

123. While the Federal Communications Commission (FCC) permits the use of a "beep tone" in interstate or international telecommunications to signify that recording is taken place, *The FCC's Role*, REPORTERS COMM. FOR FREEDOM OF THE PRESS (Aug. 1, 2012), https://www.rcfp.org/reporters-recording-guide/fccs-role, there is no reason to believe this safe harbor applies to always-on technology. Moreover, it would be impractical and disruptive in a home context. Even a visual sign that recording is taking place threatens to be insufficient, as it curtails individuals' associative options. Third parties will be forced to decide whether to visit friends and family and submit to being recorded or to insist on meeting outside of the home or not at all.

However, technology with the capability to differentiate between individuals is already available, and it will only improve and become more accessible.[124]

E. Security

Any data transmitted from an always-on device to a service provider or manufacturer's servers must be transmitted and stored using the latest encryption standards. This recommendation echoes the FIPPs, which endorse the use of "[t]echnical security measures to prevent unauthorized access," including "encryption . . . and the storage of data on secure servers . . . ."[125] It also reflects the Consumer Privacy Bill of Rights: "Consumers have a right to secure and responsible handling of personal data."[126] Finally, it is good business, both because "[d]ata breaches can be disastrous, leading to lawsuits, fines, and reputational harm"[127] and because the FTC and many state laws "require companies to properly secure user data and impose fines and other enforcement actions for lax security practices."[128]

For these reasons, legislation should require that manufacturers and service providers comply with the latest industry standards, enforceable by the FTC and a private right of action. As always-on devices become more prevalent, this Article predicts that industry leaders will form consortia to collaborate on and address security concerns. The market has the power to encourage standard formation. However, in the event that the industry engages in a race-to-the-bottom, the FTC should also promulgate security standards.

---

124. *E.g.*, Md Sahidullah & Tomi Kinnunen, *Local Spectral Variability Features for Speaker Verification*, 50 DIG. SIGNAL PROCESSING 1, 11 (2016); Tess Townsend, *Google Home Can Now Recognize Different Users by Their Voice*, RECODE (Apr. 20, 2017, 12:00 PM), https://www.recode.net/2017/4/20/15364120/google-home-multiple-accounts; Jason Cipriani, *How to Teach Siri to Recognize Only Your Voice on iOS 9*, CNET (Sept. 18, 2015, 10:11 AM), https://www.cnet.com/how-to/how-to-teach-siri-to-recognize-only-your-voice-on-ios-9/. Similar technology has been deployed in production, for example by Barclays. *See* Matt Warman, *Say Goodbye to the Pin: Voice Recognition Takes Over at Barclays Wealth*, THE TELEGRAPH (May 8, 2013, 3:39 PM), http://www.telegraph.co.uk/technology/news/10044493/Say-goodbye-to-the-pin-voice-recognition-takes-over-at-Barclays-Wealth.html.

125. PRIVACY ONLINE, *supra* note 97, at 10.

126. The White House, *supra* note 100, at 113.

127. OZER & CONLEY, *supra* note 104, at 6.

128. *Id.*

While manufacturers and service providers may object that this requirement will be costly, this will be a difficult argument to make publicly because the data security encryption provides is an integral part of developing and maintaining consumer trust.

VI. CONCLUSION

The Fourth Amendment's guarantee against unreasonable searches and seizures has always been vigorously applied to bar government intrusion into homes. But increasingly, it is not just the government who seeks to invade; corporations are doing so as well. We as consumers are now bringing sensors—always-on devices—that can capture a great deal of data that was once private into our homes. Always-on devices capture information about who is at home, what they are saying, where they are, and what they are doing—data that is so valuable that companies have misled the public about collecting it[129] and law enforcement has sought to obtain it as an investigatory tool.

This Article demonstrates that current law and regulatory regimes are insufficient to protect consumer privacy with respect to always-on devices. It also offers a solution. This proposal regulates both law enforcement access to always-on device data and commercial privacy—both for the consumer and for the unwitting third party who may come into contact with an always-on device. This comprehensive framework will protect individuals' privacy and enable the law to keep pace as always-on technology flourishes.

129. *See* Part III, *infra*.

VII. ANNEXES

A. Annex 1: The Always-On Privacy Protection Act (AOPPA)

Section 1. Definitions.

For the purposes of this section:

(1) "Always-on device" means a commercial device that continuously collects audio, video, or image data or data that can be directly used to measure biometric information, including heart rate, breathing, human movement, or human location. "Always-on device" does not include a device that collects such data only when purposely triggered by the contemporaneous physical action of a consumer.

(2) "Always-on device data" means any information obtained, recorded, or transmitted by an always-on device, including, but not limited to, raw or transcribed audio, image, or video data, timestamp information, or any personally identifiable information.

(3) "Consumer" means the owner or user of an always-on device.

(4) "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(5) "Interface" means any medium that enables consumers to interact with an always-on device.

(6) "Personally identifiable information" means data captured by an always-on device that uniquely identifies an individual. "Personally identifiable information" does not include address book, calendar, or other similar information programed into an always-on device or service by the consumer.

(7) "Service provider" means a person or entity offering services related to always-on devices, including device manufacturers, or any person or other entity that uses information obtained from always-on devices for processing and fulfillment, product development, analytics, advertising and marketing, or similar business functions.

Section 2. Restrictions on Commercial Use.

(a) Except as provided in this section, a service provider who knowingly discloses, to any person, always-on device data concerning any consumer shall be liable to the aggrieved person for the relief provided in Section 8.

(b) A service provider may disclose always-on device data concerning any consumer—

(1) to the consumer when the data pertains to the consumer him or herself;

(2) as may be necessarily incident to the rendition of the service;

(3) when the data pertains to the consumer him or herself, to any person with the consumer's informed, written or oral consent (including through an electronic means using the Internet) that—

(A) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;

(B) at the election of the consumer—

(i) is given at the time the disclosure is sought; or

(ii) is given in advance for a set period of time, not to exceed 2 years, or until consent is withdrawn by the consumer, whichever is sooner;

(C) the service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election;

(D) the service provider has provided a separate clear and conspicuous opportunity to consent to each separate type of disclosure or category of always-on data recipient;

(E) where the failure to consent to a particular type of disclosure would seriously undermine the advertised function of the always-on device, the service provider has provided the consumer with clear and conspicuous notice prior to purchase of the always-on device; and

(F) if the consent is provided orally, it is recorded and made available to the consumer pursuant to Section 6;

(4) to a government entity, if the service provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(A) a government entity that receives always-on device data pursuant to this paragraph must comply with the requirements of Section 4(b)(3); and

(5) to a government entity pursuant to Section 4.

(c) A service provider may not alter the price of an always-on device or service based on whether or not the consumer consents to the disclosure of always-on device data.

Section 3. Production of or Access to Always-On Device Data.

(a) Except as provided in this section, a government entity shall not do any of the following:
  (1) Compel the production of or access to always-on device data from a service provider;
  (2) Compel the production of or access to always-on device data from any person or entity other than the consumer; or
  (3) Access always-on device data by means of physical interaction or electronic communication with the always-on device.

(b) A government entity may compel the production of or access to always-on device data from a service provider, or compel the production of or access to always-on device data from any person or entity other than the consumer only under the following circumstances:
  (1) With the specific consent of the consumer when the data pertains to the consumer him or herself;
  (2) Pursuant to a warrant issued under the procedures described in the Federal Rules of Criminal Procedure, or, in the case of a State court, issued under State warrant procedures, by a court of competent jurisdiction;

(3) If the government entity believes that an emergency involving immediate danger of death or serious physical injury to any person requires obtaining without delay always-on device data relating to the emergency and the request is narrowly tailored to address the emergency, subject to the following limitations:
   (A) the request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to a person requires obtaining without delay the information relating to the emergency; and
   (B) not later than 48 hours after the date on which a government entity thereof obtains access to records under paragraph (3), the governmental entity shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the government entity setting forth the grounds for the emergency access.

(4) A government entity specially designated by the Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of the State, may acquire always-on device data before obtaining a warrant if:
      (A) The government entity cannot, with due diligence, obtain a warrant to address an emergency situation that involves:
         (i) immediate danger of death or serious bodily injury, or
         (ii) immediate threat to the national security interest; and
      (B) When the government entity acquires always-on device data, there are grounds upon which a warrant could be entered under this chapter to authorize the acquisition.

(5) A government entity that acquires always-on device data before obtaining a warrant authorizing the acquisition must, within forty-eight hours after the acquisition occurs or begins to occur, obtain a warrant approving acquisition in accordance with paragraph (2).

(6) In the absence of a warrant, such acquisition shall immediately terminate when the data sought is obtained

or when the application for a warrant is denied, whichever is earlier.

(7) In the event such application for a warrant is denied, or in any other case where the interception is terminated without a warrant having been issued, the always-on device data acquired shall be treated as having been obtained in violation of this chapter, and notice shall be served to all consumers about whom always-on device data was acquired according to Section 5 of this chapter.

(c) No always-on device data and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or state authority, or a political subdivision thereof, if the disclosure of that information would be in violation of this chapter.

Section 4. Notice.

(a) Unless delayed notice is ordered under subsection (b), not later than three days after a government entity receives always-on device data under Section 4, the government entity shall serve upon, or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the warrant to the consumer(s)—

(1) a copy of the warrant; and

(2) notice that informs such consumer(s)—

(A) of the nature of the law enforcement inquiry with reasonable specificity;

(B) that always-on device data maintained for such consumer(s) was supplied to or requested by that government entity and the date on which the supplying or request took place;

(C) an inventory of the always-on device data supplied, including, at a minimum, the data and time of each always-on device datum supplied;

(D) if such always-on device data was obtained from a service provider or other third party,

the identity of the third party from which the information was obtained;

(E) whether notification of such consumer(s) was delayed pursuant to subsection (b);

(F) what court made the certification or determination pursuant to which that delay was made, if applicable; and

(G) if applicable, which provision of this chapter allowed such delay.

(b) Delay of Notification— A government entity acting under Section 4 may include in the application a request for an order delaying the notification required under section 5(a) for a period not to exceed 90 days, and the court shall issue the order if the court determines that there is reason to believe that notification of the existence of the warrant will result in—

(1) endangering the life or physical safety of an individual;
(2) flight from prosecution;
(3) destruction of or tampering with evidence;
(4) intimidation of potential witnesses; or
(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(c) Upon expiration of the period of delay granted under subsection (b), the government entity shall provide the consumer(s) a copy of the warrant together with notice required under, and by the means described in, subsection (a).

(d) Preclusion of Notice to Subject of Governmental Access— A government entity acting under Section 4 may include in the application a request for an order directing a service provider to which a warrant is directed not to notify any other person of the existence of the warrant for a period of not more than 90 days, and the court shall issue the order if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

(1) endangering the life or physical safety of an individual;
(2) flight from prosecution;
(3) destruction of or tampering with evidence;
(4) intimidation of potential witnesses; or
(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Section 5. Data Retention and User Control.

(a) A service provider shall establish and maintain a consumer interface that permits any consumer to view, permanently delete, or permanently save any always-on device data pertaining to that consumer.
(b) A service provider shall permanently delete a customer's always-on device data as soon as practicable, but no later than two years from the date the information is no longer necessary for the purpose for which it was collected.
(c) Notwithstanding subsections (a) and (b), the service provider must retain—
    (1) any recording of oral consent required by Section 3(b) until the consumer withdraws his or her consent or terminates his or her relationship with the service provider;
    (2) any always-on device data the consumer has requested to permanently save under subsection (a); and
    (3) any always-on device data that is the subject of a warrant issued under Section 4(b)(2) or a preservation request issued under subsection (e).
(d) A service provider shall ensure that, to the extent reasonably possible, its always-on devices distinguish between the consumer's personally identifiable information and the personally identifiable information of individuals other than the consumer and shall permanently delete any personally identifiable information collected that pertains to individuals other than the customer immediately.
    (1) This subsection shall not apply to always-on devices:
        (A) that aid the visually impaired or the hard of hearing;
        (B) that are used exclusively for protecting, securing, or monitoring a home; or
        (C) that monitor for the protection of infants, the elderly, or the disabled.
(e) A service provider, upon the request of a government entity, shall take all necessary steps to preserve always-on device data in its possession for 14 days pending the issuance of a warrant under Section 4(b)(2).
    (1) A requesting government entity must specify in a written sworn statement:
        (A) the particular always-on device(s) for which always-on device data must be preserved; and

(B) the date or dates and timeframes for which always-on device data must be preserved.

Section 6. Data Security.

(a) A service provider shall—
  (1) store, transmit, and protect from disclosure all always-on device data using the reasonable standard of care within the service provider's industry; and
  (2) store, transmit, and protect from disclosure all always-on device data in a manner that is the same as or more protective than the manner in which the service provider stores, transmits, and protects other confidential information.
(b) The Federal Trade Commission may develop appropriate security standards for always-on device data.
  (1) This subsection preempts subsection (a) only to the extent that the security standards developed are more protective of always-on device data than the industry standard of care.

Section 7. Civil Action.

(a) Any person aggrieved by any act of a service provider in violation of this chapter may bring a civil action in the United States district court for the judicial district where the aggrieved person resides.
(b) The court may award—
  (1) actual damages but not less than liquidated damages in an amount of $100,000;
  (2) punitive damages;
  (3) reasonable attorneys' fees and other litigation costs reasonably incurred; and
  (4) such other preliminary and equitable relief as the court determines to be appropriate.

Section 8. Enforcement by the Federal Trade Commission.

(a) Violation of this chapter or any regulation prescribed under this chapter shall be treated as a violation of a rule under Section 18 of the Federal Trade Commission Act (15 U.S.C. § 57a) regarding unfair or deceptive acts or

practices. The Federal Trade Commission shall enforce this chapter in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. § 41 *et seq.*) were incorporated into and made a part of this chapter.

(b) Any person who violates this chapter or any regulation prescribed under this chapter shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated in and made part of this chapter.

(c) Nothing in this section shall be construed to limit the authority of the Commission under any other provision of law.

(d) In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this chapter or any regulation prescribed under this chapter may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(1) enjoin that practice;

(2) enforce compliance with this chapter or any regulation prescribed under this chapter;

(3) obtain damage, restitute, or other compensation on behalf of residents of the State; or

(4) obtain such other relief as the court may consider to be appropriate.

Section 9. Preemption.

The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

B. Annex 2: The Model AOPPA Section-By-Section

Section 1. Definitions.

This section provides the definitions that will be used throughout the bill. Many of the definitions are newly created, based on the capabilities— current and future—of always-on devices.

The bill explicitly covers devices such as Google Home, Amazon Echo, Apple's Siri, and Smart TVs by focusing on devices that continuously record audio, video, or image data. By including data that can be directly used to measure biometric information, the bill also looks ahead to cover devices, such as gaming systems, that generate three-dimensional images of their users using infrared light or Wi-Fi radio waves.

The bill does not cover Nest or other heat- and power grid-sensing devices, because expanding far beyond the visual and aural could inadvertently regulate the entire Internet of Things, a much larger and more complex endeavor that demands a careful look at a diverse range of devices with a variety of technological capabilities.

The bill defines always-on device service providers broadly to include anyone offering services related to an always-on device, including device manufacturers and entities who use information obtained from always-on devices, including advertisers.

The bill also differentiates between always-on device data, which refers to all information obtained by an always-on device, and personally identifiable information, which refers only to information that uniquely identifies an individual. The two categories of information are treated differently throughout the bill.

Section 2. Restrictions on Commercial Use.

Section 2 regulates the commercial use of always-on devices. Based on the Video Privacy Protection Act (VPPA) and the voluntary disclosure section of the Electronic Communications Privacy Act (ECPA), the bill provides that a service provider may only disclose always-on device data in certain enumerated circumstances, including with consumer consent, as necessary to render services, and to the government, either in an emergency or upon receipt of a probable cause warrant.

This section also lays out requirements, based on the VPPA, for obtaining consumer consent, making clear that consent must be

conspicuous and separate from the "fine print" accompanying the always-on device and that the consumer must be able to revoke his or her consent at any time. Expanding beyond the VPPA, this section requires separate consent for each type of use of always-on device data. For example, a consumer could consent to the service provider's use of the data to improve the device but not to the use of always-on device data for advertising.

The section requires that the consumer be informed in advance of purchasing the always-on device if the failure to consent to a particular type of data disclosure would jeopardize the functioning of the device.

This section also makes clear that a consumer may consent only to sharing of data pertaining to his or herself. If a device is used by more than one consumer, each consumer must consent to his or her own data sharing.

Finally, this section provides that a service provider may not charge a consumer more for withholding consent for data sharing nor may a service provider offer a discount for consenting to disclosure.

Section 3. Production of or Access to Always-On Device Data.

Based on the California Electronic Communications Privacy Act (CalECPA), Section 3 requires the government to obtain a probable cause warrant before obtaining always-on device data from a service provider, from any other person or entity other than the consumer, or by means of physical interaction or electronic communication with the always-on device in a criminal investigation.

The section provides exceptions for circumstances when the consumer has consented to the disclosure of information pertaining to his or herself and exceptions for emergencies and exigent circumstances. The emergency exceptions refer to situations when no criminal wrongdoing is suspected, a warrant could not be obtained, and the information will not be used in court, but a government entity needs to quickly obtain always-on device data in order to save life or limb. In this scenario, the bill requires the government to file with the appropriate court a statement setting forth the grounds for the emergency so that a neutral arbiter can corroborate that there was, in fact, an emergency.

The exigent circumstances exception is based on Title III of the Wiretap Act and allows the Attorney General or principal

prosecuting attorney in any state to authorize the acquisition of always-on device data in a law enforcement emergency where there is immediate danger of death or serious bodily injury or a threat to national security and there are grounds upon which a warrant could issue. In this scenario, the bill requires the government to obtain a warrant within 48 hours after always-on device data acquisition begins. This section is enforceable by a suppression remedy.

Section 4. Notice.

This section requires actual notice to the always-on device consumer when the government has obtained his or her always-on device data. In the context of e-mail and other records held by third parties, the government has in the past contended that it satisfied the notice requirement attendant to Rule 41 by notifying the service provider. This section ensures that the government notifies the individual whose data has been collected.

Mirroring language in ECPA, this section also provides for delayed notification if immediate notice would endanger the life or safety of an individual, seriously jeopardize an investigation or unduly delay a trial, or engender flight from prosecution, destruction of or tampering with evidence, or intimidation of potential witnesses. This section deliberately adopts longstanding language from existing law that courts and law enforcement agencies are accustomed to interpreting.

Section 5. Data Retention and User Control.

This section requires service providers to maintain a consumer dashboard or other interface that permits consumers to view and permanently delete always-on device data pertaining to themselves. Based on the VPPA, this section also requires service providers to proactively delete consumers' always-on device data no later than two years after the information is no longer necessary for the purpose for which it was collected unless the consumer has requested that the data be saved. The two-year limit on data retention should provide service providers with ample time to use the collected always-on device data to improve their products and innovate.

The section also allows the government to issue a preservation request, requiring that information be preserved pending the issuance of a warrant, and requires the retention of data subject to

a warrant or preservation request, notwithstanding a consumer's request for deletion. The concept of a preservation request is based on state laws governing automatic license plate readers in Utah and Vermont.

This section also endeavors to protect the privacy of third parties, who cannot practically consent to the recording, transmission, and retention of their personally identifiable information. In many cases, they may not even be aware that they have come in contact with an always-on device. Therefore, this section requires service providers, to the extent possible, to program their always-on devices to distinguish between the personally identifiable information of the consumer and the personally identifiable information of individuals other than the consumer. The legislation then requires service providers to permanently delete personally identifiable information pertaining to individuals other than the consumer. The deletion requirement specifically applies to a smaller subset of information—personally identifiable information—out of recognition that service providers may have a legitimate interest in maintaining some always-on device data to aid in product improvement. This compromise aims to balance third parties' privacy interests—by deleting the most sensitive information collected—with service providers' interests in innovation. This section provides exceptions for devices, such as those meant to aid the visually impaired or the hard of hearing or those that monitor infants, the elderly, or the disabled, that require the retention of personally identifiable information of third parties in order to perform their intended function.

Section 6. Data Security.

This section provides for data security. The proposed bill is based on Illinois's Biometric Information Privacy Act and similarly requires service providers to adhere to industry standards for the secure storage, transmission, and protection of always-on device data.

However, borrowing an idea from Washington's state law on facial recognition matching systems for driver's licenses, the bill also allows an executive agency to promulgate security standards for always-on device data storage, transmission, and protection. The bill, which allows the Federal Trade Commission (FTC) to set such standards, provides that these standards will only preempt industry practices if they are more protective than industry standards. This dual layer helps protect against a "race to the

bottom" in industry standard settings, but also provides for a standard should the FTC fail to act or should the FTC promulgate insufficiently protective standards.

Section 7. Civil Action.

This section provides for a private right of action against a service provider that improperly discloses or stores always-on device data or personally identifiable information in violation of the statute.

Section 8. Enforcement by the Federal Trade Commission.

This section provides that the bill is enforceable by the FTC as a violation of the Federal Trade Commission Act's prohibition on unfair or deceptive acts or practices. It also allows for enforcement by state attorneys general.

Section 9. Preemption.

This section provides that this bill preempts only the provisions of state or local law that require disclosure that is otherwise prohibited by the bill.