CONVENIENCE OR CONFIDENTIALITY: NEVADA'S DIGITAL DATA LAWS IN THE AGE OF ALWAYS-LISTENING DEVICES

*E. Sebastian Cate-Cribari**

TABLE OF CONTENTS

INTRODUCTION

To examine always-listening device issues and their impact on Nevada, this Note will proceed in five parts. Part I will discuss the general technological and legal background of always-listening devices—how they came to be and how

* Juris Doctor Candidate, May 2021, William S. Boyd School of Law, University of Nevada, Las Vegas. Thank you to my soon wife, Kira, for inspiring this Note and supporting me always; to my mother, Jill, for my love of writing; and to Volume 21 of the Nevada Law Journal for all the hard work dedicated to this Note.

courts have handled them so far. Part II will address possible evidentiary issues with always-listening device transcripts and audio recordings—how they are currently treated as evidence and how courts should treat them as evidence. Part III will parse through the Constitutional issues consistently connected with using recordings and transcripts from always-listening devices as evidence. Part IV will then cover how new laws concerning always-listening devices could impact criminal trials and deter domestic violence. Finally, Part V will present recommendations for specific legislation for Nevada to adopt.

I. HISTORICAL CONTEXT FOR MODERN ISSUES

A. Development of Always-Listening Devices

The past half-decade introduced a new presence into many American households. In 2019, sixty-six million American adults owned a smart speaker ("always-listening device"), which was up nearly 40 percent from ownership in 2018.[1] According to Forbes.com, 42 percent of always-listening device owners believe their devices are essential to their everyday lives.[2] These numbers indicate a growing trend in the American household that is not likely to falter anytime soon. As tech giants like Amazon, Google, and Apple develop always-listening devices, the devices become cheaper to produce and more equipped to solve users' problems. As the devices become cheaper and more convenient, users are more incentivized to purchase them. With this pairing of development and demand, it may not be long until always-listening devices find themselves in more American households than not.[3]

While always-listening devices themselves are rapidly growing in popularity, the convenient services provided for the devices' users stem from the software behind the speakers. Smart assistants, like Amazon's Alexa, Apple's Siri, and Google's Google Assistant, interact with users through the always-listening devices and can access online data for the users with the ease and speed of a person-to-person conversation.[4] Whether a user needs to set an alarm, look up

---

[1] Bret Kinsella, *U.S. Smart Speaker Ownership Rises 40% in 2018 to 66.4 Million and Amazon Echo Maintains Market Share Lead Says New Report from Voicebot*, VOICEBOT.AI (Mar. 7, 2019, 8:00 AM), https://voicebot.ai/2019/03/07/u-s-smart-speaker-ownership-rises-40-in-2018-to-66-4-million-and-amazon-echo-maintains-market-share-lead-says-new-report-from-voicebot [https://perma.cc/L438-HV9H].

[2] Rebecca Lerner, *Smart Speakers Are the Future of Audio*, FORBES (June 23, 2017, 12:49 PM), https://www.forbes.com/sites/rebeccalerner/2017/06/23/smart-speakers-are-the-future-of-audio/ [https://perma.cc/Y4NR-3N7C].

[3] *See* LOUP VENTURES, SMART SPEAKER HOUSEHOLD PENETRATION RATE IN THE UNITED STATES FROM 2014 TO 2025, STATISTA (2020), https://www.statista.com/statistics/1022847/united-states-smart-speaker-household-penetration [https://perma.cc/8ZG4-PTNN] (projecting always-listening devices will penetrate 50 percent of American households by 2021 and 75 percent by 2025).

[4] *See, e.g.*, *All Things Alexa: Alexa Features*, AMAZON, https://www.amazon.com/b/ref=aeg_l

the weather, or listen to their horoscope, smart assistants are able to dig through the internet and return the requested information in a matter of seconds.[5]

Smart assistants are not just search engines for always-listening devices. True, Apple was the first company to bring smart assistants to mainstream consumers when Siri was released on the iPhone 4s in 2011.[6] However, Apple did not create Siri. Siri was originally an artificial intelligence program created for the Defense Advanced Research Projects Agency by SRI International.[7] In 2010, SRI published the original Siri personal assistant app and within two months Steve Jobs began the process of purchasing Siri.[8]

Siri was originally only accessible to users utilizing the Siri function on their iPhones.[9] However, Apple introduced a new function in 2014 allowing users to access Siri by saying "Hey Siri."[10] That same year, Amazon entered the smart assistant market with their own program called Amazon Alexa.[11] Alexa differed from Siri in that Alexa was not restricted to a smart phone. Instead, Alexa was primarily accessible through Amazon's Echo, a small smart speaker to be placed in rooms within users' homes and connected to their home wifi.[12] Amazon's co-introduction of Alexa and Echo marked the age of smart assistants merging with always-listening devices.

Amazon's Alexa also marked a distinct shift in the direction of smart assistants because it separated the smart assistant from the smart phone. Where Siri was a feature that essentially extended the search functions already offered on

---

p_features/ref=s9_acss_bw_cg_aeglp_md1_w?node=17934672011&pf_rd_m [https://perma.cc/CU69-CY5F]; *Siri Does More Than Ever. Even Before You Ask.*, APPLE, https://www.apple.com/siri [https://perma.cc/DJ3B-DNR4]; *How Can We Help You? What You Can Ask Your Google Assistant*, GOOGLE, https://support.google.com/assistant/?hl=en#topic=7658431 [https://perma.cc/PJ54-BW4].

[5] *See* Ali Montag, *Here's What People Actually Use Their Amazon Echo and Other Smart Speakers for*, CNBC (Sept. 10, 2018, 1:19 PM), https://www.cnbc.com/2018/09/10/adobe-analytics-what-people-use-amazon-echo-and-smart-speakers-for.html [https://perma.cc/7NDG-8NSL].

[6] Press Release, Apple, Apple Launches iPhone 4s, iOS 5 & iCloud (Oct. 4, 2011), https://www.apple.com/newsroom/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud [https://perma.cc/4HZG-9K69].

[7] Bianca Bosker, *Siri Rising: The Inside Story of Siri's Origins – and Why She Could Overshadow the iPhone*, HUFFPOST (Dec. 6, 2017), https://www.huffpost.com/entry/siri-do-engine-apple-iphone_n_2499165 [https://perma.cc/X257-G83D].

[8] *Id.*

[9] Parmy Olson, *Steve Jobs Leaves a Legacy in A.I. with Siri*, FORBES (Oct. 6, 2011, 12:24 PM), https://www.forbes.com/sites/parmyolson/2011/10/06/steve-jobs-leaves-a-legacy-in-a-i-with-siri [https://perma.cc/G6QD-KXZ2].

[10] Jason Cipriani, *What You Need to Know About 'Hey, Siri' in iOS 8*, CNET (Sept. 18, 2014, 12:00 PM), https://www.cnet.com/how-to/what-you-need-to-know-about-hey-siri-in-ios-8 [https://perma.cc/ET25-MGW9].

[11] Darrell Etherington, *Amazon Echo Is a $199 Connected Speaker Packing an Always-On Siri-Style Assistant*, TECHCRUNCH (Nov. 6, 2014, 9:14 AM), https://techcrunch.com/2014/11/06/amazon-echo [https://perma.cc/8QLK-YVPD].

[12] *Id.*

internet-connected mobile smartphones, Alexa operated through home-bound always-listening devices.[13] Additionally, while Siri was fully functional without activating the "Hey Siri" function that turned a user's phone into an always-listening device, Alexa had no such setting.[14] Alexa appears to have started as, and largely remained, a smart assistant intended to operate through always-listening devices.[15]

While this might have merely been a philosophical difference between Apple and Amazon at first, the development of the technology has revealed that always-listening devices are the future of smart assistants. In 2016, Google joined the always-listening device market by releasing Google Assistant, Google's own smart assistant accessible through its own always-listening device, Google Home.[16] Google Home is a device that, both in appearance and use, mirrored Amazon's Echo.[17]

Google has since extended the Google Assistant program to their smart phones and certain Android devices, but it primarily exists as a part of Google Home and Google's new "smart display" devices.[18] In response, Amazon also extended the Alexa program by creating the Amazon Alexa App for smartphones.[19] Yet, Apple has also followed Amazon's path with the release of the HomePod,[20] an always-listening device which integrates Siri into users' smart homes.

While smart assistants may have begun as a smart phone app, always-listening devices may serve as the primary utilization of the technology.[21] With that transition looming, users who decide to purchase and activate an always-listening device must consider what this new presence will change about their privacy within their homes.

---

[13] *Id*.

[14] *Id*.

[15] Jared Newman, *For Amazon, the Future of Alexa Is About the End of the Smartphone Era*, FAST CO. (Nov. 8, 2017), https://www.fastcompany.com/40479207/for-amazon-the-future-of-alexa-is-about-the-end-of-the-smartphone-era [https://perma.cc/HXB3-KV3J].

[16] Steve Kovach, *Google Unveils Its Newest Major Product: The Google Home Speaker*, BUS. INSIDER (Oct. 4, 2016, 9:58 AM), https://www.businessinsider.com/google-home-announced-price-release-date-2016-10 [https://perma.cc/3E32-QFGD].

[17] Aaron Tilley, *Google Home vs. Amazon Echo: Everything You Need to Know*, FORBES (Oct. 4, 2016, 5:49 PM), https://www.forbes.com/sites/aarontilley/2016/10/04/google-home-vs-amazon-echo [https://perma.cc/MUZ7-FQMC].

[18] Dieter Bohn, *Google Is Introducing a New Smart Display Platform*, THE VERGE (Jan. 8, 2018, 8:00 PM), https://www.theverge.com/2018/1/8/16860142 [https://perma.cc/A9J3-HZPS].

[19] Amazon Alexa App Details and Download, AMAZON, https://www.amazon.com/Amazon-com-Amazon-Alexa/dp/B00P03D4D2 [https://perma.cc/JY4K-TYFS].

[20] *HomePod*, APPLE, https://www.apple.com/homepod [https://web.archive.org/web/20201011065142/https://www.apple.com/homepod/].

[21] Kovach, *supra* note 16.

B. Always-Listening Devices in the Law

The original legal issues Siri faced as the first-to-market smart assistant included, *inter alia*, the following: copyright, ownership of intellectual property, liability issues for reliance on Siri's mistakes.[22] However, now that smart assistants are intertwined with always-listening devices, a new set of issues must be addressed.

The biggest difference for Siri in the past decade is that a user in 2012 had to press a button to prompt Siri to begin listening, and a user in 2019 simply needs to say, "Hey Siri."[23] This change is incredibly important in the scope of legal issues because it begs the following question: how does Siri know to listen only when someone says "Hey Siri" if Siri is not already listening? More directly, are Siri/Alexa/Google devices recording all of our conversations? Apple, Amazon, and Google have all addressed this question with a concrete "no."[24] However, the companies do admit that when an always-listening device is activated, the transcript of questions and answers is stored on the respective company's cloud.[25]

Those transcripts, while private, are not exclusively accessible to the user who participated in their creation.[26] Amazon allows users to go into their account settings and manually delete audio recordings held in the Amazon cloud but otherwise retains recordings and transcribes indefinitely.[27] Even if the recordings are deleted, however, Amazon retains underlying data such as what actions were taken by Alexa in response to the question, purchase records processed through Alexa, and others.[28] Google fully discloses that it will share transcripts to "[m]eet any applicable law, regulation, legal process, or enforceable governmental request."[29]

Apple, Amazon, and Google have also come under fire because their devices listened in when they were not supposed to. For example, in 2017, a San Diego

---

[22] John Weaver, *Siri Is My Client: A First Look at Artificial Intelligence and Legal Issues*, N.H. BAR J., Winter 2012, at 6, 7–9.

[23] Cipriani, *supra* note 10.

[24] *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/CD65-22F6]; Lisa Vaas, *Siri Is Listening to You, but She's NOT Spying, Says Apple*, NAKED SEC. (Aug. 13, 2018), https://nakedsecurity.sophos.com/2018/08/13/siri-is-listening-to-you-but-shes-not-spying-says-apple [https://perma.cc/LH7L-BCX4]; *Data Security and Privacy on Devices That Work with Assistant*, GOOGLE, https://support.google.com/googlenest/answer/7072285 [https://perma.cc/MH2R-N3RH].

[25] *Alexa, Echo Devices, and Your Privacy*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V [https://perma.cc/7Z3Y-UU36].

[26] *Alexa and Alexa Device FAQs*, *supra* note 24.

[27] Charlie Osborne, *Amazon Confirms Alexa Customer Voice Recordings Are Kept Forever*, ZDNET (July 3, 2019, 2:49 AM), https://www.zdnet.com/article/amazon-confirms-alexa-customer-voice-recordings-are-kept-forever [https://perma.cc/R7VJ-7VFM].

[28] *Id.*

[29] *Privacy Policy: When You Share Your Information*, GOOGLE, https://policies.google.com/privacy?hl=en#infosharing [https://perma.cc/2JLJ-8VXT].

news anchor reporting on a child who ordered a doll house through her family's Amazon Echo stated, "I love the little girl saying, 'Alexa ordered me a dollhouse.'"[30] While the original story may have merely been a humorous misunderstanding, Amazon faced criticism when several Echo devices in San Diego homes heard the broadcast and proceeded to order dollhouses for their owners.[31] While the devices were technically activated by the trigger word "Alexa," the users did not specifically speak to the device and ask it to do anything. This misunderstanding begs a more serious question; what happens if transcripts are brought in as evidence against an always-listening device's owner in criminal court when there is a chance the defendant was not the one being recorded and transcribed?

This was an important issue for Arkansas in *State v. Bates*.[32] In late 2016, reports indicated that police in Arkansas were attempting to gain access to audio recordings from a murder suspect's Amazon Echo device.[33] The man, James Bates, hosted a viewing party for some football games, and the next morning one of his guests was found dead in Bates' backyard hot tub.[34] During their investigation, police noticed the Amazon Echo device located in Bates' kitchen and seized it.[35] They were able to gain some information from the device, but they were unable to tell if the device had recorded any audio around the time of the murder.[36] The police then obtained a search warrant for the device's cloud-based information and demanded that Amazon submit any recording information from the device, but Amazon did not fully comply.[37]

Instead of turning over all of the data, Amazon submitted only Bates' account information and purchase history.[38] Amazon then released a statement affirming: "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."[39]

---

[30] Andrew Liptak, *Amazon's Alexa Started Ordering People Dollhouses After Hearing Its Name on TV*, THE VERGE (Jan. 7, 2017, 5:52 PM), https://www.theverge.com/2017/1/7/14200210 [https://perma.cc/38BG-Y8U3].

[31] *Id.*

[32] Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant at 6–7, Arkansas v. Bates, No. CR-2016-370-2 (Cir. Ct. Ark. Feb. 17, 2017).

[33] Alina Selyukh, *As We Leave More Digital Tracks, Amazon Echo Factors in Murder Investigation*, NPR: ALL TECH CONSIDERED (Dec. 28, 2016, 3:20 PM), https://www.npr.org/sections/alltechconsidered/2016/12/28/507230487 [https://perma.cc/L242-ZZ62].

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

While Amazon's stance on the issue was never tested in that Arkansas courtroom,[40] *Bates* showed that Amazon was willing to stand by users of their always-listening device to prevent potentially errant recordings from being used against them.

This issue is not one that will just go away. With always-listening devices gaining steady popularity year after year, it is inevitable that something like the situation in Arkansas will come up again. For that reason, rather than waiting for the equally inevitable litigation to create common law based on specific circumstances, Nevada must legislate these issues.

C. Nevada's Historical Approach to Recordings

Nevada considers the unauthorized recording of a conversation a felony.[41] That means that no party may have their communications recorded and used against them in court without their consent. It may appear that this solves the issue of state prosecutors using always-listening device transcripts against their users; however, Nevadans are not saved by the lack of explicit consent to being recorded.

Nevada requires all parties to a communication consent to being recorded for the recording to be lawful.[42] This precludes the admission of telephone recordings taken without a defendant's consent against them in a criminal trial.[43] Unfortunately, that statutory protection is unlikely to prevent the admission of recordings from always-listening devices. Once activated, always-listening devices necessarily record users and transmit information over the internet.[44] This should be no secret to users who automatically consent to their recordings being used to improve their experience upon activating their always-listening device.[45] If consent to being recorded is a necessary part of the always-listening device experience, it is unlikely that a court would consider the recordings to be intercepted without consent of the user.

---

[40] "[A] circuit court judge granted [Arkansas prosecutors'] request to have the charges . . . dismissed. The prosecutors declared *nolle prosequi*, [a formal notice that there will be no further prosecution], stating that the evidence could support more than one reasonable explanation." Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence from Amazon Echo*, NPR: THE TWO-WAY (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812 [https://perma.cc/37R4-QRRR] (emphasis added).

[41] NEV. REV. STAT. §§ 200.620, 690 (2019); Ditech Fin. LLC v. Buckles, 401 P.3d 215, 217 (Nev. 2017) (quoting Lane v. Allstate Ins. Co., 969 P.2d 938, 940 (Nev. 1998)).

[42] *Ditech*, 401 P.3d at 217.

[43] McLellan v. Nevada, 182 P.3d 106, 109 (Nev. 2008).

[44] Richard Baguley & Colin McDonald, *Appliance Science: Alexa, How Does Alexa Work? The Science of the Amazon Echo*, CNET (Aug. 4, 2016, 5:00 AM), https://www.cnet.com/news/appliance-science-alexa-how-does-alexa-work-the-science-of-amazons-echo/ [https://perma.cc/H73T-LEGA].

[45] *Alexa Terms of Use*, AMAZON cl. 3.1, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 [https://perma.cc/3L3J-TEX3]. I leave the discussion of whether this should qualify as consent to another note.

With statutory protections absent, Nevadans must consider whether their use of always-listening devices could expose them to liability. Nevada's rules of evidence follow closely to the Federal Rules of Evidence. One section that is nearly identical is Nevada's section regarding treatment of records of regularly conducted activity.

A record made during the regular course of activity is an evidentiary exception presented in the federal system and in Nevada.[46] Under Nevada Revised Statute section 51.135, any record or compilation of data from information transmitted by a person with knowledge—during the course of a regularly conducted activity—may be admitted as evidence in both civil and criminal trials.[47] Under a general reading of the law, recordings made by always-listening devices seem to fall under this exception. An always-listening device records (*creates a record of*) sounds and words (*information transmitted*) of users who utter the device's trigger word (*by persons with knowledge*) every time it is triggered (*during regularly conducted activity*).[48]

Records of a regularly conducted activity may very well apply to recordings of purposefully directed questions. However, this should not be concerning for the vast majority of individuals who mainly use their device for weather updates and background music. What users should fear for is whether the exception allows the admissibility of recordings transcribed mistakenly.

This fear of mistakenly transcribed recordings is best explained through a hypothetical similar to the San Diego incident mentioned above. One hypothetical user, Alex, owns an Amazon Echo device that is set to always listen for its trigger word, "Alexa." One night, Alex has several friends over to play the video game Assassin's Creed.[49] At some point during the night, a friend needing advice for Assassin's Creed asks "Alex, how do you hide a body?"[50] Alex's Alexa is mistakenly triggered by the word "Alex," transcribes the request, and searches the internet for "how to hide a body." Several months later, Alex is falsely accused of murder and that same Alexa transcript is recovered by the prosecution. Through the regularly conducted activity exception to hearsay, the prosecution may successfully admit both "Alex's" question and Alexa's answer into evidence.[51]

Some may see this hypothetical as an example of a transcript being created outside of regularly conducted business and determine that a system to properly categorize purposeful statements from accidental statements must be established for this technology to be acceptable in court at all. After all, the recording and

---

[46] NEV. REV. STAT. § 51.135 (2019); FED. R. EVID. 803(6).

[47] NEV. REV. STAT. § 51.135 (2019).

[48] *See id*.; Baguley & McDonald, *supra* note 44.

[49] *See* Jack Fennimore, *Assassin's Creed Origins: 10 Tips & Tricks for Stealth*, HEAVY (Oct. 27, 2017, 4:29 AM), https://heavy.com/games/2017/10/assassins-creed-origins-tips-tricks-stealth [https://perma.cc/E698-NKWU].

[50] *See id*. (including the skill of hiding dead bodies among tips to play Assassin's Creed).

[51] *See* NEV. REV. STAT. § 51.135 (2019).

transcribing of a user's words outside of directly prompted requests is not the regular activity of these companies.[52] However, solving just this issue is not likely to prohibit the use of these transcripts in court. While the hypothetical lists "regularly conducted activity" as the method of admission, transcripts are not restricted to a single avenue of admissibility. For instance, the hypothetical prosecution could have also prevailed by asserting the party opponent exception to hearsay.[53]

The issue at hand, especially here in Nevada and in states with similar laws, is that no single exception to hearsay prevents potentially fraudulent transcripts into evidence. So, these states must address what can be done once the transcripts are inevitably considered admissible under multiple exceptions to the hearsay rule of evidence. To that point, courts outside of Nevada have not been able to reach a clear conclusion. For instance, in the *Bates* case discussed above,[54] Arkansas faced the challenge of determining what information the government should be able to glean from always-listening devices without the guidance of legislation.[55]

In *Bates*, the Arkansas court issued a search warrant requiring Amazon to turn over voice recordings associated with the transcript that had been previously subpoenaed.[56] While the original transcript included plenty of information, the prosecution needed the audio recordings to confirm Bates was the one who issued the questions.[57] Amazon issued a lengthy motion in support of their users' First Amendment rights to browse the internet anonymously.[58] However, before the court could issue a ruling on the matter, the defendant consented to the release of his audio recordings.[59]

This Note argues that Nevada should not wait to face the same situation Arkansas faced in 2017. Instead of waiting for issues to arise in court to determine the accessibility of these recordings to law enforcement and litigating parties, Nevada's legislature should amend statutes currently in place to include recordings from always-listening devices as information that may be requested by

---

[52] *See supra* note 24.

[53] A party's own statement is not hearsay when it is offered into evidence against the party. NEV. REV. STAT. § 51.035(3)(a); FED. R. EVID. 801(d)(2)(a).

[54] *See supra* Section I.B.

[55] Brian Heater, *After Pushing Back, Amazon Hands over Echo Data in Arkansas Murder Case*, TECHCRUNCH (Mar. 7, 2017, 6:26 AM), https://techcrunch.com/2017/03/07/amazon-echo-murder [https://perma.cc/9CUP-HABF].

[56] Brian Heater, *Amazon Cites First Amendment Protection for Alexa in Arkansas Murder Case*, TECHCRUNCH (Feb. 23, 2017, 8:45 AM), https://techcrunch.com/2017/02/23/alexa-free-speech [https://perma.cc/MSE7-PTGN].

[57] *See* Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant, *supra* note 32, at 37.

[58] Thomas Brewster, *Amazon Argues Alexa Speech Protected by First Amendment in Murder Trial Fight*, FORBES (Feb. 23, 2017, 7:10 AM), https://www.forbes.com/sites/thomasbrewster/2017/02/23/amazon-echo-alexa-murder-trial-first-amendment-rights [https://perma.cc/BT8X-K94U].

[59] Heater, *supra* note 55.

warrant and admitted as evidence by default. To understand why the legislature would do this, the rules of evidence affecting always-listening device recordings must also be understood.

II. PROSECUTION MOVES ALWAYS-LISTENING DEVICES INTO EVIDENCE

A. Transcripts and Recordings Under Nevada's Hearsay Laws

Hearsay is an out of court statement offered into evidence to prove the truth of the matter asserted.[60] This rule is in place almost identically across all jurisdictions in the United States.[61] Hearsay is dangerous in the courtroom because it carries several difficulties including trustworthiness, authentication, and reliability.[62] However, when an out of court statement is surrounded by elements quelling those difficulties, the legal system is much more inclined to accept them. Hence, there are several established exceptions to hearsay codified into the Nevada Revised Statutes and the Federal Rules of Evidence.[63]

The hearsay exception most applicable to audio recordings processed through always-listening devices is likely the record of regularly conducted activity exception.[64] This exception is often referred to as the business record exception and is used to admit business documents.[65] It would stand to reason that always-listening devices, which are certainly products within the overall business of their companies, would fall under this exception completely. However, the exception might not necessarily cover the audio recordings from an always-listening device.

On the one hand, according to Amazon, always-listening device recordings are not sold or actively traded.[66] Nor are the audio recordings specifically used in the smart assistant's search function.[67] Instead, the recordings are transcribed, and that transcript is fed into the search algorithm for business use.[68]

---

[60] NEV. REV. STAT. § 51.035 (2019); FED. R. EVID. 801(c).

[61] Stephen A. Saltzburg, *Rethinking the Rationale(s) for Hearsay Exceptions*, 84 FORDHAM L. REV. 1485, 1485 (2016); *see, e.g.*, COLO. R. EVID. 801(c); N.M. R. EVID. 11-801(C); IDAHO R. EVID. 801(c).

[62] *See* Carl C. Wheaton, *What Is Hearsay?*, 46 IOWA L. REV. 210, 219–20 (1961).

[63] NEV. REV. STAT. §§ 51.075–51.385 (2019). The Federal Rules of Evidence even provide a catch all rule which makes admissible any statement supported by "sufficient guarantees of trustworthiness" which is "more probative on the point for which it is offered" than any other reasonably obtainable evidence. FED. R. EVID. 807.

[64] NEV. REV. STAT. § 51.135 (2019).

[65] "The basis for the business record exception is that accuracy is assured because the maker of the record relies on the record in the ordinary course of business activities." A.L.M.N., Inc. v. Rosoff, 757 P.2d 1319, 1326 (Nev. 1988) (quoting Clark v. City of Los Angeles, 650 F.2d 1033, 1037 (9th Cir. 1981)).

[66] *Alexa, Echo Devices, and Your Privacy*, *supra* note 25.

[67] *Id.*

[68] *Id.*

On the other hand, the recordings are created in the process of transcribing, which is a regularly conducted business activity.[69] This may give the documents the indicia of reliability that the regularly conducted business activity exception relies on.[70] However, without firmly meeting the requirements of the regularly conducted business activity exception, the recordings must bypass Confrontation Clause issues to be admissible.[71]

The Sixth Amendment's Confrontation Clause vests criminal defendants with the right to confront witnesses testifying against him or her.[72] As the U.S. Supreme Court held in *Idaho v. Wright*, "[t]o be admissible under the Confrontation Clause, hearsay evidence used to convict a defendant must possess indicia of reliability by virtue of its inherent trustworthiness."[73] To meet this requirement, the recordings "must be at least as reliable as evidence admitted under a firmly rooted hearsay exception" to the point that "adversarial testing would add little to its reliability."[74]

Audio recordings from always-listening devices should not have to pass through these failsafe hearsay requirements to be admitted into evidence. Where written documents may present questions of reliability and trustworthiness, audio recordings may overcome such issues uncomplicatedly.. For instance, a transcript could be written by or transcribed from anyone, with very little way to guarantee that the document did or did not come from any specific person. With audio recordings, however, voices can be compared and authenticated on a case by case basis. In fact, the Nevada Revised Statutes already provide that voices heard through electronic recordings may be sufficiently identified by opinion if there is sufficient connection between the recording and the alleged speaker.[75] Thus, Nevada should adopt a uniform hearsay exception for audio recordings created by always-listening devices to avoid unnecessary litigation over the applicability of less exact exceptions that often result in admission of the recording nevertheless.

B. Transcripts and Recordings Under Nevada's Authentication Laws

One issue the legislature must consider is authentication of the recordings themselves. While an electronically recorded voice may be authenticated by opinion,[76] parties may have extensive pre-trial arguments as to whether the

---

[69] *Id.*

[70] *See Rosoff*, 757 P.2d at 1326.

[71] Idaho v. Wright, 497 U.S. 805, 818 (1990) (first citing Lee v. Illinois, 476 U.S. 530, 543 (1986), then citing Ohio v. Roberts, 448 U.S. 56, 66 (1980)).

[72] "In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . ." U.S. CONST. amend. VI.

[73] *Wright*, 497 U.S. at 822.

[74] *Id.* at 821.

[75] NEV. REV. STAT. § 52.065 (2019).

[76] *Id.*

recording may be presented in court at all.[77] While there are arguments to be made that the recording is self-authenticating or not, a solution to this inevitable dispute may already exist within the Federal Rules of Evidence.[78]

Federal Rule of Evidence 902(13)—Certified Records Generated by an Electronic Process or System—states, "[a] record generated by an electronic process or system that produces an accurate result" is self-authenticating so long as a qualified person can certify the process or system.[79] This categorization of self-authenticating evidence is exactly the type of solution the Nevada legislature should embrace ahead of any serious disputes about the authenticity of recordings from always-listening devices. By amending Nevada Revised Statute section 52 and adding a section to the presumptions of authenticity covering electronic processes and systems, any conflict surrounding the authenticity of recordings can be handled without excessive litigation.

C. Transcripts Irrelevant When Recordings Available

With questions of authentication out of the way, there is a question to the relevance of the recordings. Any evidence that is brought into a Nevada court must be relevant.[80] Nevada has defined relevant evidence to be "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence."[81] Whether audio recordings are relevant is a case-by-case determination, but one question must be answered to rationalize legislation creating a specific rule for always-listening devices' audio recordings: whether the use of audio recordings is any more relevant than the use of transcripts that are likely to already be admissible under the current rules of evidence?

The benefits of hearing these recordings are significant. Not only could the audio recordings dispel any questions about who activated the device, but they could also give key context of the tone, pace, and surrounding environment of the speaker when the question was asked. The trier of fact can use this information to determine how much weight to give the evidence. When reading a transcript is the only option, all that context is lost. Words on a page have only the context that is awarded to them by the parties in court.[82] While this Note does

---

[77] *E.g.*, White v. Texas, 549 S.W.3d 146, 149–50 (Tex. Crim. App. 2018) (noting the admissibility of an audio recording was the subject of pre-trial motions and argument).

[78] *See* FED. R. EVID. 902(13).

[79] *Id.*

[80] NEV. REV. STAT. § 48.025 (2019).

[81] *Id.* § 48.015.

[82] Norman N. Markel et al., *The Relationship Between Words and Tone-of-Voice*, 16 LANGUAGE & SPEECH 15, 15 (1973).

not advocate for the removal of advocacy opportunities, the best evidence rule implies that the recordings should be utilized if possible.[83]

The best evidence rule requires that the original document be produced in court when the content of that document is at issue.[84] Nevadan litigators face essentially identical versions of the best evidence rule in state and federal court.[85] Indeed, Nevada Revised Statute section 52.235 and Federal Rule of Evidence 1002 both specifically require that the original writing, recording, or photograph is to prove the content of the writing, recording, or photograph.[86] Similarly, both rules of evidence allow for the admission of copies if the original cannot "be obtained by any available judicial process."[87]

In the past, Nevada courts have referenced the best evidence rule, but only to hold that an exception applied.[88] For example, in *Young v. Nevada Title Co.*, the Nevada Supreme Court held that the best evidence rule did not bar copies of written work unless the writing is specifically offered into evidence to prove the terms of the writing.[89] Additionally, in *Tomlinson v. Nevada*, the Nevada Supreme Court held that the best evidence rule does not bar transcripts of audio recordings to be admitted when the audio recording is no longer available.[90] For examples of the best evidence rule mandating an original copy, one must look to opinions from the Ninth Circuit.[91]

In *United States v. Workinger*, the Ninth Circuit court considered whether the best evidence rule had been violated when a transcript of an audio recording was admitted at trial.[92] The court ultimately held that the transcript of an audio recording of defendant's interview with his wife's attorney was admissible because the audio recordings had been deleted in the ordinary course of business.[93] However, the court noted that "the tape . . . was the best evidence of its own

---

[83] Young v. Nevada Title Co., 744 P.2d 902, 904 (1987) ("[I]n proving the terms of a writing, where the terms are material, the original writing must be produced unless it is shown to be unavailable for some reason other than the serious fault of the proponent." (alteration in original) (emphasis omitted) (quoting EDWARD W. CLEARY, MCCORMICK ON EVIDENCE 230 (2d ed. 1972))).

[84] *Id.*

[85] *Compare* NEV. REV. STAT. § 52.235 (2019) ("To prove the content of a writing, recording or photograph, the original writing, recording or photograph is required, except as otherwise provided in this title."), *with* FED. R. EVID. 1002 ("An original writing, recording, or photograph is required in order to prove its content . . . .").

[86] NEV. REV. STAT. § 52.235 (2019); FED. R. EVID. 1002.

[87] NEV. REV. STAT. § 52.255(2) (2019); FED. R. EVID. 1004(b).

[88] *See, e.g.*, *Young*, 744 P.2d at 904; Tomlinson v. Nevada, 878 P.2d 311, 312–14 (1994).

[89] *Young*, 744 P.2d at 904.

[90] *Tomlinson*, 878 P.2d at 312–14 (holding a transcript of an audio recording to be admissible only because all audio copies had been destroyed).

[91] *See, e.g.*, United States v. Bennett, 363 F.3d 947, 953 (9th Cir. 2004) (excluding testimony evidence about the path of the defendant's boat because the data from the boat's GPS was available); United States v. Workinger, 90 F.3d 1409, 1415 (9th Cir. 1996); Lang v. Cullen, 725 F. Supp. 2d 925, 971 (C.D. Cal. 2010).

[92] *Workinger*, 90 F.3d at 1415.

[93] *Id.*

content."[94] Thus, if the recording was available, the best evidence rule would have compelled the court to admit the recording over a transcript.[95]

A recent example of this policy in action can be found in the Central District of California.[96] In *Lang v. Cullen*, Lang was arrested at the San Francisco International Airport for, *inter alia*, possession of a firearm without a permit.[97] Several times over the next two weeks, Lang's public defender and an investigator from the public defender's office interviewed Lang while tape-recording their exchange.[98] Prior to trial, the court granted Lang's Motion in Limine to exclude the transcripts of those interviews which were being maintained in the files of the public defender's office.[99] The court held that because the audio recording was still available, the best evidence rule mandated that the parties bring the recording into court, or leave out the content of the recording entirely.[100]

This doctrine has a clear application to always-listening devices. Whenever a company details a transcript from an audio recording, there is a chance that something is misinterpreted or misunderstood.[101] With something used as frequently, and for as many reasons, as an always-listening device, there are simply too many chances that a request was misunderstood, transcribed improperly, and not reflected accurately by any written transcript. In the real world, a misstated transcript could be pieced together, and the true meaning can be assumed. In a court of law, there is too much on the line to leave an interpretation up to chance when a better alternative exists. Thus, the best evidence rule should apply to audio recordings from always-listening devices, so the audio recordings are brought into evidence whenever possible.

The issues of authentication and misapplication of searches made by devices accessed by multiple individuals are also addressed by applying the best evidence rule. A transcript made by the device could be based on the words of anyone.[102] An audio recording does not have these issues, as Nevada already allows for authentication of a voice by simply hearing it. Defendants and plaintiffs alike do not have to worry about false searches being used against them if audio recordings are the preference. In fact, this creates an additional incentive to keep audio recordings on the servers of whichever company hosts the always-listening device. If the recordings are being stored indefinitely, at no additional cost to the

---

[94] *Id*.

[95] *See id*.; United States v. Gonzales-Benitez, 537 F.2d 1051, 1053–54 (9th Cir. 1976).

[96] *Lang*, 725 F. Supp. 2d at 972 n.83.

[97] *Id*. at 971.

[98] *Id*. at 972–74.

[99] Order Granting Petitioner's Motion in Limine to Exclude Transcript of Audiotape at 3, Lang v. Woodford, No. CV-91-04061 (C.D. Cal. Mar. 30, 2010), *rev'd sub nom*. Lang v. Cullen, 725 F. Supp. 2d 925, 925 n.1 (C.D. Cal. 2010).

[100] *Id*.

[101] Sophie Curtis, *Worst Alexa Fails: Amazon Echo Users Share Voice Assistant's Biggest Screw-Ups*, MIRROR ONLINE (Jan. 2, 2018, 12:52 PM), https://www.mirror.co.uk/tech/worst-alexa-fails-echo-amazon-11768630 [https://perma.cc/M2M9-A6F8].

[102] *See supra* note 62 and accompanying text.

user, the user can prove that an incriminating use of the device was or was not uttered by them.

One might assume that Nevada's best evidence rule already covers audio recordings from always-listening devices. However, remember that Nevada Revised Statute section 52.255(2) contains an exception which allows for transcripts of recordings to be admitted when "[n]o original can be obtained by any available judicial process or procedure."[103] As discussed above, Arkansas was unable to establish that companies like Amazon must submit audio recordings when a court issues a subpoena for such a recording.[104] If companies storing always-listening device audio recordings are not required to deliver audio recordings when Nevada courts request, prosecutors are hard pressed to introduce that evidence without the consent of the defendant.[105] Without federal legislation compelling companies to comply with state subpoenas, the only audio recordings covered by the best evidence rule are recordings stored in the physical memory of the user's always-listening device.[106]

This unfortunate reality raises an important question: how many recordings are actually available to be brought into court? Even if a user manually enters their device settings to delete the recordings, the audio recordings remain on the device company's servers.[107] Yet, companies actively discourage their users from deleting these recordings.[108] For example, Amazon claims that by not deleting the recordings, a user continuously improves their device's ability to recognize speech and language.[109] While it is all but certain that at least some users have deleted their recordings, it can be inferred that a vast majority of users have not or will not delete their recordings.

Thus, by specifying that audio recordings still possessed on defendants' devices must be disclosed if they are relevant to the suit, this new legislation would address the issue of relevance and stand by Nevada's best evidence rule.[110]

III. PROTECTING NEVADANS' CONSTITUTIONAL RIGHTS

This Note cannot suggest that Nevada's legislation codify a law requiring individuals to submit always-listening device data to law enforcement without first addressing the known constitutional issues such a law would bring. Part III

---

[103] NEV. REV. STAT. § 52.255(2) (2019).

[104] *See supra* Section I.B.

[105] *See supra* text accompanying notes 55–59.

[106] *See* NEV. REV. STAT. § 52.255 (2019). Recordings of this type would be original, obtainable, and easily authenticatable by opinion of the voice.

[107] Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019, 6:00 AM), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time [https://perma.cc/V76M-7BFJ].

[108] *Alexa, Echo Devices, and Your Privacy*, *supra* note 25.

[109] *Id*.

[110] NEV. REV. STAT. § 52.235 (2019).

of this Note specifically considers those constitutional issues and how they best guide Nevada's legislation.

A. Fourth Amendment Protections and Always-Listening Device Data

It has been argued that the government searching for and seizing recordings from always-listening devices is inherently in violation of the Fourth Amendment.[111] A common theme among those arguments is the overbreadth of the third-party doctrine, which will be discussed below.[112] Some argue that the third-party doctrine should not apply in cases where technology is involved because of the near necessity of utilizing third parties in the modern age of technology.[113] Others argue that the companies manufacturing the always-listening devices should develop the devices in such a way that they do not fall under the third-party doctrine.[114] Others argue that the third-party doctrine should be more narrowly construed so always-listening devices are considered as personal property protected from physical trespasses by law enforcement.[115]

This Note argues that Nevada should not wait for Supreme Court interpretations of the third-party doctrine to change or burden companies with manufacturing requirements. Instead, Nevada should adhere to the advice of Justices Alito and Thomas,[116] and follow the path set by Utah[117] by enacting its own legislation allowing law enforcement to retrieve data from any always-listening device so long as they obtain a warrant first.

The third-party doctrine has been discussed as a major issue with police access to private data.[118] The doctrine, established by the Supreme Court in *United States v. Miller*, excludes from Fourth Amendment protection data given up by

---

[111] *See, e.g.*, Julia R. Shackleton, *Alexa, Amazon Assistant or Government Informant?*, 27 U. MIA. BUS. L. REV. 301, 322–23 (2019); Anne Pfeifle, Comment, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421, 423 (2018); Katherine E. Tapp, Note, *Smart Devices Won't Be "Smart" Until Society Demands an Expectation of Privacy*, 56 U. LOUISVILLE L. REV. 83, 110 (2017).

[112] The third-party doctrine makes admissible any data entrusted by the defendant to third parties. *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

[113] *E.g.*, Pfeifle, s*upra* note 111, at 429–30 (quoting United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring)).

[114] *E.g.*, Stacey Gray, *Always on: Privacy Implications of Microphone-Enabled Devices*, FUTURE PRIV. F. 3, 8–9 (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/58EB-NK53].

[115] Shackleton, s*upra* note 111, at 327.

[116] Carpenter v. United States, 138 S. Ct. 2206, 2261 (2018) (Alito & Thomas, JJ., dissenting) ("Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope.").

[117] Molly Davis, *Utah Just Became a Leader in Digital Privacy*, WIRED (Mar. 22, 2019, 8:00 AM), https://www.wired.com/story/utah-digital-privacy-legislation [https://perma.cc/AF7Q-QKL3].

[118] Pfeifle, s*upra* note 111, at 429–30.

individuals to third parties.[119] In *Miller*, the Court determined that Miller's Fourth Amendment rights were not violated when Miller's bank gave his banking information to ATF.[120] The Court reasoned that because Miller had entrusted the information to a third party, his bank, he could not have a reasonable expectation of privacy to the information.[121] In a digital age where almost all information is stored on the server of one third party or another, even those within the Court have grown concerned that the third-party doctrine has become overly broad.[122]

First, one proposed solution is to place the burden on the companies that create and service the always-listening devices.[123] Rather than exposing users to privacy concerns under the third-party doctrine, companies could design the always-listening devices to store as much data as possible on the actual device in encrypted format.[124] Hypothetically, this could minimize the data that police or federal agents could access when searching through the physical device without a warrant, and would limit the overall amount of data subject to seizure solely because it was transferred to third parties.

While this approach addresses some of the issues of always-listening devices and privacy, it is unnecessary to provide Fourth Amendment protections to users. The argument is not without merit, but it ignores the impact this would have on users. These devices are not computers, cell phones, or servers. Always-listening devices were not purchased *en masse* until prices dropped to $25-$50 because, for most users, the devices serve the barebone purpose of a speaker and a search engine.[125]

If companies are forced to overhaul the design of their products by including encryption, mass storage, and other requirements to avoid falling under the third-party doctrine, the price of the devices would likely skyrocket. Nothing is stopping companies from moving into the market for expensive, secured, always-listening devices. Yet, consumers seem to want always-listening devices that are affordable.[126] Pricing out the average customer from always-listening devices is not a simple solution to privacy concerns without consequence, it is a surefire way to shut down companies' interest in developing the technology further.

---

[119] United States v. Miller, 425 U.S. 435, 443 (1976).

[120] *Id*. at 440.

[121] *Id*. at 442–43.

[122] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[T]he premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age." (citations omitted)).

[123] Gray, *supra* note 114, at 8 (explaining that *manufacturers* should build the product based in part upon consumer privacy expectations).

[124] *See, e.g*., Aaron Allsbrook, *Five Easy Ways to Build Security into the Internet of Things*, FORBES TECH. COUNCIL (Nov. 23, 2016, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2016/11/23/five-easy-ways-to-build-security-into-the-internet-of-things [https://perma.cc/3QFP-576A].

[125] Mark Sullivan, *Apple HomePod Prices Drop as Cheap Smart Speakers Take off*, FAST CO. (Dec. 12, 2018), https://www.fastcompany.com/90280807 [https://perma.cc/Z927-26MM].

[126] *Id*.

Those who choose to purchase always-listening devices simply must understand that convenience at such low prices comes with lessened protections for their confidentiality.

Second, it has been argued that an unreasonable search occurs when police gain information from always-listening devices without a compelling interest.[127] This argument appears to analogize always-listening devices to personal property like an individual's car.[128] However, it also recognizes that the third-party doctrine in its current form clearly applies to always-listening devices and even distinguishes the devices from other physical assets.[129] Accordingly, the argument compels courts to reconsider the third-party doctrine and to "use a narrower construction that would greatly limit the government's ability to obtain an individual's personal and private information."[130]

This argument appropriately recognizes that there are issues with police access to always-listening devices under currently enacted laws. However, this Note disagrees with the perspective that the third-party doctrine grants "unfettered discretion to law enforcement" in its current form.[131] Yes, the government is currently able to gain access to data stored on always-listening devices, but it is only able to do so in two ways.

The first way is accessing the always-listening device directly and pulling any relevant information from it.[132] However, as previously discussed, data is not guaranteed to be stored on the device.[133] Which leads to the second option, to gain the recordings from the company that stores them.[134] Yet, companies have recognized that their users would rather not have their information spread to the government without a compelling interest.[135] In fact, companies thus far have denied government requests to access this information, even in the face of a subpoena.[136] If the current, broad, interpretation of the third-party doctrine does not require compliance with governmental requests for the recordings, narrowing the third-party doctrine so it does not apply to always-listening devices is unnecessary.

Finally, it has been argued that principles from the Stored Communications Act[137] should be applied to all digital data so long as the digital data is considered

---

[127] Shackleton, s*upra* note 111, at 326.

[128] *Id*.

[129] *Id*.

[130] *Id*. at 327.

[131] *Id*.

[132] Russell Brandom, *How Much Can Police Find Out From a Murderer's Echo?*, THE VERGE (Jan. 6, 2017, 9:05 AM), https://www.theverge.com/2017/1/6/14189384 [https://perma.cc/5RVT-3KCN].

[133] *See supra* note 36 and accompanying text.

[134] *See e.g.*, Brewster, s*upra* note 58.

[135] *See supra* notes 32–40 and accompanying text.

[136] *See supra* notes 39–40 and accompanying text.

[137] Stored Communications Act, 18 U.S.C. § 2701.

content information.[138] The Stored Communications Act, passed in 1986, requires disclosure of wire or electronic communications that exist in electronic storage upon proper government request.[139] However, under 18 U.S.C. § 2703(a), the government can only properly request such a disclosure from an individual with a valid warrant.[140] Accordingly, this argument suggests that the lessened requirement for government requests for disclosure from the storage companies be increased from subpoena to warrant.[141]

This argument provides excellent guidance for Nevada's legislation. Nevada has already shown favor for the Stored Communications Act by reference in Nevada Revised Statute section 179.467.[142] All that remains is incorporating the warrant requirement and specifically addressing audio recordings from always-listening devices. With these additions, the proposed law would provide law enforcement with access to always-listening devices, but would first require warrants to be issued on defendants for digital data they possess relevant to the specific crime. The law would both restrict evidence discovered from an always-listening device to relevant recordings and prevent law enforcement from conducting frivolous searches of devices without probable cause, quelling Fourth Amendment concerns.

Fortunately, Nevada does not have to invent an entirely new set of laws to properly address these issues. In 2019, Utah enacted the Electronic Information or Data Privacy Act.[143] This act adopts many of the principles of the Stored Communications Act without mandating that third parties comply with warrantless requests for data.[144] Specifically, it establishes that law enforcement may request digital data from users of technology or from the third parties that store the data so long as they have a valid warrant.[145] The act also includes various exceptions to the warrant requirement that mirror well established exceptions such as exigent circumstances or consent.[146] Indeed, Utah's Data Privacy Act serves as an excellent template for Nevada to allow requests for always-listening device data without violating the principles of the Fourth Amendment.

---

[138] Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1047 (2010).

[139] 18 U.S.C. § 2703(b).

[140] *Id*. § 2703(a).

[141] Kerr, *supra* note 138, at 1043–44.

[142] NEV. REV. STAT. § 179.467 (2019) ("The Nevada Supreme Court . . . may issue orders requiring a provider of electronic communication service to disclose . . . information pertaining to a subscriber to, or customer of, such service . . . upon the conditions prescribed by 18 U.S.C. § 2703.").

[143] Electronic Information or Data Privacy Act, UTAH CODE ANN. § 77-23c-101 (LexisNexis 2020).

[144] *Id*. § 77-23c-102(1)(a).

[145] *Id*.

[146] *Id*. § 77-23c-102(2).

B. First Amendment Issues yet Unanswered

The use of always-listening device recordings in criminal cases bring up other issues that the courts have yet to address.[147] One such issue is the First Amendment concern that a recording of expressive material is admitted as evidence against a defendant without their consent.[148] In the *Bates* case, Amazon rejected a subpoena demand for search results and audio recordings from an Echo device.[149] Amazon contended that recordings taken by their devices contained expressive material, and the device's responses themselves contained expressive material as well.[150] Amazon also claimed that audio recordings should have First Amendment protections attached,[151] and the government should have to show a compelling need for the data to bypass those protections.[152]

Unfortunately, the Arkansas court never had a chance to decide the issue in *Bates*. The issue was bypassed because Bates consented to the use of the recordings.[153] Thus, the issue of whether recordings of this type are considered expressive materials which are inadmissible absent clear consent remains merely in the hypothetical. Yet, Nevada must take steps to enact legislation protecting Nevadan's Fourth Amendment rights regardless of the unknown issues yet to be fully analyzed in court.[154]

IV. WHAT'S THE USE? REAL WORLD IMPACT OF LEGAL CHANGES

With so many issues surrounding always-listening devices, it is understandable to question why Nevada should pioneer legislation which enters recordings and transcripts from always-listening devices into evidence by default. Part IV of this Note presents situations where such data from always-listening devices is incredibly useful to both law enforcement and users.

A. Always-Listening Devices in Criminal Cases

Just this year, recordings from an always-listening device have been sought for use as evidence in a murder case.[155] On July 12, 2019, Silvia Galva died from

---

147 Heater, *supra* note 55.

148 *See id*.

149 Brewster, s*upra* note 58.

150 *Id*.

151 *Id*.

152 *Id*.

153 Dwyer, *supra* note 40.

154 To be sure, there may be First Amendment concerns arising from such legislation. However, those issues are beyond the scope of this Note which advocates for legislation preempting redundant litigation on issues courts have already analyzed in this and other jurisdictions.

155 Linda Trischitta, *Spear Impales Woman and Kills Her. Now Her Boyfriend Is Accused of Murder*, S. FLA. SUN SENTINEL (July 16, 2019), https://www.sun-sentinel.com/local/broward/hallandale/fl-ne-hallandale-silvia-galva-homicide-20190716-57vpgdkiazhytaggu7gg5dfuna-s

a stab wound to her chest.[156] Her boyfriend, Adam Crespo, claimed to police that the two were in an argument and he was trying to drag her out of bed.[157] According to Crespo, he was facing away from her when she grabbed a spear with a twelve inch blade, which snapped and impaled Galva's chest as Crespo continued to try to pull her out of bed.[158] Crespo then claimed that he then pulled the blade out of her chest and put pressure on the wound while Galva's friend called 911 and performed CPR.[159] While Crespo claimed that he did not believe the injury was severe, Galva died from her wounds, and Crespo was charged with murder.[160]

This scenario is a perfect example of why always-listening devices should be admissible as evidence by default. On its face, this is an incredibly difficult situation for the justice system to deal with. While Crespo claimed that Galva's death was an accident, there were no witnesses in the bedroom that could corroborate or disprove his story.[161] However, the police quickly started considering one piece of evidence: Crespo's Amazon Echo device.[162] Just one month after Galva's death, Florida police were able to obtain a search warrant for all recordings taken by the two Echo devices in Crespo's apartment on July 12, 2019.[163]

As previously discussed in this Note, Amazon has historically been unwilling to give out recordings taken by their users' devices.[164] In the *Bates* case discussed above, Amazon refused to comply with an Arkansas search warrant, and only turned over the recordings when Bates consented to the police receiving them.[165] However, in *Crespo*, police claim to have received the recordings from Amazon, with no official objections, after issuing their warrant.[166] How these recordings will affect the case is yet to be seen.[167]

The recordings may prove to be unhelpful to either party in this case. Perhaps the event could have been missed altogether if the Echo was not activated during

---

tory.html [https://perma.cc/AV6Z-VTED]; NBC News, *Amazon's Alexa May Have Witnessed Alleged Florida Murder, Authorities Say*, WRCBTV (Nov. 2, 2019, 11:33 AM), https://www.wrcbtv.com/story/41263095/amazons-alexa-may-have-witnessed-alleged-florida-murder-authorities-say [https://perma.cc/Y3VE-M28K].

156 Trischitta, *supra* note 155.

157 *Id*.

158 *Id*.

159 *Id*.

160 *Id*.

161 Galva's friend was in the house, but she was unable to tell police anything besides that there was an argument in the bedroom. *Id*.

162 Rafael Olmeda, *Alexa, Is He Guilty of Murder? Amazon Device May Have Heard Slaying, Cops Say*, S. FLA. SUN SENTINEL (Oct. 31, 2019), https://www.sun-sentinel.com/news/crime/fl-ne-amazon-alexa-murder-investigation-20191031-qccpvdl6kng5hcx3z6eusxa264-story.html [https://perma.cc/9M3S-LKHZ].

163 *Id*.

164 *See supra* Section I.B.

165 *See supra* Section I.B.

166 Olmeda, *supra* note 162.

167 *Id*.

the argument. Alternatively, the Echo could have been activated but still failed to record anything of use, or the Echo could have recorded damning evidence that helps one of the parties prove their case. No matter the outcome, it is important that the police and the defendant be able to access the recordings of the device so they can determine which of the situations they are facing. Further, police receiving the recordings without intense litigation or Crespo's consent points to the gradual acceptance of always-listening device recordings being used in the criminal justice system.

Despite Amazon's spokespeople objecting to "overbroad or otherwise inappropriate demands" of customer information,[168] it appears that Amazon's stance on the issue has shifted somewhat over the past few years.[169] Amazon's compliance with a warrant, absent public consent from their client, marks a new age for always-listening devices in the justice system. While some argue that this new age of always-listening devices is an invasion of privacy that ruins the sanctity of the home,[170] this Note argues that these devices have the potential to provide safety to a group of people that are constantly in danger.

B. Always-Listening Devices as Deterrents to Domestic Violence

Domestic violence is an issue that affects more than ten million victims a year in the United States.[171] In a 2009 special report, the U.S. Department of Justice published their findings on domestic violence in America.[172] According to the 2005 National Crime Victimization Survey, the annual domestic violence rate—the amount of people who self-reported being victims of intimate partner domestic violence—was 0.59 percent of women and 0.21 percent of men.[173]

---

[168] "Amazon spokeswoman Faith Eischen told The Washington Post that . . . [Amazon] 'objects to overbroad or otherwise inappropriate demands as a matter of course.' " Kayla Epstein, *Police Think Amazon's Alexa May Have Information on a Fatal Stabbing Case*, WASH. POST (Nov 2, 2019, 5:28 PM), https://www.washingtonpost.com/technology/2019/11/02/police-think-amazons-alexa-may-have-information-fatal-stabbing-case [https://perma.cc/NQ3L-4NES].

[169] "Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order." *Law Enforcement Information Requests*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF [https://perma.cc/CGY2-PVVJ].

[170] *See supra* Section III.A.

[171] MICHELE C. BLACK ET AL., NAT'L CTR. FOR INJ. PREVENTION & CONTROL, CDC, NATIONAL INTIMATE PARTNER AND SEXUAL VIOLENCE SURVEY: 2010 SUMMARY REPORT 38 tbls. 4.1 & 4.2 (2011), https://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf [https://perma.cc/D6TY-VA9P]; NAT'L COAL. AGAINST DOMESTIC VIOLENCE, DOMESTIC VIOLENCE (2020), https://assets.speakcdn.com/assets/2497/domestic_violence-2020080709350855.pdf [https://perma.cc/68L9-AHP8].

[172] NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUST., PRACTICAL IMPLICATIONS OF CURRENT DOMESTIC VIOLENCE RESEARCH: FOR LAW ENFORCEMENT, PROSECUTORS AND JUDGES vi (2009).

[173] *Id.* at 1.

Always-listening devices have already been used to help protect domestic violence victims.[174] In July 2017, a woman activated her nearby Amazon Echo device during a violent exchange with her boyfriend, Eduardo Barros, in their New Mexico home.[175] The device called 911, and dispatchers heard the woman yelling "Alexa, call 911."[176] Police arrived at the scene and eventually arrested Barros after an hours-long standoff.[177] Referring to always-listening devices, Sheriff Manuel Gonzales III later told reporters, "[t]his amazing technology definitely helped save a mother and her child from a very violent situation."[178]

While the New Mexican woman's active use of always-listening devices protected her from an actively violent situation, the deterrent value of warrant access to the audio recordings is far more widespread. It is sometimes wrongly assumed that if victims know that they can dissuade their abusers from acting violently by calling the police, they will.[179] Even with police intervention available with a 911 call, studies show that many victims choose not to actively invoke police protection.[180] For victims that do not necessarily want their abusers to be arrested or prosecuted, always-listening devices could provide an alternative means of protection.

If a person fears for their safety in their own home, they would be able to take control of a hostile situation by saying "Alexa/Google/Siri, record this conversation." By recording the encounter, the victim would force the abuser to deescalate because the audio of the interaction would be stored offsite. This process would provide victims an alternative means to dissuade their abusers in individual situations while collecting evidence of instances of abuse if they later decide to involve the police.

Unfortunately, this deterrent value is stifled because prosecutors are not guaranteed access to such recordings without the consent of the victim.[181] Domestic violence studies suggest that prosecutors are less likely to charge for issues like attempted murder that required subjective findings like criminal intent.[182] This was likely due to prosecutors generally facing hesitant involvement

---

[174] Marcus Harun, '*Alexa' Automatically Calls 911 After Amazon Echo Overhears Domestic Violence Attack*, FOX61 (July 11, 2017, 9:31 AM), https://fox61.com/2017/07/11/alexa-automatically-calls-911-after-amazon-echo-overhears-domestic-violence-attack [https://perma.cc/Y3YN-DMQM].

[175] *Id*.

[176] *Id*.

[177] *Id*.

[178] *Id*.

[179] *See* EVE BUZAWA ET AL., RESPONSE TO DOMESTIC VIOLENCE IN A PRO-ACTIVE COURT SETTING 100–01 (1999) ("The literature on domestic violence strongly suggests that many victims refuse to call the police for a variety of reasons ranging from offender intimidation, financial dependence, and perceived police indifference.").

[180] *Id*.

[181] *See supra* Section III.A.

[182] BUZAWA ET AL., *supra* note 179, at 124.

from victims who have close relationships with their abusers.[183] Studies indicate that it is not uncommon for victims to request the offender not be arrested[184] and almost half of victims do not wish for their abuser to be prosecuted.[185]

Because victims may be understandably hesitant to assist prosecutors, and because there is no law which currently guarantees that recordings from always-listening devices may be seized and entered into evidence, the deterrent value of always-listening devices is incredibly limited. Without key witnesses to assist, law enforcement is currently shoehorned into charging for lesser offenses or dismissing the case entirely.[186] To this point, one study revealed that in 1995, when the Milwaukee prosecutor changed local policy to no longer require victims to participate in charging conferences, prosecutors began accepting three times as many domestic violence cases.[187] The reasons that victims do not want to assist with arrests or prosecutions is an invariably complicated issue, but one that could be potentially bypassed in many situations by the presence of an always-listening device.

Depending on the quality of recordings from always-listening devices, prosecutors could find that a victim's testimony is unnecessary to prove instances of violence and subjective criminal elements like criminal intent. It is in these situations that an always-listening device specific rule of evidence would be imperative. Without the appropriate witness to lay the foundation for the recordings, prosecutors could possess a smoking gun and have no way to bring it in to trial. If Nevada were to implement this Note's suggested changes to Nevada Revised Statute section 52,[188] the recordings could be brought in through the testimony of an Amazon/Google/Apple employee who specializes in the storage and retrieval of always-listening device recordings.[189]

Accordingly, if abusers know that their actions in the home can be recorded and accessed, even against their victim's wishes, they would no longer be able to rely on intimidating or persuading their victims to not call the police or participate in prosecution. The third-party involvement of always-listening devices would serve as a significant deterrent to abusers acting violently towards others in the home without marking the victims as the cause of the deterrent.

Of course, any deterrent value would rely on both a future where always-listening devices are so intertwined to home life that absence of these devices

---

[183] *Id*. at 125–27.

[184] BARBARA E. SMITH ET AL., AN EVALUATION OF EFFORTS TO IMPLEMENT NO-DROP POLICIES: TWO CENTRAL VALUES IN CONFLICT 60 (2011); BUZAWA ET AL., *supra* note 179, at 113.

[185] BUZAWA ET AL., *supra* note 179, at 125; SMITH ET AL., *supra* note 184, at 64.

[186] *See* NAT'L INST. OF JUSTICE, *supra* note 172, at 40–41.

[187] BUZAWA ET AL., *supra* note 179, at 121.

[188] *See supra* Section II.B.

[189] *See* NEV. REV. STAT. § 52.260(1)–(2) (2021) ("The contents of a record made in the course of a regularly conducted activity . . . may be proved by the original or a copy of the record which is authenticated by a custodian of the record . . . ."); *Id*. § 52.260(6)(a) (" 'Custodian of the records' means an employee or agent of an employer who has the care, custody and control of the records of the regularly conducted activity of the employer.")

would be of note, and on a society that accepts and encourages the use of always-listening device recordings in this way. If Nevada adopts this Note's suggestions in anticipation of this future, always-listening devices could become a tool which empowers domestic violence victims to retake control of their environment and prevent future abuse.

V. RECOMMENDATIONS FOR NEVADA

A. Minor Changes to Existing Nevada Laws

The issues above leave a difficult situation for legislators to work through as they tackle always-listening devices. For legislation to allow audio recordings taken by always-listening devices into evidence at trial, the legislation must address each of the many issues discussed above.

First, new laws must provide a standardized hearsay exception so the government is not forced to wedge the recordings in under another, less appropriate, exception. Second, new laws must specify a process to ensure that audio from an always-listening device is authenticated so the trier of fact need only determine if the recording is of the defendant's words.[190] Third, new laws must establish that the best evidence rule applies to transcripts of the audio recordings and thus deny entrance of transcripts whenever audio recordings are available.[191] Finally, new laws must allow law enforcement access to devices whenever the recordings are relevant, but still establish strong warrant requirements to avoid unconstitutional invasions of privacy.[192]

As to the hearsay issue, Nevada should enact a new exception to hearsay for "smart assistant communications." The exception should allow audio recordings created by smart assistants through always-listening devices to bypass hearsay objections. This will negate unnecessary objections to recordings that, if authenticated and determined to be spoken by the defendant, do not constitute traditional hearsay.

As to the authentication issue, Nevada should amend Nevada Revised Statute section 52 to include provisions from Federal Rule of Evidence 902(13). Nevada should specify that records generated by electronic processes or systems that produce accurate results are authenticated so long as a qualified person can certify the process or system.[193] This will ensure that the trier of fact is able to consider whether the defendant actually engaged with the device by matching the voice recorded instead of text transcribed.

As to the relevance issue, Nevada should double-down on its version of the best evidence rule by allowing law enforcement to request audio recordings when it is relevant to a case. Nevada should enact legislation that gives law

---

[190] *Supra* Section II.B.
[191] *Supra* Section II.C.
[192] *Supra* Section III.A.
[193] *See* FED. R. EVID. 902(13).

enforcement a clear process to request such recordings from a defendant's own device and from companies who are willing to adhere to the request.

To that point, and as to the Fourth Amendment concerns, Nevada should enact legislation similar to Utah's Electronic Information or Data Privacy Act.[194] Nevada should enact legislation that allows law enforcement to request data from always-listening devices from users or the third-parties that store the data. However, the legislation must require warrants to ensure that only relevant, particular, and necessary data is accessed.

CONCLUSION

With relatively minor changes to already existing Nevada Law, Nevada can avoid facing the same evidentiary, constitutional, and ethical questions Arkansas faced in *Bates* or Florida faced in *Crispo*. Instead, Nevada can move forward with confidence that the new age of always-listening devices will not hinder the administration of justice or diminish Nevadans' constitutional rights.

[194] Electronic Information or Data Privacy Act, UTAH CODE ANN. §§ 77-23c-101–105 (LexisNexis 2020).