Oklahoma Law Review

Volume 74 | Number 2

2022

Accidental Wiretaps: The Implications of False Positives by Always-Listening Devices for Privacy Law & Policy

Lindsey Barrett

Ilaria Liccardi

ACCIDENTAL WIRETAPS: THE IMPLICATIONS OF FALSE POSITIVES BY ALWAYS-LISTENING DEVICES FOR PRIVACY LAW & POLICY

LINDSEY BARRETT & ILARIA LICCARDI*

Abstract

Always-listening devices like smart speakers, smartphones, and other voice-activated technologies create enough privacy problems when working correctly. But these devices can also misinterpret what they hear, and thus accidentally record their surroundings without the consent of those they record, a phenomenon known as a "false positive." The privacy practices and preferences of device users add additional complications. A recent study of individual privacy expectations and usage of voice assistants depicts how people tend to carefully consider the privacy preferences of those closest to them when deciding whether to subject them to the risk of accidental recordings, but often disregard the preferences of others. The failure of device owners to get consent from those around them is exacerbated by the accidental recordings, as it means that the companies collecting the recordings aren't obtaining the consent to record their subjects that the Federal Wiretap Act, state wiretapping laws, and consumer protection laws require. Failure to obtain consent also contravenes the stringent privacy assurances that these companies generally provide. The laws governing surreptitious recordings also frequently rely on individual and societal expectations of privacy, which are warped by the justifiable resignation to privacy invasions that most people eventually acquire.

The result is a legal regime ill-adapted to always-listening devices, with companies frequently violating wiretapping and consumer protection laws, regulators failing to enforce them, and widespread privacy violations. Ubiquitous, accidental wiretaps in our homes, workplaces, and schools are just one more example of why consent-centric approaches cannot sufficiently protect our privacy, and policymakers must learn from those failures rather than doubling down on a failed model of privacy governance.

---

* Lindsey Barrett is a Telecommunications Policy Analyst with the National Telecommunications and Information Administration. Her views expressed here do not reflect the views or positions of the NTIA. Ilaria Liccardi is a Research Scientist at the Computer Science and Artificial Intelligence Laboratory at the Massachusetts Institute of Technology. The authors are deeply grateful to Anne McKenna, participants of the Privacy Law Scholars' Conference 2020, Megan Graham, and Paul Ohm.

Table of Contents

I. Introduction

People generally care about their own privacy. They tend to care less about the privacy of other people, and the rise of always-on, voice-activated devices has thrown that distinction, and the social problems it creates, into sharp relief. As always-on devices have become cheaper and more popular, they've faded into the fabric of daily life: people often fail to realize that their utterances are being recorded by a smartphone, a smart speaker, or a smart television that might be hidden from sight or right under their noses. While always-on smart assistants are designed to record only after they detect a specific "wake word," they also engage in "passive listening," meaning they analyze their surroundings in anticipation of a command to begin recording, and (purportedly) delete what they recorded until the command was received. But these devices can incorrectly perceive the utterance of a wake word, which means they record their surroundings without the awareness or consent of the people they've recorded. That includes third parties, given that most people don't tend to begin every social interaction they have within earshot of their phone or television by getting the consent of everyone in the vicinity to record anything they might say. Companies may also use the recordings that occur after keyword detection to "improve their products," and whether those improvements include making privacy-invasive inferences about the data subjects for advertising purposes or trying to ascertain details about the company's competitors is anyone's guess. Vocally activated, always-on smart assistants have transformed our devices into innocuous-seeming wiretaps,

and the owners of those devices, unsuspecting third parties, and existing privacy laws are ill-equipped to grapple with the ramifications.

To learn more about how people respond to the privacy implications of always-on devices for themselves and others, one of us conducted a study on the preferences and expectations of the users of always-on devices.[1] Participants were asked to download a bespoke, always-on assistant to their smartphone and answered questions about their privacy preferences and behavior before and after doing so. The study found that while participants were often sensitive to the privacy preferences and expectations of people close to them, like romantic partners, they often disregarded the potential for violations of the privacy of other people they might be recording, such as co-workers, acquaintances, or health professionals. Participants declined to inform people with whom they had less intimate relationships that they were being recorded, even when they reported believing that the acquaintances would object to the recording.

The potent combination of surreptitious recordings by always-on devices and the prevalent disregard for colleagues' and acquaintances' privacy that this study reflects has broad implications for privacy law and policy. Companies' interception, use, and disclosure of recordings without third-party consent likely violates wiretap laws in states with two- or all-party consent standards.[2] These recordings may also violate the Federal Wiretap Act[3] and laws in states with one-party consent standards, as boilerplate consent to a privacy policy will likely not suffice for recordings of users that they were unaware of, or the recordings of third parties. Surreptitious recordings by always-on devices may also violate consumer protection laws designed to prohibit businesses from lying to their customers or collecting personal information from children. Recording children under thirteen without obtaining their parents' verifiable consent violates the Children's Online Privacy Protection Act (COPPA),[4] and the acquisition and use of these surreptitious recordings despite public claims that the devices only record when commanded to do so likely violates prohibitions on unfair and

1. Ilaria Liccardi & Jose Juan Dominguez Veiga, Wiretapping Your Friends: Privacy Implications of Voice Activated Assistants (Aug. 2019) (unpublished technical report) (on file with authors). As of January 2022, this study is under review for future publication.

2. *See infra* Part V.

3. 18 U.S.C. §§ 2510–2523.

4. *See* 15 U.S.C. § 6502(b)(1) (requiring parental consent to record children).

deceptive acts and practices in both state and federal law.[5] Enforcement of these laws by the Federal Trade Commission (FTC), state attorneys general, and in the case of wiretap laws, private plaintiffs, could mean damaging liability claims for companies selling these devices, and in the case of the Wiretap Act and state wiretapping statutes, possible criminal liability.

The disparity among how existing privacy laws conceptualize human behavior, how always-on devices actually function, and how people actually act has clear implications for existing privacy laws and the companies violating them. That disparity also has significant implications for future privacy laws. The unwillingness or inability of device users to obtain consent from the people they're recording serves as an umpteenth example of why consent is a failed method of privacy governance when relied on as the primary bulwark against privacy violations.[6] And the "Wiretapping Your Friends" study's illustration of some participants' resignation to privacy invasions underscores the significant limitations of relying on privacy expectations as a factor in determining privacy protections. Finally, the uneven array of state wiretap standards demonstrates the value of a strong federal privacy law that takes all of these considerations into account, and until and unless such a law is politically feasible, strong state legislation that pushes the threshold that companies will gravitate around even without a federal mandate.

Ubiquitous, surreptitious recording devices present an unusually stark problem for privacy law, but the problems they raise are far from unique. Privacy is a collective value,[7] and reliance on individual decision-making to protect either individuals or communities is a doomed proposition that will never provide meaningful privacy safeguards. A legal regime that assumes a person's capacity and willingness to obtain meaningful consent from everyone they might accidentally record ignores reality in favor of tidy abstractions, a preference that—given the laxity of most privacy laws and their underenforcement—redounds to the benefit of extractive companies. The United States needs privacy laws that repudiate a discredited model of

---

5. *See generally* 15 U.S.C. § 57a(a)(1)(B) (granting the Federal Trade Commission authority to define an unfair or deceptive act or practice).

6. *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1894–95 (2013) (discussing the inadequacy of consent in data collection); *see infra* Section III.C.

7. *See generally* Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555 (2020) (discussing the interdependency of privacy based on other people's decisions and disclosures).

human behavior that currently leaves people vulnerable to privacy violations, not laws that use that model as a foundation. The prevalence of wiretapping consumer devices and how people respond to them despite what existing law expects is simply one more example of the disparity between what consent-centric privacy laws envision, and how people actually live their lives.

Part II of this Article provides an overview of always-listening devices and the privacy implications of both their function and malfunction through false positives. Part III outlines the relevant legal standards that the collection and use of false positives appears to violate—the Federal Wiretap Act, state wiretap statutes, state and federal unfair and deceptive trade practice statutes, and COPPA—then critiques their outsized reliance on consent and privacy expectations. Part IV describes the study of device users' privacy considerations regarding false positives and passive listening by voice-activated assistants. Part V explains how device companies likely violate wiretapping and consumer protection laws through their collection and use of recordings prompted by false positives. Part VI considers how regulators and legislators should respond to the disparity between existing law's vision of privacy practices and how people and companies actually use these devices, and Part VII concludes.

II. Always-On Devices, Privacy, and False Positives

Voice-activated technologies have become tremendously popular in the past five years or so, from smart assistants incorporated into smartphone or computer operating systems, to stand-alone smart speakers and voice-activated capabilities incorporated into various sensor-enabled devices, such as smart watches,[8] connected televisions,[9] gaming consoles,[10] voice-assistant-enabled locks,[11] voice-activated toys,[12] and smart thermostats.[13] A

8. Matthew Woodall, *My New Apple Watch Is a Privacy Nightmare*, MEDIUM: THE STARTUP (Dec. 4, 2019), https://medium.com/swlh/my-new-apple-watch-is-a-privacy-nightmare-fcf6c84662c5.

9. James K. Willcox, *How to Turn Off Smart TV Snooping Features*, CONSUMER REPS. (Feb. 17, 2021), https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/.

10. Joseph Cox, *Microsoft Contractors Listened to Xbox Owners in Their Homes,* VICE (Aug. 21, 2019, 1:00 PM), https://www.vice.com/en/article/43kv4q/microsoft-human-contractors-listened-to-xbox-owners-homes-kinect-cortana.

11. Search for "Yale Assure SL," YALE, https://shopyalehome.com/products/yale-assure-lock-sl?variant=28400472588388 (last visited Jan. 25, 2021).

Pew Research Center study found that one quarter of American adults describe having a smart speaker in their home,[14] while a more recent study by National Public Radio and Edison Research reported increased usage of voice assistants on smart speakers and other devices during the COVID-19 pandemic, with more than half of device users keeping the assistant enabled at all times.[15] Mobile device users increasingly rely on voice assistants for search functions,[16] and sinking hardware costs, increased consumer comfort, and other structural factors make it likely that that growth will continue. The ease of using a vocal command rather than a visual interface can be compelling, and it can be transformative for the elderly[17] and for people with disabilities who struggle to use other modalities due to vision, motor, or other difficulties.[18]

At the same time, always-on systems create meaningful privacy concerns. An always-listening robot that records your every interaction with it continues to strike many people as creepy and invasive.[19] These privacy concerns are entirely justified, given the intimacy of the data that can be

12. Moustafa Mahmoud et al., *Towards a Comprehensive Analytical Framework for Smart Toy Privacy Practices*, *in* STAST, PROCEEDINGS: 7TH WORKSHOP ON SOCIO-TECHNICAL ASPECTS IN SECURITY AND TRUST 64 (2018), https://dl.acm.org/doi/10.1145/3167996.3168002 (registration required).

13. *Control Google Nest or Home Devices by Voice*, GOOGLE NEST HELP, https://support.google.com/googlenest/answer/7207759?hl=en#:~:text=You%20can%20use%20your%20voice,Filters%20or%20Do%20not%20disturb (last visited Jan. 25, 2021).

14. Brooke Auxier, *5 Things to Know About Americans and Their Smart Speakers*, PEW RSCH. CTR. (Nov. 21, 2019), https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/.

15. *The Smart Audio Report*, NPR & EDISON RSCH. (Apr. 2020), https://www.nationalpublicmedia.com/uploads/2020/04/The-Smart-Audio-Report_Spring-2020.pdf.

16. Deyan Georgiev, *2020's Voice Search Statistics – Is Voice Search Growing?*, REV. 42 (July 22, 2021), https://review42.com/voice-search-stats/.

17. Kathryn M. Daniel et al., *Emerging Technologies to Enhance the Safety of Older People in Their Homes*, 30 GERIATRIC NURSING 384, 387 (2009) (describing assistive technologies available to help the elderly conserve energy).

18. Yusuf Uzunay & Kemal Bicakci, *SHA: A Secure Voice Activated Smart Home for Quadriplegia Patients*, *in* IEEE COMPUT. SOC'Y, PROCEEDINGS: 2007 IEEE INTERNATIONAL CONFERENCE ON BIOINFORMATICS AND BIOMEDICINE 151 (2007), https://ieeexplore.ieee.org/document/4425413 (registration required); Fabio Masina et al., *Investigating the Accessibility of Voice Assistants with Impaired Users: Mixed Methods Study*, 22 J. MED. INTERNET RSCH. e18431 (2020).

19. *The Smart Audio Report*, *supra* note 15, at 20–23; Auxier, *supra* note 14.

captured and the circumstances in which it might be captured.[20] Smart speakers implicate similar privacy concerns as a search engine operator with visibility into a person's search history, or an internet service provider that can monitor a person's web browsing, turbocharged by the intimacy and comfort that an easily accessible, anthropomorphized voice assistant is intended to create.[21] Beyond the sensitivity of a person's search queries and range of personal details a voice assistant can have access to,[22] voice data as a category can also be tremendously revealing about a person. Researchers have reportedly devised methods of inferring ethnicity, gender, personality, and physical strength from voice data.[23] Even when these methods are unreliable, a belief in the ability to accurately infer sensitive characteristics about people from vocal attributes will lead companies to characterize them accordingly. People also tend to consider audio recordings to be a sensitive category of information,[24] meaning that abuse of that information could feel particularly violative.

Always-listening devices can enable the abuse of harmful power dynamics. Amazon's Echo offers a "Drop In" feature,[25] which allows one Echo user to connect to another device so long as the other user provided consent in advance. But there's no guarantee that consent would be meaningful or obtained without coercion, and the Drop In feature could allow an abusive partner, parent, or similar figure to subject their target to the perpetual concern of aural surveillance. Amazon offers an Alexa service

---

20. *See, e.g.*, Alex Hern, *Apple Contractors 'Regularly Hear Confidential Details' on Siri Recordings*, GUARDIAN (July 26, 2019, 12:34 EDT), https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings (reporting incidents in which Siri recorded personal medical details, couples having sex, and seemingly criminal business deals).

21. Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 790 (2015) (citing the consumer protection challenge of regulating a robot that feels like a "social actor" to human beings).

22. Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1239, 1279–86 (2017).

23. Liccardi & Dominguez Veiga, *supra* note 1.

24. Nathan Malkin et al., *Privacy Attitudes of Smart Speaker Users*, PROC. ON PRIV. ENHANCING TECHS., Oct. 2019, at 250, 250, https://sciendo.com/article/10.2478/popets-2019-0068.

25. *Alexa Communications*, AMAZON, https://www.amazon.com/b?node=16713667011 (last visited Feb. 4, 2021).

for landlords[26] and hospitals,[27] both areas in which occupants may face limited choice in their ability to physically vacate the space or avoid being recorded by a device without doing so. Some teachers[28] and librarians[29] are using Alexa devices in schools, which presents similar concerns, as well as possible chilling effects for intellectual privacy.[30] Smartphones with voice-activated assistants, such as Apple's Siri or Samsung's Bixby, are even more difficult, if not functionally impossible, to avoid than smart speakers are, given the acceptance of ubiquitous smartphones in a wide range of social and professional contexts, and their relatively small and easily concealed design.[31] Voice-activated versions of typical objects like lightbulbs and plugs may also inculcate a mistaken sense of safety and prevent people from effectively assessing the risks they pose.[32] Moreover, whatever your Google Home might record is accessible to law enforcement via a warrant or subpoena, providing yet another avenue through which data-collecting technologies can enable governmental surveillance.[33]

---

26. Edward Ongweso Jr., *Amazon Wants Alexa to Move into Your Apartment Before You Do*, VICE (Sept. 4, 2020, 9:00 AM), https://www.vice.com/en/article/qj45kx/amazon-wants-alexa-to-move-into-your-apartment-before-you-do.

27. Melanie Ehrenkranz, *'Alexa, Find Me a Doctor.' 'Okay, Finding You a Daughter.'*, GIZMODO (Apr. 4, 2019, 1:20 PM), https://gizmodo.com/alexa-find-me-a-doctor-okay-finding-you-a-daughter-1833806971.

28. Benjamin Herold, *Teacher's Aide or Surveillance Nightmare? Alexa Hits the Classroom*, EDUC. WEEK (June 26, 2018), https://www.edweek.org/technology/teachers-aide-or-surveillance-nightmare-alexa-hits-the-classroom/2018/06; *Alexa in Education*, AMAZON, https://aws.amazon.com/education/alexa-edu/ (last visited Jan. 25, 2021).

29. Miriam E. Sweeney & Emma Davis, *Alexa, Are You Listening: An Exploration of Smart Voice Assistant Use and Privacy in Libraries*, INFO. TECH. & LIBRS., Dec. 2020, at 1 (vol. 39, no. 4), https://ejournals.bc.edu/index.php/ital/article/view/12363/10229.

30. *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 419 (2008).

31. *See generally* Matt Novak, *The FBI Can Neither Confirm nor Deny Wiretapping Your Amazon Echo*, GIZMODO (May 11, 2016, 5:00 PM), https://paleofuture.gizmodo.com/the-fbi-can-neither-confirm-nor-deny-wiretapping-your-a-1776092971 (voicing concerns that "people would willingly put microphones in their own homes" through their use of smartphones and unobtrusive "always-listening" devices).

32. Malkin et al., *supra* note 24, at 251.

33. *See* Sidney Fussell, *Meet the Star Witness: Your Smart Speaker*, WIRED (Aug. 23, 2020, 7:00 AM), https://www.wired.com/story/star-witness-your-smart-speaker/; *see also Amazon Drops Privacy Rights Fight in Arkansas Murder Case, Hands Over Amazon 'Echo' Data*, ASSOCIATED PRESS (Mar. 6, 2017, 7:17 PM), https://cbs4indy.com/news/national-world/amazon-drops-privacy-rights-fight-in-arkansas-murder-case-hands-over-amazon-echo-data/ (discussing the admission of Amazon Echo recordings in a murder trial).

In the case of smart speakers and other voice-activated devices, integrating an internet-connected device into private spaces—or public spaces that people face limited choice in frequenting, such as a hospital or a school—also introduces cybersecurity vulnerabilities that can put people in danger of privacy violations and other harms. Researchers have demonstrated how smart speakers can be manipulated into tricking their owners into divulging personal information, including their passwords, making them vulnerable to financial loss, dignitary or physical harms, and the anxiety of having their most intimate personal details revealed.[34]

To understand the privacy and associated legal problems with always-listening devices, it's helpful to understand the precise mechanics of how they work. Amazon's Alexa perpetually records its surroundings and analyzes those recordings for its programmed wake word ("Alexa," "Computer," or something else).[35] When it detects the wake word, it sends that recording to the Amazon cloud, at which point the cloud saves the recording, interprets what was recorded, and directs the Alexa device to execute the command it detected, such as reporting the day's weather, operating an Alexa "skill," or providing another service.[36] The recordings on the Alexa device are encrypted when they're sent to Amazon.[37] It's unclear how much computation actually occurs on Google's voice-activated devices, as opposed to Google's cloud: Google devices continually record snippets of audio and send them to the cloud, but investigative reporting and individual users examining the logs of what their devices recorded have revealed that the devices appear to send much longer recordings to Google than the company claims.[38] Apple claims that its HomePod and other voice-activated devices only send audio to the cloud once the local device has detected the wake word, and the audio is encrypted and not associated with

34. Victoria Song, *Your Google Home and Alexa Can Be Used to Eavesdrop and Phish for Your Passwords*, GIZMODO (Oct. 21, 2019, 12:10 PM), https://gizmodo.com/your-google-home-and-alexa-can-be-used-to-eavesdrop-and-1839223529.

35. *Common Questions About Alexa Privacy*, AMAZON, https://perma.cc/9Q85-VSZM (last visited Feb. 1, 2021).

36. *Id.*

37. *Alexa and Echo Devices Are Designed to Protect Your Privacy*, AMAZON, https://perma.cc/T8UM-DS7B (last visited Feb. 1, 2021).

38. Third Amended Consolidated Class Action Complaint at 29, *In re* Google Assistant Privacy Litigation, No. 5:19-cv-04286-BLF (N.D. Cal. filed July 25, 2019).

the user's identity, but the company's policy on the snippets of audio recorded before (and in anticipation of) the wake word is unclear.[39]

Many of these companies have more privacy-protective policies when it comes to voice-activated devices than they used to. In 2019, reporting by a number of news outlets revealed that companies like Microsoft, Apple, Amazon, and Google were also using human contractors to transcribe, correct, and annotate recordings from their voice-activated devices, without disclosing that fact to device owners. The Guardian reported that Apple contractors "regularly hear[d] confidential medical information, drug deals, and recordings of couples having sex" as well as "business deals [and] seemingly criminal dealings," accompanied by location data, contact information, and information about app usage, despite Apple's claims that the recordings were anonymized[40] and its claims that recordings aren't sent to the company at all. Google also employs human contractors to review voice recordings, and a Belgian news outlet was able to identify people from their recordings and locations thanks to a dataset provided by a whistleblower.[41] While the company also claimed that the recordings were anonymized before being provided to contractors, the Belgian outlet was able to identify people from them, including one recording that contained a person's address, and others that captured people discussing their children and romantic lives.[42] Amazon also used, and continues to use, human workers to transcribe recordings, and two employees told Bloomberg that they heard what they believed to be a sexual assault on one recording;[43] on

39. *HomePod Overview*, APPLE, https://www.apple.com/homepod-2018/ (last visited Feb. 1, 2021) ("After HomePod recognizes the words 'Hey Siri,' what you say is encrypted and sent anonymously to Apple servers without being tied to your Apple ID.") (screenshot on file with authors). Apple does not appear to directly address what happens to those audio recordings in its privacy policies and statements about Siri-enabled devices. *Ask Siri, Dictation & Privacy*, APPLE (Dec. 13, 2020), https://perma.cc/837Q-3MAV; *Apple Privacy Policy*, APPLE (Dec. 14, 2020), https://perma.cc/H7GR-73Q4.

40. Hern, *supra* note 20.

41. Kari Paul, *Google Workers Can Listen to What People Say to Its AI Home Devices*, GUARDIAN (July 11, 2019, 4:41 PM), https://www.theguardian.com/technology/2019/jul/11/google-home-assistant-listen-recordings-users-privacy; *see also* Blake Montgomery, *Apple and Google Workers Stop Listening to What You Ask Your Voice Assistant, For Now*, DAILY BEAST (Aug. 2, 2019, 5:43 PM), https://www.thedailybeast.com/apple-and-google-pause-human-voice-recording-review-over-privacy-concerns.

42. Paul, *supra* note 41.

43. Alex Hern, *Amazon Staff Listen to Customers' Alexa Recordings, Report Says*, GUARDIAN (Apr. 11, 2019, 7:28 AM), https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says.

other occasions, employees shared recordings they found to be amusing in an employee chatroom.[44]

Apple and Google paused their use of human reviewers for recordings shortly after the 2019 revelations. But the companies resumed a few months later, adding additional disclosures in their privacy policies.[45] Google also subsequently introduced a "Guest Mode" setting for its smart speaker, which tells the device to delete audio recordings and descriptions of how the subject interacts with the device instead of saving them.[46] When someone using Guest Mode uses services other than Google Assistant (such as another Google product or a service owned by another company), the information associated with that interaction is not necessarily treated any differently than if the device were operating normally.[47] Apple also now deletes recordings by default unless the user opts in,[48] and so does Microsoft,[49] while Amazon appears to still keep recordings and associated data until the user deletes them.[50]

---

44. Nicole Nguyen, *A Team at Amazon Is Listening to Recordings Captured by Alexa*, BUZZFEED NEWS (Apr. 10, 2019, 8:15 PM), https://www.buzzfeednews.com/article/nicolenguyen/amazon-employees-listening-to-alexa-echo-recordings.

45. Mae Anderson, *Apple Resumes Human Reviews of Siri Audio with iPhone Update*, ASSOCIATED PRESS (Oct. 29, 2019), https://apnews.com/article/078755dbec364b71a7b34abf63fb6284.

46. *Control Your Privacy on Your Shared Devices with Guest Mode*, GOOGLE ASSISTANT HELP, https://support.google.com/assistant/answer/10217706?p=guestmode&visit_id=637468437516938656-4231995297&rd=1 (last visited Jan. 23, 2021).

47. Sara Morrison, *Google Assistant's New Guest Mode Is More Private, but There's a Trade-off*, VOX (Jan. 13, 2021, 1:30 PM), https://www.vox.com/recode/22229008/google-assistant-guest-mode.

48. Chaim Gartenberg, *Apple Apologizes for Siri Audio Recordings, Announces Privacy Changes Going Forward*, VERGE (Aug. 28, 2019, 11:07 AM), https://www.theverge.com/2019/8/28/20836760/apple-apology-siri-audio-recordings-privacy-changes-contractors.

49. Daphne Leprince-Ringuet, *Still Talking to Cortana? Microsoft Gives You More Control over How Your Voice Recordings Are Used*, ZDNET (Jan. 18, 2021, 3:35 PM), https://www.zdnet.com/article/still-talking-to-cortana-microsoft-gives-you-more-control-over-how-your-voice-recordings-are-used/.

50. Amazon has not announced changes to this policy since the company's response to Senator Coons, and more recent documentation of its policies, such as a white paper explaining the company's Alexa data collection and retention policies published in December 2019, do not contradict it. *Alexa Confidentiality and Data Handling Overview*, AMAZON (Dec. 20, 2019), https://d1.awsstatic.com/whitepapers/White%20Paper-Alexa%20Confidentiality%20and%20Data%20Handling%20Overview%20Dec%202019.pdf; *see also* Makena Kelly & Nick Statt, *Amazon Confirms It Holds On to Alexa Data Even if*

These changes are generally an improvement, even if belated and compelled by undesired scrutiny and public pressure. Automatic deletion is valuable, given the heavy impact of default settings on user behavior.[51] But for companies that don't delete recordings automatically, most have given few clear assurances about how the recordings will be used,[52] and the exhaustively documented struggles that people encounter in attempting to protect their privacy through data collection controls will heavily limit the privacy-protective effects of those changes.[53]

Always-listening devices present plenty of privacy risks when working correctly, but their potential for error creates an additional and worrisome vector of potential privacy harms. The sounds that constitute "OK Google" or "Alexa" can be sufficiently similar to other words, allowing always-on devices to mistakenly start recording without the knowledge of the people being recorded. For example, an Oregon family's Alexa recorded their conversation and accidentally sent it to someone in their contact list, an employee of one of the family members.[54] One study documents how popular Netflix shows set off various smart speakers,[55] while other

---

You Delete Audio Files, VERGE (Jul. 3, 2019, 4:14 PM), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy.

51. *See* Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509, 512 (2015) (describing the impact of default settings on privacy choices).

52. *See, e.g.*, *FAQs on Privacy: Google Nest*, GOOGLE, https://support.google.com/googlenest/answer/9415830 (last visited Feb. 4, 2021) ("Your device interactions via the Google Assistant or other Google services (such as YouTube) may be used to personalize your Google experiences, including to show you relevant ads. For example, the text of your voice interactions with the Google Assistant can inform your interests for ad personalization."). Discarding the recording itself doesn't address the privacy implications of extracting the substance of what was said on the recording, in addition to the revelatory possibilities of metadata and Google's characterizations of the recording (such as inferred intent).

53. *See infra* Section III.C.

54. Hamza Shaban, *An Amazon Echo Recorded a Family's Conversation, Then Sent It to a Random Person in Their Contacts, Report Says*, WASH. POST (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/.

55. Daniel J. Dubois et al., *When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers*, PROC. ON PRIV. ENHANCING TECHS., Oct. 2020, at 255, 255, https://sciendo.com/article/10.2478/popets-2020-0072 ("After playing two rounds of 134 hours of content from 12 TV shows near popular smart speakers in both the US and in the UK, we observed cases of 0.95 misactivations per hour, or 1.43 times for every 10,000

researchers have documented Amazon's Alexa alerting to "unacceptable" and "election," Google Home alerting to "Ok, cool," Siri to "a city," and Cortana to "Montana," among other confusions.[56] What's more, these devices may not always be limited to recording solely in response to verbal commands, creating an even wider universe for potential mistakes and privacy violations. Google recently admitted to accidentally turning on an unannounced new feature for certain Google Home users that involved re-programming the device to alert to certain non-verbal cues, such as a smoke alarm or broken glass.[57] "Alexa Guard" —Amazon's home security feature for always-on devices—already listens for smoke alarms, carbon monoxide alarms, and the sound of breaking glass,[58] and Amazon has filed a patent for an always-recording voice assistant software that doesn't rely on a wake word at all.[59] Alexa's "Follow-Up" mode, which currently allows the device to complete user requests without repeating the wake word, seems to anticipate that potential shift.[60] False positives resulting from misperceived verbal commands are just the beginning.

False positives by always-listening software have clear privacy implications for the people who knowingly use it through a smartphone, smart speaker, or another connected device. The decision to purchase a smart phone or speaker cannot be equated with the knowing acceptance of the potential to be recorded at any moment, with that recording being

---

words spoken, with some devices having 10% of their misactivation durations lasting at least 10 seconds.").

56. Lea Schönherr et al., *Exploring Accidental Triggers of Smart Speakers*, UNACCEPTABLE, https://unacceptable-privacy.github.io/ (last visited Feb. 1, 2021).

57. Janko Roettgers, *Google's Secret Home Security Superpower: Your Smart Speaker with Its Always-On Mics*, PROTOCOL (Aug. 3, 2020), https://www.protocol.com/google-smart-speaker-alarm-adt.

58. *Using Alexa Guard with Alarm to Detect Broken Glass, Smoke, and Carbon Monoxide*, RING, https://support.ring.com/hc/en-us/articles/360028205592-Using-Alexa-Guard-with-Alarm-to-Detect-Broken-Glass-Smoke-and-Carbon-Monoxide (last visited Feb. 1, 2021).

59. Jennings Brown, *Amazon Patent Reveals Its Vision for an Alexa Device That Records Every Word You Speak*, GIZMODO (May 24, 2019, 10:50 AM), https://gizmodo.com/amazon-patent-reveals-its-vision-for-an-alexa-device-th-1835004420 ("But under the technology laid out in the patent, when Alexa detects a wakeword, it will then 'look backward' to find if a command was made before, and use speech pauses to find the start of the command. It would be able to do this because it would be recording constantly, and supposedly deleting what it doesn't need.").

60. *Turn on Follow-Up Mode*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202201630 (last visited Aug. 8, 2021).

analyzed by human beings and used to target the speaker for products and services. But this problem is even more concerning when it comes to accidentally recorded bystanders, who generally have even less reason to suspect that they've been secretly recorded, as they might not have a reason to be aware of the recording device and are dependent on the device's owner to monitor the device for potential erroneous recordings. Expecting device owners to protect themselves from encroachments on their privacy is unreasonable enough. But it's even more unreasonable to expect people to protect themselves from always-on devices they aren't aware of. Nor can we place the privacy protections of bystanders solely at the feet of device-owners, as though requiring guests to sign a release before they enter your home or warning everyone you speak to of the potential for recording would be feasible or effective. Applicable privacy laws are poorly suited to that reality, as the next section discusses, and the privacy practices of device owners will continue to leave most of the other people recorded by these devices vulnerable, as Part IV describes in conjunction with "Wiretapping Your Friends."

III. The Legal Landscape

The United States has plenty of federal privacy laws—they simply haven't been very effective at preventing or deterring privacy violations. Always-on devices shine a particularly harsh light on problems with these laws that privacy advocates and scholars have criticized for decades: namely the misguided conception of consent as the primary guardrail for privacy rights, and the failure to recognize how hinging privacy protections on privacy expectations can dilute those protections thanks to resignation inculcated by frequent and unavoidable privacy invasions.[61] The following section discusses the existing wiretapping laws and consumer privacy laws that are most relevant to always-on devices.

A. State and Federal Wiretapping Laws

Federal and state wiretap laws were designed to strictly limit exactly the kinds of privacy invasions that always-on devices enable: surreptitious

61. Solove, *supra* note 6, 1880–81; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1464 (2019) (arguing that while consent should not be wholly rejected as a privacy safeguard, "we have relied upon it too much, and deployed it in ways and in contexts to do more harm than good, and in ways that have masked the effects of largely unchecked (and sometimes unconscionable) power").

recordings of conversations. The Federal Wiretap Act and wiretap laws in every state but Vermont[62] govern the intentional interception, disclosure, and use of the contents of wire, oral, and electronic communications, though some states use wording that differs slightly from the Wiretap Act's phrasing, such as "private" or "confidential" communications.[63] State legislatures recognized the threat to privacy that wiretapping presented as early as the 1860s, with states like California, New York, and Illinois passing prohibitions on telegraph and telephone wiretapping, and with a steady stream of other states following in their wake over the next seventy-odd years.[64] By 1967, thirty-six states had banned wiretapping outright, with twenty-seven allowing a judicially authorized law-enforcement exception.[65] Congress passed the Wiretap Act in the wake of several Supreme Court cases that oscillated on the constitutional implications of wiretapping, with the Court finally and famously concluding in *Katz v. United States* that as "the Fourth Amendment protects people, not places," warrantless wiretapping by the government was unconstitutional.[66] The law was intended to limit the privacy invasions that wiretapping enables while allowing law enforcement to continue to rely on it in a carefully limited, constitutionally permissible manner, as outlined by the Court in *Berger v. New York* and *Katz*.[67] Congress updated the law's protections for wire and oral communications to include electronic communications in 1986, and made additional tweaks to the law in 1994 and 2001.[68]

The Wiretap Act identifies three categories of communications for protection—wire communications, oral communications, and electronic

62. Carol M. Bast, *Conflict of Law and Surreptitious Taping of Telephone Conversations*, 54 N.Y.L. SCH. L. REV. 147, 150 (2009).

63. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 2:29 (3d ed., rev. vol. 2019).

64. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV 801, 841 (2004).

65. *Id.* at 846 (citing Berger v. New York, 388 U.S. 41, 48–49 (1967)).

66. *See Berger*, 388 U.S. at 47–49; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

67. S. REP. NO. 90-1097, at 46 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2163 ("Working from the hypothesis that any wiretapping and electronic surveillance legislation should include the above constitutional standards, the subcommittee has used the Berger and Katz decisions as a guide in drafting title III."); Carol M. Bast, *What's Bugging You?: Inconsistencies and Irrationalities of the Law of Eavesdropping*, 47 DEPAUL L. REV. 837, 842 (1998).

68. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 384–85 (2014); Bast, *supra* note 67, at 842.

communications[69]—which can essentially be understood as telephone conversations, surreptitiously recorded oral conversations, and digital communications that exclude voice recordings. It prohibits the intentional interception, disclosure, or use of the contents of wire, oral, and electronic communications unless the interceptor is a party to the communications, the interceptor obtains consent from one of the parties, or an exception applies.[70] The statute is enforceable both by federal prosecutors and private plaintiffs,[71] whom the statute authorizes to obtain "statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000"; if greater, actual damages; punitive damages, when appropriate; and attorney's fees.[72] While the hassle and expense of suit will deter the vast majority of potential plaintiffs, and others may be kept out of court on civil claims by arbitration clauses[73] and other procedural hurdles, damages and attorney's fees are nevertheless potentially meaningful teeth.

The District of Columbia and every state but Vermont have their own counterparts to the federal statute, all of which make wiretapping a criminal offense and thirty-five of which provide a civil action for private plaintiffs.[74] Thirty-eight of these laws mirror the Wiretap Act by requiring only one party to consent to a recording. Twelve states[75] require all parties

69. 18 U.S.C. § 2511(1)–(2).

70. *Id.* § 2511.

71. *Id.* § 2520.

72. *Id.*

73. In a recent example, an ongoing class action suit in the Ninth Circuit concerning allegations that Amazon violated the Wiretap Act by surreptitiously recording people with its Alexa devices currently depends on whether or not the plaintiffs be compelled to arbitrate, rather than litigate, their claims, despite the fact that the consent to arbitration was provided by the device owner only, in the form of accepting a boilerplate terms of service contract during the device activation process. Brief for Public Justice, P.C. as Amicus Curiae Supporting Plaintiffs-Appellees, B.F. v. Amazon.com, Inc., No. 20-35359 (9th Cir. 2020).

74. Hannah Clarisse, Note, *Wiretapping in a Wireless World: Enacting a Vermont Wiretap Statute to Protect Privacy Against Modern Technology*, 43 VT. L. REV. 369, 379 (2018).

75. These states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. REPS. COMM. FOR FREEDOM OF THE PRESS, REPORTER'S RECORDING GUIDE 1, 2 (2012), https://www.rcfp.org/wp-content/uploads/imported/RECORDING.pdf [hereinafter REPORTER'S RECORDING GUIDE]. The Michigan Supreme Court has yet to resolve the open question of whether all parties must consent to one of the parties recording a private conversation. *Reporter's Recording Guide: Michigan*, REPS. COMM. FOR FREEDOM OF THE PRESS (May 2020), https://www.rcfp.org/reporters-recording-guide/michigan.

to consent to the interception of oral and wire communications under most circumstances, such that the device owner alone providing consent to the interception, disclosure, or use of a recording without the consent of her conversational partner would be insufficient. These states have taken a range of approaches in defining when consent is required, such as whether the conversation was "secret."[76] California, Connecticut, Massachusetts, Montana, Nevada, and Washington require that all parties consent to secret recordings.[77] These states have defined secrecy in a range of ways,[78] and some provide examples of how it might be overcome, such as with an audible beep at specific intervals (Connecticut[79]) or an announcement made in a "reasonably effective manner" at the beginning of the recording (Washington[80]).

Other states define protected circumstances through the lens of when recording subjects have a reasonable expectation of privacy. Maryland and Illinois require that all parties consent to the recording in situations where the parties have a reasonable expectation of privacy in their communications.[81] Pennsylvania law requires that all parties consent to recording, except in situations where there is no reasonable expectation that the communications would not be intercepted.[82] New Hampshire does not have any secrecy requirement or explicitly establish a reasonable-expectation-of-privacy standard, but the New Hampshire Supreme Court

---

76. REPORTER'S RECORDING GUIDE, *supra* note 75.

77. *Id.*

78. *Id.*; *see, e.g.*, MASS. GEN. LAWS ch. 272, § 99 (1998).

79. CONN. GEN. STAT. § 52-570d (2019).

80. WASH. REV. CODE § 9.73.030 (2021) ("Where consent by all parties is needed pursuant to this chapter, consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded.").

81. MD. CODE ANN., CTS. & JUD. PROC. § 10-401(13)(i); Agnew v. State, 197 A.3d 27, 35 (Md. 2018) (defining an "oral communication" as being spoken in private); *Reporter's Recording Guide: Maryland*, REPS. COMM. FOR FREEDOM OF THE PRESS (May 2020), https://www.rcfp.org/reporters-recording-guide/maryland/; 720 ILL. COMP. STAT. 5/14-1, 5/14-2 (2014) (defining the offense of eavesdropping on a "private conversation" and "private electronic communication"); 725 ILL. COMP. STAT. 5/108B (1976) (defining "private communication"); *Reporter's Recording Guide: Illinois*, REPS. COMM. FOR FREEDOM OF THE PRESS (May 2020), https://www.rcfp.org/reporters-recording-guide/illinois/.

82. 18 PA. CONS. STAT. § 5703 (1988); Commonwealth v. Byrd, 235 A.3d 311, 320 (Pa. 2020).

has permitted constructive consent when the totality of circumstances demonstrated that the subject was aware of the recording.[83]

B. State and Federal Consumer Protection Laws

Wiretapping laws were crafted to target surveillance by law enforcement, as well as privacy-invasive conduct by individuals. But the outsized role that private industry now occupies in creating, selling, and licensing surveillance technologies means that the conduct targeted by wiretap laws is also subject to laws intended to constrain predatory trade practices, such as state and federal unfairness and deception statutes and COPPA. Unlike the wiretap statutes, these laws generally lack a private right of action, making their enforceability contingent on the resources, priorities, and political will of regulators who have often struggled to hold tech companies accountable for privacy violations.[84] Consumer protection statutes are nevertheless an additional area of the law that always-on devices appear to frequently violate, and the statutes represent another area of law where the status quo approach to privacy rights is ill-adapted to how people actually use and understand data-collecting technologies.

The FTC is the primary consumer privacy regulator in the United States, and deceptive trade practices are the bread and butter of FTC privacy policy.[85] The reasonable belief that a company made deceptive statements or omissions about its products and services in a way that would materially mislead a reasonable consumer entitles the agency to seek injunctive and monetary relief from a company to be sanctioned by an internal administrative law judge or a federal court.[86] These sanctions include

83. State v. Locke, 761 A.2d 376, 380–81 (N.H. 1999) (citing N.H. REV. STAT. ANN. §§ 570-A:1 to 570-A:11 (1986 & Supp. 1999)).

84. *See generally* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 774–76 (2020) (describing how privacy law is failing to constrain privacy violations, in part due to the hollowing out of public enforcement mechanisms); Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 356 (2015) (same); Craig Timberg, *Sex, Drugs, and Self-Harm: Where 20 Years of Child Online Protection Law Went Wrong*, WASH. POST (June 13, 2019), https://www.washingtonpost.com/technology/2019/06/13/sex-drugs-self-harm-where-years-child-online-protection-law-went-wrong/ (discussing COPPA's failure to reign in pervasive collection and misuse of children's data, largely due to underenforcement).

85. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628 (2014) (describing the FTC's use of its deception authority in privacy cases).

86. *See* FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 1–2, 2 n.4, 5–6 (Sept. 2021), https://www.ftc.gov/reports/ftc-report-congress-privacy-security

corrective marketing campaigns, refunds, and other measures intended to specifically and generally deter corporate predation.[87] Misleading representations might take the form of advertising materials, privacy policies, statements by executives, and other descriptions of the product or service that would lead the consumer to make a purchasing decision they would have declined to make with relevant information. Relevant privacy cases have rested on circumstances like a children's toy company falsely stating in a privacy policy that consumer information would be encrypted when it was not,[88] a payment app mischaracterizing the extent to which consumer transactions were visible to the public,[89] a router company that touted the security of its product while leaving consumers vulnerable to their webcams being hacked,[90] and similar cases based on misleading representations and contravened expectations.[91] State statutes targeting unfair and deceptive trade practices offer attorneys general the opportunity to pursue similar claims,[92] and the FTC sometimes works with them on particular cases.[93] Unfair and deceptive practice statutes have served as a privacy stopgap in the void left by the absence of a federal comprehensive privacy law, and the statutes are both highly relevant to the problem of

(describing consumer redress approaches, including the new constraints placed on the agency's ability to obtain monetary relief for consumers by a recent Supreme Court case, *AMG Cap. Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (2021)).

87. *Id.* at 1–2, 4–6.

88. Press Release, Fed. Trade Comm'n, Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

89. Press Release, Fed. Trade Comm'n, PayPal Settles FTC Charges That Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

90. Press Release, Fed. Trade Comm'n, FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras (Jan. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

91. Solove & Hartzog, *supra* note 85, at 629–30 (describing additional privacy deception cases).

92. *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016).

93. *FTC Hearing #14: Roundtable with State Attorneys General*, FED. TRADE COMM'N (June 12, 2019, 8:30 AM), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-14-roundtable-state-attorneys-general.

surreptitious and accidental recordings by always-on devices and deeply reflective of the flawed vision of notice and choice as an effective method of privacy governance. Policing broken promises can be valuable, but given that a company can avoid liability for disclosing exploitative practices in a sufficiently artful way, more focus on the practices themselves is needed.[94]

The FTC and state attorneys general also enforce COPPA, which governs companies' collection and use of children's private information. The statute requires companies that direct online services to children under the age of thirteen, or that have actual knowledge they are collecting the personal information of children under thirteen, to provide clear and conspicuous notice of their collection and use to their parents and obtain their verifiable consent, among other requirements.[95] Given that children are subjected to recording by always-on devices intended for adults as well as always-on devices intended for child-specific use,[96] COPPA is similarly relevant here.

C. The Role of Consent and Reasonable Expectations of Privacy

Consent plays a pivotal role in the privacy laws that govern always-listening devices. In the case of the Wiretap Act and one-party consent state statutes, one person assenting to recording means that the other party to the conversation can be legally recorded without their knowledge.[97] When sued, companies are certain to argue that device owners consented to

94. *See* Brookman, *supra* note 84, at 358 ("Under this line of [FTC deception] cases, the baseline privacy law in the United States was effectively 'don't go out of your way to lie about what you do.'").

95. 15 U.S.C. §§ 6501–6506.

96. *See, e.g.*, CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD ET AL., *IN RE* REQUEST FOR INVESTIGATION OF AMAZON, INC.'S ECHO DOT KIDS EDITION FOR VIOLATING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT iii-iv (2019), https://www.law.georgetown.edu/wp-content/uploads/2019/05/Echo-Dot-Complaint-FINAL-1.pdf; E.J. Dickson, *Kids' Toys Are the Latest Battleground in the Online Privacy Wars*, VOX (Dec. 13, 2018, 1:16 PM EST), https://www.vox.com/the-goods/2018/11/21/18106917/kids-holiday-gifts-connected-toys (describing the COPPA concerns stemming from toys with audio recording capabilities, ensuing advocacy campaigns, and responses by the FTC and other consumer privacy regulators); GINA STEVENS, CONG. RSCH. SERV., LSB10051, SMART TOYS AND THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998 (Jan. 8, 2018), https://crsreports.congress.gov/product/pdf/LSB/LSB10051 (same).

97. 18 U.S.C. § 2511(2)(d); NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 938, 951 (N.D. Cal. 2014); Christina Wong, Comment, *The Need for the Federal Wiretap Act to Expand Protection of Our Wireless Communications*, 16 U. PA. J. BUS. L. 333, 358 (2013) (describing consent as "immediately remov[ing] a subject from the statute's protections").

accidental recordings because they had to tick an "I accept" box below a privacy policy to use the device.[98] Courts start from the argument that acceptance of a privacy policy can be sufficient to establish explicit consent, though the validity of the consent tends to rely on the discrepancy between the alleged conduct and the company's description of it, ignoring the problem of unequal bargaining power, decision fatigue, and other factors that prevent privacy policies from facilitating informed privacy decision-making.[99] Vague descriptions of data use may not be sufficient for a company to successfully argue that users provided explicit consent for any and all uses of their data,[100] but that will depend on the specific language of the policy that very few people are likely to read, even fewer will understand, and hardly anyone will be in a position to correctly process the associated risks, much less respond to them accordingly.

Consent is also fundamental to the substance and enforcement of consumer privacy laws, including unfairness and deceptive practice statutes and COPPA, without accounting for the practical realities of the cognitive limitations that skew privacy decision-making,[101] structural obstacles to the ability to reject undesirable terms, or meaningful requirements for knowing,

98. *See, e.g.*, *In re* Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1028–29 (N.D. Cal. 2014); *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013); Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014); Campbell v. Facebook Inc., 77 F. Supp. 3d 836, 847 (N.D. Cal. 2014).

99. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1029 (considering whether Yahoo email users provided consent vitiating their Wiretap Act claims that the company had intercepted their electronic communications, and determining that the users' acceptance of the Yahoo privacy policy and the fact that it was available to them constituted "explicit" consent); *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *14 (explaining that a reasonable user "would not have necessarily understood" Gmail's privacy policy to permit additional methods of obtaining electronic communications and uses of those communications); *Backhaut*, 74 F. Supp. 3d at 1046 ("In light of the specific language of the license agreement, the Court concludes that a reasonable iMessage user would not be adequately notified that Apple would intercept his or her messages when doing so would not 'facilitate delivery' of the messages.").

100. *Campbell*, 77 F. Supp. 3d at 847 (holding that Facebook users' acceptance of a privacy policy that disclosed that the company "may use the information we received about you" for "data analysis" was "not specific enough to establish that users expressly consented to the scanning of the content of their messages—which are described as 'private messages'—for alleged use in targeted advertising").

101. Solove, *supra* note 6, at 1883–88.

voluntary, and well-informed consent.[102] The FTC has long considered notice and choice the bedrock of its approach to consumer privacy enforcement.[103] Historically, most of its enforcement has targeted how a company deceives its users, rather than normative condemnation of the practices the company sought to hide.[104] Yet that procedural approach to privacy enforcement sets a low bar for business practices considered worthy of sanction.[105] It is relatively easy for a company to provide a legally sufficient form of notice, but there is a vast distance between what that notice entails and the kind of informed autonomy that consent regimes assume that notice can foster.[106]

Indeed, the fallacies underlying the logic of consent regimes in privacy laws have been repeatedly documented and widely decried.[107] The notion that providing disclosures about collection practices will enable informed consumer choices and thus prevent widespread privacy invasions ignores lack of information, cognitive difficulties hindering meaningful decision-making,[108] lack of available alternatives, and other structural difficulties

---

102. Richards & Hartzog, *supra* note 61 (arguing that consent is a valuable mechanism that privacy law currently relies upon too heavily in ways that redound to the detriment of individual privacy and autonomy).

103. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998) (describing notice as the "fundamental" basis of the agency's privacy approach); *see also* Solove & Hartzog, *supra* note 85, at 634 (describing notice and choice as "one of the most central aspects" of the agency's work).

104. *See* G.S. Hans, Note, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 165 (2012) (describing the FTC's reliance on its deception authority in privacy cases).

105. Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 525 (2018) ("The idea that privacy controls such as notice and choice are adequate to protect consumers in the current environment has been described as quaint.").

106. Richards & Hartzog, *supra* note 61, at 1471–72.

107. The Editorial Board, *How Silicon Valley Puts the 'Con' in Consent*, N.Y. TIMES (Feb. 2, 2019), https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html; Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1072 (2019) [hereinafter Barrett, *Confiding in Con Men*] (describing years of critiques of notice-and-choice privacy governance by policymakers, privacy scholars, social scientists, and consumer advocates).

108. Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J., no. 1, 2018, at 1, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1634&context=chtlj [hereinafter Barrett, *Model(ing) Privacy*] (discussing literature documenting the hindering effects of bounded

that make "take it or leave it" an ineffective privacy governance mechanism. People encounter far too many data-collecting technologies in a day to make reading the privacy policy of each one a rational choice,[109] and even if they tried to read each one, the information they contain is often insufficient to explain the relevant risks, if not outright misleading.[110] More importantly, the most clearly written privacy policy in the world can't facilitate meaningful choice in a highly consolidated ecosystem where an alternative product or service just doesn't exist.[111] Nor can it improve the highly limited human capacity to effectively evaluate risk.[112] The rosy picture of a frictionless interaction fueled by perfect information also ignores the inconvenient reality of how corporate incentives are shaped by money, power, and regulatory inaction. Years of "light-touch" governance have facilitated the growth of a technological ecosystem that blames people for choices they're ill-equipped to make, all while their information is bought and sold by companies they've never engaged with.[113]

Smartphones, for example, are a functionally unavoidable part of modern life. Many people rely on them to do their jobs and stay in touch with family and friends, and the few who don't are frequently within recording range of those who do.[114] The idea that phone owners' clicked agreement to

---

rationality, hyperbolic discounting, the difficulty with assessing cumulative risk, and decision fatigue hindering privacy decision-making).

109. *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 543 (2008) (noting that privacy policies can take a significant time to skim and are encountered on many websites by Internet users).

110. *See* Joel R. Reidenberg et al., *Disagreeable Privacy Polices: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 86–87 (2015); Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 274 (2012); Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 77 (2018).

111. *See, e.g.*, Kashmir Hill, *I Cut the 'Big Five' Tech Giants from My Life. It Was Hell*, GIZMODO (Feb. 7, 2019, 12:00 PM), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

112. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 43 (2021).

113. *See, e.g.*, Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCHOL. & PERSONALITY SCI. 340, 341 (2012) (noting that "users have very little control over the way in which information, once posted [on Facebook], will be used by a third-party application").

114. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("Cell phone location information is not truly 'shared' as one normally understands the term. . . . [C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life'

an inscrutable policy constitutes informed consent for secretly recording their conversations and using that information for any purpose seems like a fairytale's contract used to teach children about unfairness. And yet, the legal fiction that clicking past a boilerplate privacy policy that no one in their right mind would read constitutes "control" over one's privacy choices persists, carefully guarded by the powerful entities whose profits depend on acceptance of the myth.[115]

The primacy of hinging privacy protections on people's expectations of privacy has also been criticized, if not to quite the same degree. The Fourth Amendment's *Katz* test—requiring a probable-cause warrant before a search or seizure of persons, papers, or effects by the government, absent consent or a litany of other exceptions—has been characterized as circular, given that prediction of a privacy invasion is tantamount to acceptance thereof.[116] The Fourth Amendment's reliance on the *Katz* standard is directly relevant for the Wiretap Act, as its drafters were responding to the Supreme Court's jurisprudence on the topic, and judges have frequently

---

that carrying one is indispensable to participation in modern society." (citing Riley v. California, 134 S. Ct. 2473, 2484 (2014))).

115. While technology companies in the United States argued for years against any sort of privacy regulation whatsoever, their messaging strategy has shifted to pushing for weak privacy laws based on notice and choice that emphasize "transparency" and "control." *See* Barrett, *Confiding in Con Men*, *supra* note 107, at 1065, 1071; Mark Zuckerberg, Opinion, *The Facts About Facebook*, WALL ST. J., Jan. 25, 2019, at A15, https://www.wsj.com/articles/the-facts-about-facebook-11548374613 ("Ultimately, I believe the most important principles around data are transparency, choice and control. We need to be clear about the ways we're using information, and people need to have clear choices about how their information is used. We believe regulation that codifies these principles across the internet would be good for everyone."); Sundar Pichai, Opinion, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, N.Y. TIMES, May 8, 2019, at A25, https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html ("Privacy is personal, which makes it even more vital for companies to give people clear, individual choices around how their data is used."); *see also* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016) (criticizing the "control illusion").

116. Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) ("[A] knowledge-based Fourth Amendment will shrink and weaken over time as public awareness of new technologies and threats to privacy continues to grow."); *see also* U.S. CONG. OFF. OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 18 (1985) (reviewing the need to update the Wiretap Act to include electronic communications) ("Determining whether a place is sufficiently private to offer protection against official surveillance is more and more difficult as the public sphere of activities encroaches on what was once deemed private.").

read the statute's "expectation of non-interception" test to be interchangeable with it.[117] Privacy expectations are also a key component analyzing what would deceive a "reasonable consumer" in the context of unfair and deceptive trade practice enforcement.[118] Consumer privacy scholars have highlighted the role that resignation and learned helplessness play in how people perceive their privacy choices; if your data is constantly collected and used without your permission, and there is rarely any meaningful opportunity to prevent that from happening, it can be difficult to find a reason to "expect" privacy at all.[119]

A race to the bottom that denies protections in response to the rational conclusion that past experiences can be predictive erodes privacy protections against surreptitious recordings. As always-listening devices become more and more prevalent, judges may decide that the expectation of being recorded is more rational than the expectation of being let alone. As the expectation of non-interception is part of the definition of "oral communications," that logic would exclude surreptitious listening from being subject to the Wiretap Act at all, while a consumer acting "reasonably" will be required to expect and guard against privacy invasions they can't avoid. Expectations are not a sufficient mechanism for gauging the appropriateness of privacy protections under such circumstances.

IV. The Study

As detailed above, privacy expectations and preferences affect the applicability of the Wiretap Act's protections for oral communications, certain state wiretap statutes, deception and unfairness enforcement by the

117. *See* Bast, *supra* note 67, at 842.

118. CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 123–25 (2016); McSweeny, *supra* note 105, at 517 (describing the modern FTC's approach as "address[ing] reasonable consumer expectations regarding the collection, use, and protection of their data").

119. Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 NEW MEDIA & SOC'Y 1824, 1825 (2019); Madiha Tabassum et al., "*I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks*, *in* USENIX, PROCEEDINGS OF THE FIFTEENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 435, 443–46 (2019), https://www.usenix.org/system/files/soups2019-tabassum.pdf (describing participants in a study on the privacy attitudes of smart home users as being subject to "optimism bias"—the assumption that a possible risk is unlikely to occur for the subject personally—and reporting participants' assumptions that they incur only "marginal" additional risk to their privacy from the use of smart home devices when compared to the information already collected about them).

FTC and state attorneys general, and privacy torts,[120] and these expectations and preferences are frequently highlighted in discussions of what new privacy laws should look like.[121] With the outsized role of expectations and consent in privacy law and policy in mind, one of us conducted a study examining participants' privacy preferences, expectations, and decision-making concerning the use of voice-activated assistant technologies, whether as a stand-alone device in their home or as a smartphone app.[122]

Previous privacy and security research has examined the privacy preferences, knowledge, and behaviors of voice assistant and smart speaker users,[123] as well as the problem of bystanders having data collected about them without their knowledge or consent.[124] But only a few studies have

120. This Article does not examine the role of the privacy torts in depth, primarily because they don't play as large a role in corporate considerations of privacy risks and are thus less influential for the kinds of invasions that occur. *See generally* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMM. & HIGH TECH. L. 357, 384 (2011); Danielle K. Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1806 (2010) ("[T]he privacy torts often cannot properly redress contemporary privacy injuries."); Solove & Hartzog, *supra* note 85, at 587 (citing *The Limits of Tort Privacy* by Neil M. Richards and noting that "common law torts fail to regulate the majority of activities concerning privacy"); Scott Skinner-Thompson, *Privacy's Double Standards*, 93 WASH. L. REV. 2051, 2051 (2018) (describing privacy tort law as "beleaguered").

121. Barrett, *Model(ing) Privacy*, *supra* note 108, at 35 (describing the role of privacy expectations in policy discussions).

122. Liccardi & Dominguez Veiga, *supra* note 1.

123. *See, e.g.*, Josephine Lau et al., "Alexa, Stop Recording": Mismatches Between Smart Speaker Privacy Controls and User Needs (Sept. 2018) (poster presented at the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)), https://www.usenix.org/sites/default/files/soups2018posters-lau.pdf (finding that voice assistant users have an incomplete understanding of related privacy risks and rarely adopt available privacy controls); Noura Abdi et al., *Privacy Norms for Smart Home Personal Assistants*, *in* ACM, CHI '21: PROCEEDINGS OF THE 2021 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS paper 558 (2021), https://dl.acm.org/doi/pdf/10.1145/3411764.3445122 (registration required) (applying Helen Nissenbaum's contextual integrity framework to a range of scenarios involving privacy preference regarding recording, focusing exclusively on the device owner as the subject).

124. Eric Zeng et al., *End User Security & Privacy Concerns with Smart Homes*, *in* USENIX, PROCEEDINGS OF SOUPS 2017: THIRTEENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 65 (2017), https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf (examining, inter alia, the "mismatch between the concerns and power of the smart home administrator and other people in the home"); Eric Zeng & Franziska Roesner, *Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study*, *in* USENIX, PROCEEDINGS OF THE 28TH USENIX SECURITY SYMPOSIUM 159 (2019), https://www.usenix.org/system/files/sec19-zeng.pdf

focused on how device owners consider sharing behaviors when captured audio includes accidental recordings of other people.[125] "Wiretapping Your Friends" addresses a key question that has gone unanswered by the literature: given technologies that can accidentally and surreptitiously record both the device owner and unsuspecting bystanders, what do the owners of those devices believe is their responsibility towards those people, and how do they evaluate different privacy risks? The researchers hoped to develop a better understanding of the factors influencing people's willingness to allow audio recordings to be captured and shared.

To answer those questions and assess people's preferences, perceptions, and behavior relating to potentially surreptitious recordings by voice-assistant technologies, the researchers created a mixed-method empirical study of cross-sectional and longitudinal observations.[126] The bespoke apps

---

(examining "how peoples' behavior and usage of the smart home can impact each others' security and privacy"); Yaxing Yao et al., *Privacy Perceptions and Designs of Bystanders in Smart Homes*, 3 PROC. ACM ON HUM.-COMPUT. INTERACTION article 3 (Nov. 2019), https://dl.acm.org/doi/pdf/10.1145/3359161 (examining the privacy perceptions and concerns of bystanders themselves); Karola Marky et al., "*I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments*, *in* ACM, NORDICHI'20: THE 11TH NORDIC CONFERENCE ON HUMAN-COMPUTER INTERACTION article 4 (2020) (examining the problem of voice assistants violating the privacy of their owners to bystanders, and noting that both device owners and bystanders reported "wish[ing] for a device mode that considers the presence of bystanders"); Martin J. Kraemer et al., *Further Exploring Communal Technology Use in Smart Homes: Social Expectations*, *in* ACM, CHI'20: EXTENDED ABSTRACTS OF THE 2020 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS LBW116 (2020), https://arxiv.org/pdf/2003.04661.pdf (online study examining communal use of technology in smart homes, touching briefly on how participants considered the privacy concerns of guests in offering to pair their phones with smart home systems); Christine Geeng & Franziska Roesner, *Who's in Control?: Interactions in Multi-User Smart Homes*, *in* ACM, CHI 2019: PROCEEDINGS OF THE 2019 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS paper 268, at 9–10 (2019), https://dl.acm.org/doi/pdf/10.1145/3290605.3300498 (briefly noting the privacy implications of recording devices in smart homes for guests and other non-residents).

125. Hyunji Chung et al., *Alexa, Can I Trust You?*, COMPUTER, Sep. 2017, at 100; Schönherr et al., *supra* note 56; Dubois et al., *supra* note 55 (providing a systematic review of false positives).

126. Liccardi & Dominguez Veiga, *supra* note 1, at 5.

Procedure and Participants in the study:

Participants: The study was advertised in twenty-one of the thirty-eight one-party consent states, excluding Nevada (a one-party consent state in which the Supreme Court interprets the law as requiring all-party consent). *Id.* at 8. Participants were recruited through different social media groups, e-mail mailing lists, Craigslist, and paper flyers posted in

and devices examined included Amazon Alexa, Google Home, and apps like OK Google and Samsung Bixby.[127] Current users and non-users of voice-activated devices who wanted to participate in the study were first interviewed and asked about their capture and sharing preferences regarding audio recordings. In particular, the researchers inquired about how participants would choose to share or not share audio recordings that captured utterances by other individuals.[128]

Next, the researchers had participants install a bespoke app[129] on their smartphones designed to capture audio files, and then interviewed subjects before and after it was installed to gauge their privacy behavior associated with voice-activated devices.[130] The initial interview was conducted to evaluate participants' existing perceptions, preferences, and usage of voice assistants, including their perceptions of how the respective companies behind the devices capture and use the data.[131] This was then followed by a one-to-one information session to familiarize participants with the study procedures and to install a bespoke Experience Sampling Method ("ESM") Android app.[132] The app collected data on the participants' preferences and usage of voice assistants, as well as their perceptions on how the respective companies behind the devices would use their data.[133] After this

---

public spaces. *Id.* at 6. Fifty-three participants completed the study: eighteen females (avg. age = 32), thirty-four males (avg. age = 31), and one non-binary individual (avg. age = 21). *Id.* at 11–12. These participants were spread across nineteen one-party consent states: Alabama, 1; Georgia, 2; Idaho, 1; Indiana, 3; Kentucky, 1; Louisiana, 1; New Jersey, 4; New York, 3; North Carolina, 5; Ohio, 1; Oregon, 2; South Carolina, 3; Tennessee, 2; Texas, 3; Utah, 1; Vermont, 11; Virginia, 6; West Virginia, 1; Wisconsin, 2. *Id.* at 12, 12 n.19.

Procedure: People wanting to participate in the study signed up using an online questionnaire. Participants were asked to confirm the state in which they were located (this was corroborated during the information session) as well as provide demographic information and ownership and usage of their own voice-activated devices. *Id.* at 6. Participants who met the study requirements (i.e., were located in the one-party consent states) were contacted and asked to meet online using video conference software with the researchers. *Id.* at 8. The study was approved by an internal review board.

127. *Id.* at 5, 9. The researchers did not study Apple devices. *See id.* at 11 (noting that the app for data collection was compatible only with Android devices).

128. *Id.* at 5.

129. Study participants were told that the researchers wanted to test a new voice detection algorithm and compare it to the results from the Google Speech API. *Id.* at 6.

130. *Id.* at 5.

131. *Id.*

132. *Id.*

133. *Id*.

longitudinal experience phase, the researchers interviewed participants again to assess whether any of their answers deviated from the data sharing and collection preferences that they initially reported.[134]

Several trends in participants' reported perceptions and behaviors illustrate the mismatch between a consent-focused legal regime and the responses of always-on device owners to the privacy concerns of the people around them. Key factors that weighed heavily on the participants' decisions included the perceived or known preferences of other individual(s) captured in the audio recording;[135] the content of the recording; the participants' own perceived preferences;[136] the participants' own perceived benefits from sharing the information;[137] and in particular, the intimacy of the relationship with the other individual(s) captured in the audio recording.[138] Participants carefully considered the privacy preferences of close-knit relations, which heavily influenced whether they shared recordings or took part in the study.[139] But participants frequently disregarded the preferences of more distant relationships, such as colleagues, clients, or doctors.[140] With the exception of two participants who informed people of the study on a need-to-know basis, and three participants who did not disclose it to anyone (even their spouse or partner), the remainder disclosed the aim of the study to close-knit relations, who were often recorded.[141]

Participants reported considering and even often asking people they were close to about their specific preferences (related to a captured conversation) or general preferences (related to their preferences about sharing their information for the duration of the study) when they believed the other person would likely be recorded.[142] In fact, in some cases their loved ones' preferences took precedence over their own.[143] Participant 2 reported that

134. *Id*.
135. *Id.* at 21–23.
136. *Id.* at 13–14.
137. *Id.* at 20.
138. *Id.* at 21–23.
139. *Id.* at 21.
140. *Id.* at 22.
141. *Id.* at 21. One participant disclosed their participation in the study to their partner after a couple of weeks, as they were starting a new relationship and were afraid that it might not had been received well. *Id.*
142. *Id.*
143. *Id.*

he would have shared more had it not been for his partner's uneasiness of sharing even "complete random nonsense" and not wanting to lie to her:

> *[Participant 2:] I started to select 'not sharing' when she was involved so that I could definitely and honestly tell her that I had done so.*[144]

Even in instances where close-knit relations were not informed about the study, participants reported considering them when making their choices:

> *[Participant 35:] I thought that whatever didn't connect the person to the information that was being recorded would be all right to share [. . .], there were some times where confidently talking to each other—like about personal stuff—I wouldn't share even if it didn't have any identifying content. Just like trying to fulfil their wishes.*[145]

That was not always the case when children were involved. For example, Participant 6 reported sharing conversations that captured them disciplining their child.[146]

In contrast, the thirty-one participants who reported being employed decided not to share the information with their colleagues.[147] Participants explained that it could have caused problems and might have affected the way in which people would have reacted around them.[148] For example, Participant 2 reported making the decision for them because they were not sharing the information anyway:

> *[Participant 2:] If I ask anybody if they were okay with it—about what was going on—they had said, 'yes, that's okay, [they] can release my information.' That's essentially either accidentally or intentionally violating our company policy so either way it did not make sense [to ask them]. I was deciding for them because*

144. *Id.*

145. *Id.* at 22 (second alteration in original).

146. *Id.* ("I did not ask him because he might not want to share it but I would. In fact, I would welcome it, to share it with companies in case they could help with parenting tips, being a single parent and all.").

147. *Id.* at 21.

148. *Id.*

> *even if that's a yes it was going against what [they] should have really said [. . .] I was making the smart decision for them.*[149]

Participant 2 continued to explain that even in circumstances where the information could have been shared, he chose not to share those recordings with researchers because he would have wanted to inform his colleagues:

> *[Participant 2:] There were some conversations that were actually not work related so could be shared but it goes back to my previous point because I have to tell that it is on all the time — even when we are having conversations that should be isolated — so I decided for all or nothing situation whether I will just tell everybody or I will just not tell anybody and assume that no sharing would happen.*[150]

Participants also reported instances in which they were willing to violate what they perceived and knew to be their colleagues' preferences and shared conversations when they knew those colleagues might be recorded. One participant reported that his colleagues would likely object to being recorded given that they move out of frame when he takes pictures, but the participant did not care about respecting those clear preferences.[151]

Furthermore, when people from distant or non-existent relations were also captured, participants (with the exception of two) reported not consulting or even considering their possible preferences.[152] Only a small number of friends were asked about their preferences, while the remainder of the distant relationships—clients, acquaintances, health professionals or strangers—were never asked.[153] In fact, when distant or non-existent relations were part of a recording, participants reported their preferences took precedence even if that meant knowingly contravening the preferences of others. Participant 13 reported instances where they felt as though they probably should have not shared the information, even to the point of feeling that they should have not recorded it at all, but did so regardless.

> *[Participant 13:] If I had told people, I felt like I would have liked created a problem that I did not know how to solve, theoretically I could have put my phone somewhere else but then*

149. *Id.* (second, third, and fifth alterations in original).
150. *Id.*
151. *Id.*
152. *Id.* at 22.
153. *Id.*

> *I would have not had my phone . . . that it make me feel more uncomfortable, so I kept it.*[154]

Participants reported not needing to consider or even think about distant people's preferences when deciding how to share the recording, given that they were not the ones participating or deciding in the first place.[155]

> *[Participant 19:] I did not really care if other people heard it or not and if other people (in the conversation) do, that is on them, if they differ from my opinion honestly I just didn't care [. . .] I did not really think about what they wanted as much, it was my decision whether to share it or not.*[156]

For the few participants who reported considering distant relations in their decision-making process, their expectation of privacy was very low to none, which they attributed to the types of listening devices that are available and popular today.[157]

> *[Participant 23:] In 2019, I think it's inevitable with all of the smart devices happening, you know, your information, all information, you know is essentially public at this point [. . .] if I wanted to not share something, I wouldn't talk about it in the vicinity of any of my smart devices, actually, so I think, you know, I care less because I understand how much less privacy there is.*[158]

V. Implications for Existing Privacy Laws

The study's reported consent practices point to a likely failure of many companies to comply with existing wiretap laws, as well as unfair and deceptive practices statutes and COPPA. Not only are accidental recordings capturing device owners without their consent, but it is highly unlikely that third parties are aware that they might be recorded, or that their consent is being obtained in any sort of way. The following section discusses how

154. *Id.* at 22 (second alteration in original). This participant also shared these instances when the study did not require them to. The researchers further inquired about this behavior and their motivations for their choices, and the participant reported that "it was their [the participant's] decision to do so." *Id.*

155. *Id.* at 22.

156. *Id.* (second alteration in original).

157. *Id.*

158. *Id.* at 22–23 (second alteration in original).

companies are likely violating those laws and why their available legal defenses will often be untenable.

A. State and Federal Wiretapping Laws

As discussed in Section III.A, federal and state wiretapping statutes prohibit the intentional interception and disclosure of the contents of wire, electronic, and oral communications unless the interceptor is a party to the communications, obtains consent from one of the parties, or one of a few exceptions applies. The plaintiff must demonstrate that the defendant intentionally intercepted the contents of an oral communication using a device.[159] Intentionally disclosing, using, or endeavoring to disclose or use the contents of communications that the person or entity knew or had reason to know were obtained in violation of the statute is also prohibited.[160]

In the case of an always-on device, the company operating the device intentionally intercepts the contents of oral communications—not merely metadata, or attributes about the recording like the date or length of recording, but the recording itself—when the always-on device sends a recording to the cloud for processing. These recordings are most aptly characterized as "oral communications" under the Federal Wiretap Act,[161] as they are utterances by people who believe their conversations are not being recorded by their devices (such as device owners when their devices are accidentally recording them, or bystanders unaware that they could be or are being recorded), in a circumstance justifying that expectation.[162]

159. *See supra* Section III.A.

160. 18 U.S.C. §§ 2511(1)(a)–(d).

161. There is some variation in how state wiretap statutes define "oral communications," with most states following the federal language minus the reference to electronic communications (which Congress added in 1986). Arizona, Georgia, Maryland, Massachusetts, New York, Ohio, Texas, and Washington do not define "oral communications" specifically, while Florida's definition excludes "any public oral communication uttered at a public meeting." 1 JAMES G. CARR ET AL., LAW OF ELECTRONIC SURVEILLANCE § 3:5 (rev. ed. Aug. 2021).

162. 18 U.S.C. § 2510(2); *see also* Kee v. City of Rowlett, 247 F.3d 206, 211 n.7 (5th Cir. 2001); United States v. Turner, 209 F.3d 1198, 1200 (10th Cir. 2000); United States v. McKinnon, 985 F.2d 525, 527 (11th Cir. 1993); S. REP. NO. 90-1097, at 2178 (1968) (stating the legislature intended the statutory definition for "oral communication" to reflect pre-existing law). The Wiretap Act's statutory definition requires an oral communication to be "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation," 18 U.S.C. § 2510(2), which was drafted in response to Fourth Amendment cases and mimics Justice Harlan's language

The Wiretap Act defines "intercept[ion]" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[163] Courts have not categorically defined when the act of "interception" takes place, and the analysis will be fact specific. We believe that a voice-activated device sending recordings to a remote server—i.e., to the company—constitutes an "acquisition." The device company likely does not "acquire" the contents of oral communications when a device does not rely on cloud-based computers to process requests, such that the recordings remain on the user's device without ever being sent to a remote server.[164] The companies would also be separately liable for "use," such as using the recordings for targeted advertising or improving the machine learning capabilities of their devices, or "disclosure" to third parties (such as contractors).

The intentionality requirement demonstrates why interceptions should be attributed to the service provider and not the device owner: the very problem with always-on devices is that both the owner and the other parties being recorded will often be unaware that false positive recordings are happening. The "Wiretapping Your Friends" study involved informing

---

in *Katz* of "an actual (subjective) expectation of privacy" where "society is prepared to recognize [that expectation] as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Some courts have referred to the Wiretap Act's requirement as a "reasonable expectation of privacy," though some commenters have suggested that conflation of the two tests would nullify certain scenarios involving § 2511(2)(d)'s prohibition on intercepting one's own conversation for a criminal or tortious purpose. FISHMAN & MCKENNA, *supra* note 63, § 2:27. *But see* CARR ET AL., *supra* note 161, § 3:5. ("Although either view—expectation of privacy or non-interception—might be appropriate, the more accurate assessment, based on the legislative history of Title III, is whether a reasonable or justifiable expectation of privacy exists."); Kristine Cordier Karnezis, Annotation, *Construction and Application of Provision of Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. § 2520) Authorizing Civil Cause of Action by Person Whose Wire, Oral, or Electronic Communication Is Intercepted, Disclosed, or Used in Violation of Act*, 164 A.L.R. Fed. 139, § 2[a] (2000) ("The statutory definition has been referred to in short-hand fashion as a reasonable expectation of privacy.") (noting that some courts have required a "reasonable expectation of privacy" in civil actions under 18 U.S.C. § 2520 and others have required the plaintiff to show a "protectable expectation that his or her oral communications would not be intercepted").

163. 18 U.S.C. § 2510(4).

164. For example, Amazon's Alexa can revert to processing recordings on the user's device for limited functions when it cannot sufficiently rely on an internet connection, which it needs to send recordings to Amazon's cloud. *Alexa Confidentiality and Data Handling Overview*, *supra* note 50, at 4 n.2. A device that processed recordings locally, without ever sending them to the company's remote servers for analysis, could avoid this problem.

participants that their devices would record others in order to gauge what participants believed their social obligations were in a range of scenarios, but most device users, including the users of voice-activated devices specifically, aren't terribly knowledgeable about the privacy risks their devices create.[165] The overwhelming majority of device owners couldn't "intentionally" record the oral communications of the people around them, because they won't realize that the accidental recordings are happening. What's more, these recordings are "unintentional" in so far as the device is recording due to its incorrect perception that someone has uttered the wake word. But the companies selling the devices are aware of this deficiency and nevertheless profit from the recordings they produce, which should be sufficient to demonstrate intentionality.[166] A software bug could be unintentional, but the choice to build a profitable infrastructure around a bug is not. Moreover, one-party wiretap laws like the federal statute and those in thirty-eight states are generally predicated on the idea that the act of interception necessarily involves a third party.[167]

In the case of the Wiretap Act, the "expectation of non-interception" requirement in the definition should also be met in many cases involving always-on devices. The expectation does not depend on the sensitivity of what is recorded, but rather the expectation that the conversation is not recorded;[168] a banal conversation where the utterer had reason to believe the conversation is not recorded, such as small talk made in a dressing room at a volume that would be difficult to overhear, would most likely be protected.[169] A Superior Court of New Jersey case involving a television

165. Lau et al., *supra* note 123.

166. *See, e.g.*, Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014); *see also in re* Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 815–16 (N.D. Cal. 2020) ("The Court agrees with Plaintiffs and these various courts that interceptions may be considered intentional where a defendant is aware of the defect causing interception and takes no remedial action. . . . To be clear, the Court does not hold that inaction in the face of a known design defect *necessarily* makes an interception 'intentional' under the Wiretap Act—only that the facts alleged here are sufficient to survive a motion to dismiss." (emphasis added)).

167. Rauvin Johl, *Reassessing Wiretap and Eavesdropping Statutes: Making One-Party Consent the Default*, 12 HARV. L. & POL'Y REV. 177, 181–82 (2018) (citing Billeci v. United States, 184 F.2d 394, 397 (D.C. Cir. 1950)) (concluding that, based on the assumption of third-party involvement, "recordings made by a party or with a party's consent should not qualify as eavesdropping or wiretapping").

168. FISHMAN & MCKENNA, *supra* note 63, § 2:24.

169. *See, e.g.*, LaPorte v. State, 512 So. 2d 984 (Fla. Dist. Ct. App. 1987) (holding that speech made between models when "in a state of undress or in the process of changing clothes" was private, based upon the models' expectation of privacy); Planned Parenthood

network sued by police officers for filming them provided a non-exhaustive list of factors bearing on the expectation of non-interception, including the volume of the conversation, the proximity of others in earshot, the potential for communications to be reported, the steps taken by speakers to protect their privacy, whether "technological enhancements" are required to hear the conversation, and where the conversation takes place.[170] The potential scenarios involving always-on devices vary wildly, but many should find favor under those factors particularly given the assurances people receive from always-on device companies that the device only records on command, the fact that they're generally used indoors, and the recording device itself is a "technological enhancement."

The unavoidability of the false positives should also make it more likely that a court will find that a plaintiff has an expectation of non-interception.[171] Making privacy self-help a prerequisite for legal protections has troubling implications given how difficult and ultimately futile any self-help attempts tend to be. The flaws of that standard aside, it would be difficult to blame most plaintiffs for failing to avail themselves of privacy-protective steps that they're either unaware of or simply don't exist.[172] In a case involving a conversation recorded via the plaintiff's pocket dial, the United States Court of Appeals for the Sixth Circuit found his failure to take "a number of simple and well-known measures" such as merely

---

Fed'n Am., Inc. v. Ctr. For Med. Progress, 402 F. Supp. 3d 615, 688–92 (N.D. Cal. 2019) (describing the test as "whether the person being recorded had a subjective expectation of privacy and whether that expectation was reasonable under the circumstances" and analyzing those expectations against the subjective belief in the privacy of the recorded conversations and the steps taken to keep them private).

170. Hornberger v. Am. Broad. Cos., 799 A.2d 566, 593 (N.J. Super. Ct. App. Div. 2002) (citing Kee v. City of Rowlett, 247 F.3d 206, 213–15 (5th Cir. 2001)).

171. The variations in the precise standards articulated in state wiretapping laws, beyond the number of parties required to consent makes the analysis of relevant conduct slightly different in some cases. The Wiretap Act's preemption of less protective state laws means that no statute may provide lesser privacy protections, but the specifics of state standards and their subsequent interpretation over time by state courts may nevertheless be meaningful. S. REP. NO. 90-1097, at 2187 (1968); *see also* Leong v. Carrier IQ Inc., Nos. CV 12-01562 GAF (MRWx), CV 12-01564 GAF (MRWx), 2012 WL 1463313, *3 (C.D. Cal. Apr. 27, 2012) (discussing the Wiretap Act's preemption of lesser protective state laws and sanction of more protective ones).

172. *See* Huff v. Spaw, 794 F.3d 543, 550 (6th Cir. 2015) (noting that a plaintiff's mere "internal belief in privacy" is insufficient to satisfy *Katz*'s reasonable-expectation test and that a plaintiff must "*exhibit* an intention to keep statements private" through affirmative steps and safeguards against third-party exposure).

locking the device, setting up a passcode, or using an anti-pocket-dial app precluded him from exhibiting an expectation of privacy.[173] Here, false positives will often be entirely unavoidable, given that they result from the malfunctioning of the device, including in situations where a third party is unaware that a device was present.

Product design choices intended to minimize potential privacy invasions could influence a judge's interpretation of assumption of the risk, and companies that allow their customers to delete recordings, or to opt out of having their recordings saved or transcribed, may argue that the plaintiff's expectation of non-interception is undermined by a failure to do so. Some courts may find such an argument compelling. They should not, as it fails to consider how difficult it is for individuals to manage their privacy decisions, and acceptance of this line of thinking would reinforce corrosive precedents of expecting individuals to take burdensome steps that most people don't take in order to receive legal protections for their privacy. Certainly, the failure to exercise an opt-out or privacy control couldn't be held against someone who doesn't have access to the device. Reasoning behind Chief Justice Roberts's decision in *Carpenter v. United States* concerning assumption of the risk when assumption is functionally involuntary could also support rejecting these types of argument, given that judges frequently invoke Fourth Amendment precedents in wiretapping cases.[174]

The terms of service, instructions, and marketing of always-on devices frequently emphasize that an affirmative command, whether in the form of a wake word or pushing a button, is required for the device to record the user's utterances.[175] People buy those devices believing those assurances,

---

173. *Id.* at 552.

174. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018); Lindsey Barrett, *Carpenter's Consumers*, 59 WASHBURN L.J. 53, 57 (discussing Chief Justice Roberts's analysis of assumption of the risk in expectation of privacy analysis, which repudiates the idea that the act of carrying a smartphone can obviate a reasonable expectation of privacy).

175. *See generally Is Alexa Recording?*, AMAZON, https://perma.cc/H53P-V6WM (last visited Feb. 1, 2021) ("The answer to all these questions is no. Privacy is built in to Alexa and all of our Echo devices, from wake word technology to microphone controls to the ability to review and delete the voice recordings associated with your account."); *Google Nest Commitment to Privacy in the Home*, GOOGLE, https://perma.cc/JB22-6M9G (last visited Dec. 10, 2020) ("Your home is a special place. It's where you get to decide who you invite in. It's the place for sharing family recipes and watching babies take first steps. You want to trust the things you bring into your home. And we're committed to earning that

and they proceed about their daily lives engaging in the kinds of activity that they would otherwise have every reason to believe is not being recorded and collected by some company, such as private conversations in their homes, their cars, or those of friends or colleagues.[176] The failure to find an expectation of privacy based on the absence of self-help or resignation to privacy invasions would profoundly erode the Wiretap Act's privacy protections for oral communications. Accepting the argument that people should expect to be spied upon and taken advantage of—even when a company violates the explicit promises to only record upon the owner's request, promises that those people subsequently relied upon—affirmatively condones and invites that malfeasance.

Consent to recording from one or all of the parties plays a crucial role in both state statutes and the Wiretap Act, and in most cases, companies are failing to obtain it from the full array of people being recorded. Companies almost certainly aren't obtaining consent in all-party consent states, where everyone being recorded must give their consent. But even in one-party consent states, the device owner's acceptance of a terms-of-service contract should not suffice as consent for recording other people without their knowledge when that consent is insufficient to permit surreptitious recordings of even the device owner. And as the "Wiretapping Your Friends" study illustrates, most device owners probably aren't bothering to alert the people around them potentially being recorded by always-on devices. Under the Wiretap Act and one-party consent state statutes, the interception is not prohibited if one party to the conversation gives consent to the recording.[177] Consent must be explicit, and the subject's awareness of the technical possibility of interception, rather than awareness of actual interception, is insufficient.[178] A party can provide consent to only some communications, but not all of them.[179]

---

trust."); *HomePod Privacy and Security*, APPLE, https://perma.cc/BEK6-EH2Y (last visited Feb. 3, 2021) ("Security and privacy are fundamental to the design of HomePod.").

176. *See generally Nest Audio*, GOOGLE STORE, https://store.google.com/product/nest_audio?hl=en-US (last visited Dec. 10, 2020) (screenshot on file with authors) ("Privacy built in. Nest Audio is designed to protect your privacy. You can delete your history by saying, 'Hey Google, delete what I just said.'"); *Apple Home Pod*, APPLE https://perma.cc/WEB8-H826 (last visited Dec. 10, 2020) ("HomePod and HomePod mini keep everything private and secure, and only listen for 'Hey Siri.'").

177. Wong, *supra* note 97, at 358.

178. Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).

179. Griggs-Ryan v. Smith, 904 F.2d 112, 119 (1st Cir. 1990) ("The parameters of consent may be circumscribed depending on the subtleties and permutations inherent in a

The question here is whether consent obtained by the device owner's acceptance of a privacy policy constitutes consent to the interception of false positive recordings. We believe it does not and should not. As Orin Kerr emphasized in the context of internet service providers' monitoring their customers' browsing history, the standard is actual consent, not constructive consent, where the person recorded has been provided with clear notice and opted to continue using the service regardless.[180] The overwhelming majority of people do not read privacy policies—and even if they did, most of the popular services do not clearly describe how their recording devices work such that users could provide informed consent.[181] Acceptance of opaque boilerplate does not constitute specific, actual consent to unsolicited recording, particularly for non-device owners who are recorded and will have almost never received notice of any kind.

Of course, electronic communications (like someone's internet browsing history) and oral communications (like conversations recorded by an always-on device) are not directly interchangeable. But the privacy interests in conversations the speakers had no reason to believe were being recorded is certainly comparable to the interest in one's browsing history, particularly given the prevalence of always-on device being used in the home, and the rich tradition of protections for the home as a private zone. And as Kerr notes, most of the cases establishing the consent standard involved the interception of telephone calls, which is a close analogue to the utterances and conversations that an always-on device records.[182]

---

particular set of facts."); *In re* Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003) ("A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications.").

180. Orin Kerr, Opinion, *The FCC's Broadband Privacy Regulations Are Gone. But Don't Forget About the Wiretap Act*, WASH. POST (Apr. 6, 2017), https://www.washingtonpost.com/news/117olokh-conspiracy/wp/2017/04/06/the-fccs-broadband-privacy-regulations-are-gone-but-don't-forget-about-the-wiretap-act/; *see also* United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) ("The surrounding circumstances must convincingly show that the party knew about and consented to the interception in spite of the lack of formal notice or deficient formal notice.").

181. *See, e.g.*, Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; Kim Hart, *Privacy Policies Are Read by an Aging Few*, AXIOS (Feb. 28, 2019), https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html (presenting survey results in which 56% of respondents reported "always" or "usually" accepting privacy policies without reading them).

182. Kerr, *supra* note 180.

Relevant decisions in which tech companies have argued that consent to a boilerplate privacy policy is sufficient under the statute also support the view that consent to a vague privacy policy is insufficient to excuse the interception, use, or disclosure of surreptitious recordings.[183] An ongoing class action alleging violations of the Wiretap Act, Stored Communications Act, and a number of California laws based on Google's collection of Google Assistant recordings obtained via passive listening makes the same argument, which the presiding judge preliminarily accepted.[184]

Other consent exceptions should similarly fail to provide a defense. Courts have made certain exceptions for consent offered on behalf of spouses and children, but that would only extend to recording instances involving those relationships.[185] Moreover, courts have increasingly narrowed the circumstances when spouses and parents can provide such consent. Six circuits have held that there is no interspousal exception to the Wiretap Act, while five have not addressed the issue.[186] Other courts have recognized that a parent or guardian may provide consent on behalf of minor children, but narrowed the acceptable circumstances to when the parent has concerns about the child's safety.[187] Parents don't provide consent to the makers of always-on device companies because they believe that the company is constantly recording the child for the child's safety, to the extent that they knowingly provide that consent at all.[188]

---

183. *In re* Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 789–90 (N.D. Cal. 2019); Campbell v. Facebook Inc., 77 F. Supp. 3d 836, 847 (N.D. Cal. 2014); *In re* Google Location Hist. Litig., 428 F. Supp. 3d 185, 192 (N.D. Cal. 2019) (rejecting that consent to location tracking during use of a map app constitutes consent to store location data).

184. *In re* Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020).

185. Cary J. Mogerman & Stephanie L. Jones, *The New Era of Electronic Eavesdropping and Divorce: An Analysis of the Federal Law Relating to Eavesdropping and Privacy in the Internet Age*, 21 J. AM. ACAD. MATRIM. L. 481, 494–95 (2008).

186. *Id.* at 500.

187. State v. Whitner, 732 S.E.2d 861, 864 (S.C. 2012) (holding that as long as the minor child's mother had a good faith and objectively reasonable basis for believing that the recording of her child's telephone conversation with the defendant, the child's father, was necessary and in the best interest of the child, the consent provision of the State Wiretap Act (S.C. Code Ann. § 17-30-30(C)) applied to and encompassed the "vicarious consent" doctrine such that the mother could vicariously consent on behalf of the child to the recording).

188. Other ostensibly applicable exceptions will likely be insufficient to excuse the collection and use of surreptitious recordings by always-on device makers, such as the "ordinary course of business" exception. The exception only applies to the statute's

For both states that clearly require all-party consent and the states that hinge consent from all parties on a reasonable expectation of privacy, passive listening by always-on devices is unlikely to meet those standards. The possibility that always-on devices are violating those laws thus has considerable implications for individual privacy, for the companies selling those devices, and for privacy law and policy. If device users typically aren't getting consent to record the people around them and companies are collecting, using, or disclosing those recordings, that should create liability for the company. Both the state and federal wiretap statutes are enforceable by government prosecutors and individuals, which means that the practical implications of violations are ideally more meaningful than a hypothetically applicable law that regulators don't have the time or wherewithal to

---

definition of "telephone equipment" (which always-on devices wouldn't be), and the conduct must be within the user's ordinary course of business, as well as "instrumental" to the provision of the actual service. Courts have confirmed the narrowness of the exception when companies have previously attempted this argument in online tracking cases, holding that the kinds of interceptions permitted by the exception must actually facilitate the communications service, not simply render it more lucrative, and that accepting the companies' interpretation would contradict the meaning of the statute and congressional intent in enacting it. *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *9 (N.D. Cal. Sept. 26, 2013), *motion to certify appeal denied*, 2014 WL 294441, at *4 (N.D. Cal. Jan. 27, 2014) ("[T]he statutory scheme suggests that Congress did not intend to allow electronic communication service providers unlimited leeway to engage in any interception that would benefit their business models, as Google contends."); *id.* at *8–11 (finding that for the exception to apply, there must be "some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good"); *Campbell*, 77 F. Supp. 3d at 844 ("The court rejects the suggestion that any activity that generates revenue for a company should be considered within the 'ordinary course of its business.'"). Making advertising more granular and the company's data sets even more valuable is not necessary to provide a voice assistant service; it is simply conducive to its further monetization.

The exception also only applies to wire and electronic communications, not oral communications—which makes sense, considering that the Wiretap Act's authors in the 1960s and its amenders in the 1980s did not contemplate eavesdropping-as-a-service for which an "ordinary course of business" exception would be remotely relevant. The use of phones (wire communications) and email (electronic communications) involves intermediaries with legitimate service quality prerogatives, whose carefully limited ability to monitor the efficacy of their services addresses the needs of consumers, as well as the needs or preferences of the service providers. Oral conversations conducted with an expectation of privacy and nevertheless recorded by a mechanical device would have appeared at the time to lack the same infrastructural component and corresponding need. The exception is extremely narrow, and simply does not apply to the collection and use of audio recordings without consent to make data collection even more profitable.

enforce.[189] The damages available to plaintiffs also make violations an impactful consideration. The legal status quo is tenuous and points to larger problems in privacy law and policy that will continue to be created by always-on devices, and which are not limited to wiretapping laws.

B. State and Federal Consumer Protection Laws

The failure of device companies and device owners to obtain consent from everyone being recorded has similarly significant implications for consumer protection laws, including COPPA and state and federal unfairness and deceptive practice statutes. Recording third parties without their consent, while representing that the devices only record when the wake word is uttered, is exactly the kind of practice that the FTC has previously found to be material in unfairness and deception cases.[190]

Representations by tech companies that their devices only record conversations upon the utterance of a specific command are misleading, as are omissions of specific, clear, and unambiguous disclosures that the recordings might occur at other times and will be used by the company for a range of purposes other than fulfilling the device owner's command, such as advertising. There are minor distinctions from product to product in terms of the privacy representations the companies make—as discussed in Part II, some of the bigger companies that were criticized for their undisclosed use of human contractors to transcribe recordings have made a range of product changes, both cosmetic and substantive. But the space between "our device only records you when you say the wake word and we care deeply about your privacy" and "our device will often record you, as well as people who haven't consented to being recorded, and our company will use those recordings for whatever we want" is, broadly speaking, a material misrepresentation for the companies still making the former claim.[191] Consumers acting reasonably would assume that the company is

189. *Cf.* Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 535 (2017) (describing the track records of private litigation in vindicating privacy harms as "stunningly poor" as the result of "denial of standing, enforcement of boilerplate waivers, denial of class certification, disposal via opaque multidistrict litigation proceedings, and cy pres settlements").

190. *See supra* Section III.B.

191. *See generally* Letter from James C. Miller, Chairman, to Hon. John Dingell, Chairman, Comm. on Energy and Com., H.R., (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf ("A 'material' misrepresentation or practice is one which is likely to affect a consumer's choice of or

not lying to them when it claims to only record them and the people around them when they say the wake word. The acquisition and/or use of surreptitious recordings is unequivocally material, as it would change people's willingness to purchase the product.

The collection and use of surreptitious recordings might also constitute an unfair trade practice under the FTC Act or state unfair and deceptive acts and practices statutes. An unfair trade practice is one that causes or is likely to cause significant injury to consumers and is not reasonably avoidable by them, with no countervailing benefits to consumers or competition.[192] The authority rests on the inherent danger of the practice itself, rather than the company's characterizations of it, and establishes a higher bar for the regulator to justify the intervention, as they are required to show a finding of injury that deception does not require. The FTC has frequently relied on deception arguments in privacy cases, but it has made unfairness claims in a number of cases that involve data security practices that violate people's privacy, such as a dating website that failed to take reasonable steps to secure users' information, like robust protocols to access a corporate virtual private network,[193] and a smart TV company that conducted pervasive and invasive tracking on everything people watched through a setting that was nearly impossible to locate and disable.[194] Having all kinds of sensitive information recorded and used without one's knowledge is a substantial injury, and given that always-on devices don't make clear when they're recording (or may not be visible to the people being recorded), the injury is not reasonably avoidable.

In addition to state and federal wiretap laws and unfair and deceptive practices, many always-on devices are likely violating COPPA. Voice recordings are personal information subject to the statute, and unless companies are discarding every recording in which a child's voice is included (or using it to complete a direct request from the child, and then

---

conduct regarding a product. In other words, it is information that is important to consumers.").

192. Letter from Michael Pertschuk et al., Chairman, FTC Commissioners to Hon. Wendell H. Ford, Senator, & Hon. John C. Danforth, Senator (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

193. Complaint for Permanent Injunction and Other Equitable Relief at 9–10, FTC v. Ruby Corp., No. 1:16-cv-02438 (Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf.

194. Complaint for Permanent Injunction and Other Equitable and Monetary Relief at 8–9, FTC v. Vizio, Inc., No. 2:17-cv-00758 (Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

discarding it), operators are required to obtain verifiable parental consent from the parents or guardians of every child whose voice recording they're collecting and failing to delete—which they are almost certainly not doing.[195] A legally acceptable method of verifiable parental consent must be reasonably calculated to ascertain that the consent obtained is from the child's parent or guardian, such as by requiring a small credit card charge refunded to the parent when a child's user account is created.[196]

The vast majority of companies collecting this information will almost certainly claim that COPPA does not apply to their service, which is a tenuous claim at best. Most always-on device companies will argue that their services are for audiences of all ages, rather than targeted to children (frequently true), and that they do not have the actual knowledge of collecting children's personal information that the statute requires for general audience services. But these companies are labeling and transcribing recordings and will often be able to infer that the speaker is a child. And the objective of these transcriptions, after all, includes identifying various attributes of the speakers from the recordings. It is simply implausible that companies whose business models rely on pervasive and granular data collection are unaware that a child is in the household, particularly when information about children in a household is a primary indicator of purchasing behavior—key for the advertisers these companies make their money from. Other companies offer specifically child-directed voice services, like the Echo Dot Kids' Edition.[197] COPPA governs companies' collection of private information, such as voice recordings, from children under thirteen in either situation.

While some of these companies could be obtaining verifiable parental consent when the adult who bought the device is the guardian of the child being recorded, they do not appear to be obtaining it for any other children that the device records. If Child A has a playdate at the home of Child B, Parent B may have given verifiable parental consent for any recordings of

195. *See generally* Fed. Trade Comm'n, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings (Oct. 20, 2017), https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.

196. *Complying with COPPA: Frequently Asked Questions: Verifiable Parental Consent*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#I.%20Verifiable%20Parental%20Consent (last visited Feb. 2, 2021).

197. *See* CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD ET AL., *supra* note 96.

Child B, but cannot provide (and likely did not contemplate providing) verifiable consent for Child A. If common sense and the "Wiretapping Your Friends" study are any indication, the likelihood that parents are even attempting to obtain consent in this way—or feel an obligation to do so—is slim at best. The collection, use, or disclosure of recordings under such circumstances violates COPPA.[198] The statute does not include a private right of action, but it is enforceable by both the FTC and state attorneys general, all of whom have their work cut out for them.

VI. Broader Policy Implications

This Article has illustrated how surreptitious, accidental recordings by always-on devices are likely violating state and federal wiretap and consumer protection laws. The possibility that regulators could bring enforcement actions, or that individual plaintiffs could bring suit based on those violations, has very real implications for the companies selling those devices as the law currently stands. But those implications rest on a key assumption: that the regulators in charge of enforcing those laws have the resources and political will to enforce them. Private rights of action under state and federal wiretap laws may present a more meaningful deterrent to companies, but COPPA and unfair and deceptive acts and practices statutes rely on the FTC and the state attorneys general for their penalties to mean anything at all. Tech companies have rampantly violated U.S. privacy laws with impunity, in part due to their lack of enforcement, and will have no reason not to continue doing so unless regulators give them a reason to stop.[199] They must do so, and the elected officials those regulators answer to must ensure their capacity to change corporate incentives by funding enforcement agencies like the FTC and state attorney general offices, demanding more vigorous enforcement efforts,[200] and supporting regulators when those efforts are the subject of disingenuous attacks.[201]

---

198. *See id.*

199. *See generally* Waldman, *supra* note 84, at 774–75 (describing how privacy law is failing to constrain privacy violations, in part due to the hollowing out of public enforcement mechanisms).

200. *The Technology 202: The Government's Top Silicon Valley Watchdog Only Has Five Full-time Technologists. Now It's Asking Congress for More*, WASH. POST (Apr. 4, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/04/04/the-technology-202-the-government-s-top-silicon-valley-watchdog-only-has-five-full-time-technologists-now-it-s-asking-congress-for-more/5ca512661b326b0f7f38f30d/ (describing the FTC Chairman's request to the House Energy and Commerce Committee for

Even for cases where the legal theories under relevant wiretap statutes are strong, private plaintiffs will face an uphill battle, given the chasm between the right to sue a company for illegal conduct and the practical ability to do so. Decades of judicial hostility to privacy litigants[202] and the widespread use of forced arbitration clauses will be substantial obstacles, as though finding the time and resources to vindicate violated rights through litigation weren't difficult enough for most people already. That doesn't mean that plaintiffs' firms and advocacy groups shouldn't try, particularly given the ripple effects that individual cases can have for companies attempting to anticipate and mitigate future liability concerns. But litigation alone cannot solve this problem or the broader systemic problems of corporate surveillance that surreptitious listening devices exemplify. Proactive and structural changes that limit invasive corporate practices are needed.

Those changes must focus on the exploitative practices of corporations, not the wishful fantasy that a better set of privacy controls for individual users can correct the power imbalance between powerful companies and the people they surveil. The fact that always-on devices often record people in the background without their consent, and that many companies are likely using these recordings to build ever more granular profiles of the people they record, is just one more example on a very long list illustrating the futility of consent-based approaches.[203] A consent regime that coalesced with the reality of always-on devices would depend on social practices that do not currently exist and which would never be a reliable or consistent safeguard: parents requiring other parents to read a privacy policy and give their consent to the device company before a playdate, dinner party hosts doing the same for their guests, and so forth. The flaws of human decision-making compel an approach that primarily focuses on regulating corporations, not individuals. Policymakers asking judges for injunctive relief or drafting new privacy laws must resist the pretense that privacy self-

---

more money and staff, given that the agency has only forty full-time staff focused on privacy and five full-time technologists, as opposed to the UK's counterpart agency's five-hundred-person staff or Ireland's 110, countries with much smaller jurisdictions).

201. *See, e.g.*, Lindsey Barrett et al., *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 BERKELEY TECH. L.J. 793, 816 (2021) (describing such attacks and citing Luke Herrine's additional history of them); Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 467, 506–09 (2021).

202. Cohen, *supra* note 189; Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361–63 (2014).

203. *See generally* Solove, *supra* note 6.

management (and indeed, privacy bystander management) is an effective governance scheme and instead focus on corporate use limitations and prohibitions, retention limitations, deletion requirements, and changes that make those protections expensive and risky to ignore, as well as strengthening regulatory capacity to conduct vigorous oversight and enforcement.

In addition, the effect of resignation on privacy expectations reported by study participants illustrates why privacy expectations should not be the sole dictate of legal protections for people's privacy. Resignation to privacy violations and learned helplessness make an expectation-based standard a race to the bottom,[204] and the unpredictability of those expectations and preferences makes coherent application difficult. Privacy laws and regulations should be designed to reorient the structural incentives of companies away from collecting first and asking questions later, rather than relying on the reactions of people who've understandably grown accustomed to having their privacy invaded. Any expectation-based standard to determine the degree of protections people will receive for their privacy must account for the effects of resignation and lack of meaningful choice. Regulators and courts applying expectation-based standards must address how resignation and lack of choice molds those expectations, and those that don't will further entrench an exploitative feedback loop that favors corporate profit incentives over the imperative of protecting individual rights. Future privacy laws should learn from the mistakes of current ones and avoid making privacy expectations determinative of privacy protections.

VII. Conclusion

Always-on devices are just one example of a larger paradigm in technology policy. They're often cheap and tremendously popular; they're sold by powerful companies with the means and motivation to broaden their already substantial market power by making these devices ubiquitous; they violate people's privacy on a massive scale that regulators have, so far, failed to meaningfully constrain; and they illustrate the fundamental failure of consent as a primary privacy safeguard, and the severe limits of tying privacy protections to resignation-skewed expectations.

---

204. Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 NEW MEDIA & SOC'Y 1824 (2019); Solove, *supra* note 112, at 5 ("Resignation is a rational response to the impossibility of privacy self-management.").

But as the genesis of wiretapping laws illustrates, both real people and the laws designed to protect their privacy have long treated surreptitious recordings as an unusually severe invasion. The right advocacy strategy and public awareness campaign could enable always-on devices to serve as the example of why meaningful sector-wide privacy reforms that fundamentally remold corporate incentives are so badly needed. At the very least, one might hope that an enterprising state attorney general or the FTC might take notice of the companies violating an array of privacy laws by surreptitiously listening to their customers and decide to do something about it.

The "Wiretapping Your Friends" study illustrates the need to acknowledge privacy as a broader, collective social problem. Privacy decisions aren't made in a vacuum, and they have collective consequences that a focus on individual decision-making often ignores.[205] A privacy governance model that relies exclusively on individual decision-making will always provide inadequate protections, and a model that hinges privacy protections on the decisions of every smartphone owner we come into contact with is even weaker still. The focus of new privacy laws and regulations must be on reversing corporate incentives to violate individual privacy, rather than continuing to rely on a paradigm that those companies hope to preserve because of how dangerously permissive it is.

205. *See generally* Emre Sarigol et al., *Online Privacy as a Collective Phenomenon*, *in* ACM, COSN'14: PROCEEDINGS OF THE 2014 ACM CONFERENCE ON ONLINE SOCIAL NETWORKS 95 (2014), https://arxiv.org/pdf/1409.6197.pdf; Bernadette Kamleitner & Vince Mitchell, *Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements*, 38 J. PUB. POL'Y & MKTG. 433, 433 (2019), https://journals.sagepub.com/doi/pdf/10.1177/0743915619858924; Barocas & Levy, *supra* note 7.