Journal of Artificial Intelligence and AI Ethics

SCIVOLVE

Research Article

Open Access Full Text Article

Listening Whether I Like it or Not: You, Me, Zoom, and Your Alexa

Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.
— Judith Jarvis Thomson (1975)

J. L. A. Donohue[*1]

[1]*Assistant Professor, Department of Philosophy, University of Arkansas, 313 Old Main, University of Arkansas, Fayetteville, AR 72701.*

***Correspondence:**
J. L. A. Donohue
Assistant Professor,
Department of Philosophy, University of Arkansas,
313 Old Main, University of Arkansas, Fayetteville, AR 72701, USA.

Received: January, 05, 2026; **Accepted:** January 23, 2026; **Published:** January 29, 2026.

How to cite this article:
J. L. A. Donohue. (2026), 'Listening Whether I Like it or Not: You, Me, Zoom, and Your Alexa', *Journal of Artificial Intelligence and AI Ethics*, vol. 1, no. 1, pp. 1–7.

Abstract

Amazon recently announced the removal of a privacy setting on its Echo devices that had allowed users to opt out of having their voice requests sent to the company's cloud servers (Rascoe 2025). While users may still choose not to save voice requests, those requests will be sent to "Amazon's secure cloud" before deletion. This policy change exacerbates the already serious privacy concerns that Echo and other "always-listening" devices (such as Apple's HomePod and Google's Home) raise. In order to do what they are designed to do, such systems continually listen for their "wake" word: a word that is designed to alert the device to listen and respond to user commands. Because they are always listening and frequently recording, these devices carry a high risk of inadvertently recording private conversations without consent. The privacy invasions made possible by these devices are significant, and ought to be taken seriously by both regulators and ordinary members of the public.

In this paper, I explore the privacy concerns raised by "always-listening" devices by focusing on a case study: our increased reliance on Zoom meetings for professional and personal purposes during the COVID-19 pandemic. Because many of us were newly on Zoom with classmates, coworkers, and friends during this period, we were newly exposed to others' always-listening devices. Even those of us who had deliberately avoided always-listening devices for privacy reasons may have been unwittingly and unwillingly recorded while in Zoom meetings with others who had always-listening devices in their homes. While these privacy-oriented individuals may have consented (explicitly or implicitly) to being recorded for expressly educational purposes such as a class's being recorded so an absent or sick student could watch it later, they are unlikely to have understood themselves as consenting to being recorded by an always-listening device.

After arguing that these individuals' privacy rights were likely violated, I draw implications for the regulation of always-listening devices. I argue that existing privacy laws provide affected individuals with little legal recourse, and that further legislative action in this area is required to protect citizens' reasonable privacy concerns.

Keywords: Privacy; Always-listening devices; Voice assistants; Consent; Digital surveillance; Zoom; Technology ethics

1. Introduction

Amazon recently announced the removal of a privacy setting on its Echo devices that had allowed users to opt out of having their voice requests sent to the company's cloud servers (Rascoe 2025). While users may still choose not to save voice requests, those requests will be sent to "Amazon's secure cloud" before deletion. This policy change exacerbates the already serious privacy concerns that Echo and other "always-listening" devices (such as Apple's HomePod and Google's Home) raise. In order to do what they are designed to do, such systems continually listen for their "wake" word: a word that varies from device to device

and is designed to alert the device to what the user says next so that it can respond to a command. Because they are always listening and frequently recording, these devices raise special privacy concerns, recording house guests without their consent, inadvertently recording would-be private conversations after a so-called "false wake,"[1] and even recording audio of sexual assault that is then listened to by Amazon staffers[2].

These concerns are justified, and the privacy invasions made both possible and actual by these devices are significant: they ought to be taken seriously by the public and legislature alike. The focus of this paper is on a particular kind of privacy concern that is raised by the combination of always-listening devices and the huge increase in the use of Zoom meetings to handle education, business, and social life during the COVID-19 pandemic.

Because many of us were newly on Zoom with classmates, conference participants, and countless others, we were unwittingly exposed to always-listening devices even if we did not have them in our own homes. Even people who have explicitly avoided always-listening devices for precisely the kinds of privacy concerns I mention above may have been unwittingly and unwillingly recorded while in a Zoom meeting with another person who has an always-listening device in their home. While they may have consented (explicitly or implicitly) to being recorded for expressly educational purposes such as a class's being recorded so an absent or sick student could watch it later, they are unlikely to have understood themselves as consenting to being recorded by an always-listening device.

Unfortunately, as I will explain below, not much recourse is available legally for such persons under any statute that only requires one-party consent for recording, including ECPA (Electronic Communications Privacy Act) and others. COPPA (Children's Online Privacy Protection Act) may offer more protection, though even that is limited. More promising are statutes that require two-party consent, though even here the argument that legal recourse is available and possible will be tentative (and certainly has not yet been affirmed by the courts, though some relevant cases are pending). In this paper, I focus on Alexa-enabled devices because this focus allows us to consider the specific details of Amazon's privacy policy and how Alexa is designed to function. Some of these concerns will also apply to other always-listening devices, but it should be noted that other companies perform better across some of the privacy dimensions I will raise here, including deleting recordings more frequently and not allowing for their employees to listen to those recordings (Kuruvilla 2019, 2035–36). I conclude by drawing implications for the regulation of always-listening devices. In sum, further legislative action in this area is required to protect citizens' reasonable privacy concerns.

2. Alexa and Privacy: COVID-19, Zoom, and Recording without Consent

Alexa-enabled devices are always listening and are designed to record audio that follows their wake word, "Alexa." For example, if a user says, "Alexa, add milk to my grocery list," the Alexa-enabled device is designed to begin recording after recognizing "Alexa" and to send the recording to Amazon's cloud so that the request can be processed. When the device detects the wake word and begins recording, it activates a visual or audible indicator to indicate that it is recording audio that will be streamed to the cloud.[3] Users have an option to review and delete their audio recordings, and they also can elect to turn off the always-listening feature and activate Alexa by the push of a button instead of an audio cue. Doing so can help to protect users' privacy by giving them greater control over what Alexa records and diminishing the numbers of "false-wakes" (instances in which Alexa records audio even though the wake word was not actually uttered).[4] However, turning off the always-listening features is not costless: a significant reason that Alexa-enabled devices are convenient is because users do not have to press a button in order to accomplish the relevant task, such as playing music, turning on the lights, or adding items to their shopping carts. The Alexa-enabled device could be across the room, your hands could be dirty, or a disabled user might not be able to touch the device for a variety of reasons. Being able simply to speak the command without touching is part of the appeal of the device in the first place, but that very feature requires the device to always be listening for its wake word.

Once the recordings are sent to Amazon, they are both reviewed and stored. Amazon employs people to review voice recordings with the express intention of improving Alexa's capacities: by reviewing the recording and how it was interpreted by Alexa, the employees can make corrections, and Alexa can even be trained to perform better on a variety of audio inputs (Kuruvilla 2019, 2034–35). By default, Amazon keeps these recordings indefinitely, but users can choose to review and delete recordings associated with their account or to change their account settings so that the recordings are automatically deleted after 3 or 18 months in the cloud. Prior to March 2025, users also had the option not to have their voice recordings sent to the cloud at all. Recently, Amazon has disabled that option: all recordings are now sent to the cloud (Rascoe 2025). The recordings and their storage raise a concern about privacy: though many recordings involve mundane comments such as requests to tell the user about the weather or to add eggs to a grocery list, some involve significantly more private content, such as a conversation between husband and wife that one Alexa-enabled device mistakenly sent to one of the husband's employees (Shaban 2018). In addition, the review of those recordings by Amazon employees raises an additional privacy concern: other people are quite literally listening to audio recorded in the user's home.

In order to set up an Alexa-enabled device in her home, a user has to agree to Alexa's terms of service, so the user has arguably consented to these recordings and the review by Amazon employees. It is less clear and even doubtful that *others* who may be recorded by the device have consented to these recordings and review. For example, guests in the user's home may be recorded by the device despite never having consented to being recorded. If an invited guest enters the home and has what she takes to be a private conversation in that home that is recorded and sent to Amazon, she may understandably be concerned about the

[1] Always-listening devices have "wake words" that are designed to indicate that the human user intends what follows as a command for the device. The device is designed to activate upon the utterance of the "wake word." A "false wake" occurs when an always-listening device "activate[s], transmit[s], and/or record[s] audio from their environment when the wake word is not spoken" (Dubois et al. 2020, 1). These are also sometimes called "misactivations." For example, Alexa's wake word is "Alexa," so a user might say, "Alexa, add milk to the grocery list." The device should "wake" upon hearing "Alexa", record and transmit "add milk to the grocery list" so that the command can be interpreted by the algorithm, and then execute the command. But researchers have found that the device "wakes" upon utterances of other words or sounds.

[2] For example, see (Kuruvilla 2019; Dubois et al. 2020; Neville 2020; Shaban 2018; Thorne 2019), among others.

[3] See Amazon's Alexa FAQ:
https://www.amazon.com/gp/help/customer/display.html?ots=1&slotNum=0&imprToken=6ebc3523-ab89-59a1-c21&tag=w050b-20&linkCode=w50&nodeId=201602230

[4] False wakes are uncommon but far from impossible (Dubois et al. 2020).

recording and review.

Further, the ubiquitous use of Zoom due to the COVID-19 pandemic resulted and continues to result in many people being exposed to Alexa-enabled devices in *other* people's homes, even while they themselves remain in their *own* homes. Though they are conducting business or attending class from their own homes, which may not contain any always-listening devices (perhaps out of privacy concerns, or perhaps for other reasons), their conversations may be recorded and sent to Amazon. In addition to concerns about the content of the recordings, there is also a concern about Amazon just having access to so many voices and potentially having that data available for later use (Thorne 2019).

3. What's the Privacy Harm Here? Why Should the Law Care?

There are different potential privacy harms related to Alexa-enabled devices' recording of users via Zoom. While it is beyond the scope of this paper to analyze them all, it is worth exploring in detail some of the main privacy harms that are worthy of communal concern and thus legal attention. The main harms on which I will focus are connected with different stages of the life cycle of data, which consists in collection, processing and use, storage, and disclosure (Mcgeveran 2016, 326). I will focus on (1) being recorded without one's consent and (2) Amazon employees listening to those recordings.

First, in the collection phase, being recorded without one's consent can constitute a moral harm, especially if one does not even have the option to avoid such recording. Because participation in Zoom meetings was mandatory for many either due to employment or school being moved online, many people do not have the option to avoid being recorded. To lose this option is a harm. One way to see this is to consider that it eliminates the possibility of conducting oneself in the absence of recording. As Julie Cohen points out, even just knowing that one is being surveilled can be experienced as intrusive (Cohen 2012, 139). Having space to explore and develop one's identity in the absence of surveillance and recording is an important moral right. So even just being recorded without the possibility of refusal amounts to a privacy harm in the moral sense.[5]

Second, in the processing and use phase, there is a privacy harm in Amazon employees *listening* to the recordings, especially if they contain personal or otherwise private information. Amazon uses the recordings not just to facilitate the function of the user's Alexa-enabled device, such as adding milk to the grocery list, but also to improve performance of the device in the future. Those who are recorded against their preference and without their consent are thus listened to by strangers.

Other harms might also arise in other phases of the data life cycle: suppose Amazon shares the recordings with a third party, or uses the recorded data to facilitate and improve advertising. Or if they inadvertently share recordings or make use of the voice recordings as biometric markers. But I will not focus on those harms here and will instead limit my discussion to the harms discussed above.

Because Amazon's Alexa-enabled devices are involved with these privacy harms, we might hope for legal recourse for the person who is recorded without their consent. For example, they may hope to be able to pursue deletion of the recording, so as to prevent future sharing of their voice data without their consent.[6] Or perhaps to seek damages for the harm of being recorded without their consent. (Amazon's privacy policy provides ways for the Alexa-enabled device *owner* to request that recordings be deleted, but third parties are unable to do so.) Someone who is recorded without their consent might have legal recourse they could pursue against either Amazon or the Alexa-enabled device owner, depending on who we understand as the person doing the recording. Unfortunately, if the device owner is taken to have given consent to the recording accepted by Alexa's Terms of Service at set-up, most legal statutes will not apply, since most jurisdictions only require one-party consent for recording content. I will assume for the remainder of my discussion that the device owner is understood to have legally consented to the recording and Amazon's storage of that recording in the cloud. So I will focus on a case in which a fellow student or colleague is recorded by the device over Zoom without their consent.[7] In the following section, I survey some of the available legal rules under which the person who has been recorded without their consent might seek damages or simply pursue deletion of the recording.

4. Legal Recourse against Amazon? Against the Alexa-Enabled Device Owner?

4.1 ECPA (Wiretapping)

The Electronic Communications Privacy Act (ECPA) seems a natural place to begin. Under ECPA, interception of telephone calls by private individuals is a crime and also a civil infraction. Significantly for our purposes, individuals have a private right of action against the government or private defendants for violations (Mcgeveran 2016, 340). ECPA classifies relevant communications into three types: wire, oral, and electronic. If we were considering the case of two persons talking in person in a house that has an Alexa-enabled device, that would count as oral communication, since they are communicating with each other orally. But our case is slightly different. We have two or more parties communicating via Zoom, which would count as a wire communication, since it is an aural transfer "for the transmission of communications by the aid of wire, cable or other like connection" (ECPA, Title 1, §2510 (1)).

In order to determine whether the Alexa-enabled device's recording of the Zoom conversation is in violation of ECPA, we need to consider whether it falls under any of the exceptions in

[5] In §4 I will explore whether it also constitutes a cognizable legal harm according to any existing legal privacy regimes in the U.S.: the argument here is limited to moral harm.

[6] One might object on behalf of the Alexa-enabled device owner that *they*, too, have rights, that they have elected to purchase and use the device, and that the device is being used in their own home. Just because Zoom has opened their homes to others, why should their autonomy rights be secondary to those of the person who would prefer not to be recorded? This is an interesting objection, and full consideration of the moral and legal questions surrounding the intersection of Zoom and Alexa-enabled devices would need to engage with it. To begin a reply, it doesn't seem to me that having an Alexa-enabled device turned on is among one's autonomy rights. We would expect that someone not blare loud music over Zoom during a meeting or class and not have overly-distracting video feeds because these interfere with the purpose of the Zoom meeting—to learn or to communicate regarding a business purpose. If Cohen is right that the risk of constant surveillance undermines our ability to learn, grow, and form our identities, it seems that Alexa-enabled devices recording Zoom meetings also interferes with their purpose (2012).

[7] In defense of Amazon or the device owner, one might argue that the other party to the conversation has also consented, especially if they have consented to the Zoom recording. I am going to assume they have not consented to the recording of what they say by the Alexa device, even if they did consent to the meeting host's recording the Zoom session for educational or business purposes. I will not fully defend this assumption here, but the reader should feel free to substitute an instance in which they agree that consent has not been given, even if that only applies to cases in which the Zoom meeting itself is not being recorded by Zoom. I would argue that even if the participant has consented to, for example, the host recording the meeting and posting it to the course website, they have not consented to Amazon having access to this recording. For a theory of privacy that might support my interpretation, see Nissenbaum's contextual privacy (2004). In this context, the transmission principle would allow for sharing with other classmates or relevant business colleagues but not with Amazon or their employees.

§2511. Significantly, §2511 (2)(d) specifies that "it shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution of laws of the United States or of any State." (Mcgeveran 2016, 343). This language is quite dispositive in Amazon's favor. Due to the nature of the Alexa-enabled device, we have two possible candidates as the recorder: the Alexa-enabled device owner and Amazon itself. Either way, the case seems to fall under the exception. The Alexa-enabled device owner is party to the communication, so if we understand them as the recorder, then their recording does not violate ECPA. On the other hand, if we understand Amazon as the recorder, then their recording also does not violate ECPA because Amazon has been given consent to record by one of the parties to the conversation namely, the Alexa-enabled device owner, since they had to agree to Alexa's Terms of Service. (Recall that we are assuming that agreeing to Alexa's Terms of Service is sufficient for consent.) So unless the recordings are "for the purpose of committing" a crime, they are not a violation of ECPA.

This result might be frustrating to the nonconsenting party. After all, *they* did not agree to have their communication recorded. Unfortunately for them, because ECPA is a one-party consent statute and one of the parties *did* consent to the recording, their lack of consent does not render the recording a violation of ECPA. We will return to the importance of consent later when we examine how the result might differ in states that require two-party consent.

4.2 COPPA

Legal privacy protections concerning children's information are more stringent than those concerning adults. There is good reason to think that this disparity is justified, perhaps along the lines of something like Joel Feinberg's concern with children's right to an open future (Feinberg 1980). The Children's Online Privacy Protection Act (COPPA) established demanding requirements for the collection and handling of personal information of young children (under the age of 13) in the online context (Mcgeveran 2016, 303). While Amazon claims that its devices adhere to COPPA, the company has been the target of several lawsuits alleging that Alexa-enabled devices illegally store recordings of children (Thorne 2019). Could the case we are considering be covered by COPPA? Consider a child call her Amber participating in an online class via Zoom with other students and a teacher, and suppose one of the children call him Bobby has an Alexa-enabled device in his home that wakes while Amber is talking and records her voice. In this case, Amber is being recorded without her consent and without the consent of her parents. Let us assume that Amber is under the age of 13, say 10. Could either Amazon or Bobby's parents be liable under COPPA for recording Amber's voice without her parents' consent?

COPPA has relatively narrow scope, prohibiting "unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet" (Mcgeveran 2016, 303). In order to determine whether the recording of Amber's voice could constitute a violation of COPPA, we first need to know whether COPPA applies. Under §312.3, "It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part" (Mcgeveran 2016, 306).

First, we note that the recording of Amber's voice does count as "personal information" according to COPPA §312.2: "*Personal information* means individually identifiable information about an individual collected online, including: (Nissenbaum 2004) a photograph, video, or audio file where such file contains a child's image or voice" (Mcgeveran 2016, 305). So, the personal information in question would be the recording of Amber's voice. COPPA protects against such collection without parental consent in the *online* context: would an Alexa-enabled device's recording count as online collection or as collection of a different sort? It seems like the recording would count as online collection due to its intimate connection to the Internet as well as the transfer of the recording to Amazon's servers.

Next, we need to consider whether the device or its use counts as an "online service directed to children" (Mcgeveran 2016, 306). Some Alexa-enabled devices seem clearly directed to children, such as the "Echo Dot Kids Edition". Others do not seem obviously directed to children. Could Amazon argue that it avoids liability under COPPA due to not directing its services to children? Perhaps, but the argument seems strained at best: it is hard to agree that Amazon does not have "reliable empirical evidence regarding audience composition" and that the company is unaware that the devices are likely to record children's voices (Mcgeveran 2016, 305). I think Amazon's best argument is a split one. That is, they should argue that cases like Bobby's should be treated differently from cases like Amber's and then give distinctive analyses of each. First, they should argue that with respect to children like Bobby, whose parents have Alexa-enabled devices in their own homes, they do have verifiable parental consent to record the children's voices. After all, Bobby's parents consented when they set up their Alexa-enabled device and agreed to its Terms of Service. Second, they should argue that with respect to children like Amber, they did not have actual knowledge that such children's voices were likely to be recorded by the Alexa-enabled device. After all, the widespread use of Zoom due to the COVID-19 pandemic was unprecedented and unpredicted. I think it remains possible that parents of children like Amber might have a case against Amazon that makes use of COPPA, but I think it would be a difficult one.

In this case, it does not seem like Bobby's parents are in violation of COPPA. Though they presumably have actual knowledge that the voices of Bobby's classmates may be picked up by their Alexa-enabled device, they presumably do not count as a web site or online service directed to children (Mcgeveran 2016, 305), and so COPPA does not apply to them.

4.3 Privacy Torts

In this section, I will consider whether Zoom participants being recorded by Alexa-enabled devices without their consent might appeal to any privacy torts to make their cases. There are currently four legally recognized privacy torts: intrusion upon seclusion, public disclosure of a private fact, appropriation, and false light. These torts were catalogued by torts scholar William Prosser in the mid-twentieth century, both in a law review article he published as well as in the second *Restatement of Torts* (Mcgeveran 2016, 99).

4.3a Intrusion Upon Seclusion

Intrusion upon seclusion has two elements: (1) the person must have intruded upon the solitude or seclusion of another, and (2) the intrusion in (1) must be highly offensive to a reasonable person

(Mcgeveran 2016, 100). Because the recorded Zoom participants have consented to participating in a Zoom conversation, meeting, or class, the case we are considering does not seem to fall under seclusion. Things would be different if someone were to, say, set up an Alexa-enabled device in the home or private space of someone else.

4.3b Public Disclosure of Private Facts

The second privacy tort is public disclosure of a private fact, and it has four elements: (1) the fact must be made public, (2) the content of the fact must be a private matter, (3) the publicity of that private fact must be highly offensive to the reasonable person, and (4) the fact that is publicly disclosed must not be newsworthy (Mcgeveran 2016, 112). For the first element, there are (at least) two ways to interpret what counts as publicizing the fact, one corresponding to the majority opinion and the other to the minority opinions in *Bodah v. Lakeville Motor Express* (Minn. 2003). The majority rule is that in order for a fact to count as being made public it must have been distributed widely or highly likely to be. According to the minority rule, the publicity element would be fulfilled simply by the fact that being disclosed to a specific audience, if the disclosure to that audience is likely to bring embarrassment to the subject of the fact.[8] Even in states that apply the more expansive minority rule, this privacy tort will not apply to the case at hand unless Amazon discloses information about the person who was recorded without her consent and the sharing of that information with that audience was highly offensive. It would not be enough that Amazon had the recordings and was storing them: they would have to disclose them to a sufficiently public audience.

In at least one case, an Alexa-enabled device is known to have recorded a sexual assault, and that recording was shared with many Amazon employees (Kuruvilla 2019, 2035). There is a possibility of a public disclosure of a private fact tort case here, since what was shared was highly offensive, if the audience of Amazon employees is taken to be public enough to fulfill element 1 (and perhaps it would be, if we take the minority view, due to the very highly sensitive nature of the material recorded). But most of the Alexa-enabled device recording that happened via Zoom during the pandemic (and afterward) will not fulfill the elements of this privacy tort because they will not be disclosed to the public and are unlikely to have been of facts the disclosure of which would count as highly offensive to the reasonable person.

4.3c Appropriation

The third privacy tort is appropriation of one's name or likeness. An Alexa-enabled device simply recording a Zoom conversation or meeting is very unlikely to be covered unless we alter or enhance the facts significantly, such as Amazon using the recording itself in an advertisement.

4.3d False Light

The fourth and final privacy tort is false light. Again, this tort is not applicable to the case under consideration. Amazon simply recording and even reviewing those recordings does not amount to what would be required for false light to be relevant. Rather false light requires giving publicity to incorrect information about another person that is either (1) highly offensive to the reasonable person or (2) publicized with reckless disregard (Mcgeveran 2016, 141).

4.4 Two-Party Consent Recording Statute: California Focus

So far, we have seen that not much is available in the way of legal recourse for someone who is recorded by an Alexa-enabled device over Zoom without her consent. However, some individual states within the U.S. have stricter statutes often called "two-party consent" laws that govern recording and require that all parties to the recording consent to being recording. Here I will consider one example of such a statute, namely California Penal Code §632.[9]

§632 prohibits the recording of a confidential communication "intentionally and without the consent of all parties" via "telegraph, telephone, or other device, except a radio" and makes such recording punishable by a fine no greater than $2,500 per violation and no greater than $10,000 if they have previously been convicted under this statute (§632(a)). It seems to apply to this case, as one of the parties to the communication has (by assumption) not consented to Amazon's recording of them nor to the Alexa-enabled device owner's recording of them. One complication is whether or not a Zoom conversation would count as a "confidential communication." §632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes… any… circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded" (§632(c)).

How should we understand what is meant by "may reasonably expect that the communication may be overheard or recorded"? If the California state courts understand this language along similar lines to the way federal courts have understood "reasonable expectation of privacy," it will face serious normative concerns. I do not have space here to explain in detail all of these concerns, but it will help to have a few on the table in order to think about how §632 does and does not apply to the case under consideration.[10] The main problems stem from the fact that "expectation" has both predictive and normative senses. This ambiguity can make it difficult to determine when someone has a "reasonable expectation of privacy". If I expect that my conversation is private in the predictive sense, I predict (based on my evidence) that it is likely to be private. Or more strongly, I believe that it is private. If I expect that my conversation is private in the normative sense, I believe that I am entitled to its being private. These two different ways of understanding what is meant by "expectation" can generate different results in many cases. Further, understanding "reasonable expectation of privacy" in the predictive way is particularly problematic because of the way it easily allows for what we might call "intrusion-creep." As new technology becomes better and better at invading privacy, it becomes less and less reasonable (based on one's evidence) to expect (in a predictive way) that one's conversations remain private.

Nevertheless, the statute defines "confidential communication" so as to exclude those conversations in which the "parties to the conversation may reasonably expect that the communication may be overheard or recorded" (§632(c)). So, in order to determine whether the case of Alexa recording a nonconsenting party via Zoom counts as a confidential communication or not, we need to know whether the nonconsenting party has a reasonable expectation that the communication may be overheard or recorded. Suppose that the nonconsenting party *does* know that the Zoom call itself is being recorded. That is, they have been informed

[8] The minority rule is more in line with Nissenbaum's influential view of privacy (2004).

[9] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=632

[10] See Selbst (2013) for compelling criticisms of the "reasonable expectation of privacy" test, among others.

that the Zoom meeting is being recorded and even consented (via clicking on a pop-up window) to its recording. Though it is their expectation that the recording will only be made available to the meeting participants or to the relevant parties (e.g. students who have missed class that day), they nevertheless consented to the recording. They haven't consented to *Amazon's* recording them, but it is pretty clear that doesn't matter according to the text of the statute. Because they have consented to the Zoom meeting's being recorded *at all*, they seem to have a reasonable expectation that the conversation may be recorded. This means that even a 2-party consent statute, which seemed most promising at the outset and even one which only requires recording and not disclosure ends up not really offering recourse to the frustrated unconsenting person who has been recorded via another Zoom participant's Alexa-enabled device.

Why might the statute only require that the parties reasonably expect that the communication be recorded rather than that they expect (or consent to) it's *being recorded?* That is, why is consenting to Zoom's recording enough to allow Amazon to be "off-the-hook" for its own recording?

To answer this, we have to think a bit about the judicial history of privacy law in the United States. §632 seems to be operating within the so-called "secrecy paradigm," according to which privacy is understood as governing information users have kept private (or "secret") but no longer governing information once it has been revealed or shared with anyone (once it is no longer "secret").[11]

According to the secrecy paradigm, Amazon would not need *direct* consent for recording the conversation so long as other parties have already been given consent to record (in this case, Zoom) because this conversation is no longer private (in the sense of privacy recognized by the secrecy paradigm). Of course, this understanding of privacy is not the only one available (and, in my view, it is not a very compelling understanding of privacy). But it does seem to be the conception of privacy that is operating in §632 and is thus relevant to our analysis of any currently-available legal recourse for an Alexa-enabled device's recording of someone via Zoom.

Are things different if not all parties to the Zoom conversation consent to the Zoom recording in the first place? Some Zoom meetings are not recorded, so there will be cases in which at least some of the participants have not consented to the recording. In such cases, it is much less obvious that "parties to the conversation may reasonably expect that the communication may be overheard or recorded" (§632(c)). Amazon might try to avail itself of the secrecy paradigm again, arguing that parties *should* reasonably expect to be overheard (perhaps by family members or roommates of those with whom they are on Zoom) and so their conversation does not meet the statute's definition of "confidential information".

5. What Should be Next?

Even under a 2-party consent statute such as §632 in California, then, there isn't much recourse available to the person who is recorded without their consent (and perhaps even without their knowledge) by an Alexa-enabled device via a Zoom conversation they have with someone who has such a device in their home. What would need to change if we were worried about this kind of invasion of our privacy and wanted to ensure that legal action were available in this arena?

I think (at least) two major policy changes are required. First, we would need more widespread use of 2-party consent, whether by more states adopting such legislation or by enacting a federal law. Second, such legislation (whether state or federal) would need to move away from the problematic concepts of (1) reasonable expectation of privacy and (2) the secrecy paradigm. Instead, such legislation should be based on a more defensible set of normative concepts, such as "actual and explicit consent".

We have already seen the difference that moving toward more widespread 2-party consent laws would make, in my analysis above of California. But we also saw that that change on its own was not enough, since even in the 2-party consent regime of California's §632, very little (if any) legal recourse was available. So, this is the reason for the necessity of policy change (2). What is meant by "actual and explicit consent"? As it stands, §632 does not offer recourse against Amazon in many cases because people may have consented to their conversation's being recorded, perhaps believing that such recording was to be used only for limited purposes, such as being viewed by other classmates. Though they gave consent to the recording itself, they may not have known that Amazon would have any recording of their conversation and thus did not explicitly consent to *Amazon's* recording of it. A principle of "actual and explicit consent" would require that any party doing the recording obtain consent from all parties being recorded *to that particular party's* recording of them. This would protect against Amazon's recording conversations of those who do not have Alexa-enabled devices in their own homes and are inadvertently recorded via Zoom. Of course, such regulation would be hard to enforce since people would still somehow need to know that Amazon had recorded them without consent in order to bring legal action. But it would at least indicate a commitment to privacy on the part of our community. And it wouldn't leave those who find out that Amazon has a recording of them without legal recourse.

6. Conclusion

The practically ubiquitous use of Zoom during the COVID-19 pandemic and increased use of it post-pandemic has been good in some significant ways: it allowed for the continuation of many kinds of work that would otherwise have been impossible while maintaining safe physical distance from one another, from business meetings to educational classes. It has improved access to classes and conferences (among other things) to those who cannot attend such classes and conferences physically in person, for a variety of reasons. But because so many people are working from home and communicating online, we have invaded one another's homes in unprecedented ways. And because the transition to Zoom happened rapidly due to a global pandemic and under emergency circumstances, not as much attention was paid to the risks and problems that such widespread use of Zoom raises. This includes subjecting ourselves to recording devices that others may have in their homes, including Alexa-enabled devices that record small bits of conversation and send those recordings to Amazon for latter review and storage. These devices raise special privacy concerns in part due to their "always listening" capacity and in part due to the recordings they make and the way that Amazon chooses to handle those recordings.

In this paper, I have argued that current U.S. legal regimes offer very little recourse to protect citizens who might be interested in not having Amazon have access to recordings of their conversations, for whatever reason. One reply to this worry might be just not to participate in Zoom conversations with anyone owning an Alexa-enabled device (and not to visit their house, either). However,

[11]For a helpful discussion of the secrecy paradigm and (some of) the problems it faces, see Skinner-Thomas (2020, Chapter 1).

restricting oneself in this way is eminently impractical for many, including students who are enrolled in classes with others and have little to no control over who else is enrolled in those classes. Privacy matters, and we need to find ways to protect it when possible, including against new recording technologies.

Acknowledgements

I am grateful for help and critical comments from Michael Barnes, David Gray Grant, and Andrew Selbst. Previous versions of this paper were presented at the Midwest Early-Career Social Philosophy of Technology Workshop at the University of Notre Dame and the 2025 Annual Meeting of the Philosophy, Politics, and Economics Society (PPE), and I am grateful to the audiences at both of those events for stimulating discussion and thoughtful questions. The ideas in this paper were largely developed for a course at the law school at the University of California, Los Angeles (UCLA), and I am grateful to everyone in the Law and Philosophy program at UCLA for stimulating discussions over the years. Publishing this paper open access was made possible by funding through the Open Access Publishing Fund administered through the University of Arkansas Libraries.

Reference

Cohen, J.E. 2012, *Configuring the networked self: law, code, and the play of everyday practice*, Yale University Press, New Haven, CT.

Dubois, D., Kolcun, R., Mandalari, A., Paracha, M., Choffnes, D. and Haddadi, H. 2020, 'When speakers are all ears: characterizing misactivations of IoT smart speakers', *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 4, pp. 255–276, doi:10.2478/popets-2020-0072.

Feinberg, J. 1980, 'The child's right to an open future', in W. Aiken and H. LaFollette (eds), *Whose child? Children's rights, parental authority, and state power*, Rowman and Littlefield, Totowa, NJ.

Kuruvilla, R. 2019, 'Between you, me, and Alexa: on the legality of virtual assistant devices in two-party consent states', *Washington Law Review*, vol. 94, no. 4, pp. 2029–2056, viewed 24 January 2026, https://digitalcommons.law.uw.edu/wlr/vol94/iss4/11

McGeveran, W. 2016, *Privacy and data protection law*, University Casebook Series, Foundation Press, New York.

Neville, S.J. 2020, 'Eavesmining: a critical audit of the Amazon Echo and Alexa conditions of use', *Surveillance & Society*, vol. 18, no. 3, pp. 343–356, doi:10.24908/ss.v18i3.13426.

Nissenbaum, H. 2004, 'Privacy as contextual integrity', *Washington Law Review*, vol. 79, no. 1, pp. 119–157, viewed 24 January 2026, https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Rascoe, A. 2025, 'Amazon smart speakers disable a privacy setting that allowed local storage of voice recordings', *NPR*, 23 March, viewed 24 January 2026, https://www.npr.org/2025/03/23/nx-s1-5333729/amazon-smart-speakers-disable-a-privacy-setting-that-allowed-local-storage-of-voice-recordings

Selbst, A.D. 2013, 'Contextual expectations of privacy', *Cardozo Law Review*, vol. 35, no. 2, pp. 643–709, doi:10.2139/ssrn.2093594.

Shaban, H. 2018, 'An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says', *Washington Post*, 24 May, viewed 24 January 2026, 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/

Skinner-Thompson, S. 2020, *Privacy at the margins*, Cambridge University Press, Cambridge, doi:10.1017/9781316850350.

Thomson, J.J. 1975, 'The right to privacy', *Philosophy & Public Affairs*, vol. 4, no. 4, pp. 295–314, viewed 24 January 2026, http://www.jstor.org/stable/2265075

Thorne, J. 2019, 'Does Alexa illegally record children? Amazon sued for allegedly storing conversations without consent', *GeekWire*, 12 June, viewed 24 January 2026, https://www.geekwire.com/2019/alexa-illegally-record-children-amazon-sued-allegedly-storing-conversations-without-consent/