The Struggle for Control of Personal Data

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Matthew Hancock

April 6, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Matthew Hancock

Sociotechnical advisor: Peter Norton, Department of Engineering and Society

The Struggle for Control of Personal Data

Personal data in the digital age wasn't widely understood or regulated before 2010. Internet connected voice assistants, part of the Internet of Things (IoT), gained popularity in 2011 when Apple released Siri (Apple 2011). Amazon's Echo was the first mainstream smart home speaker (Amazon 2015). Prior to launch, tech companies stayed quiet about how their voice assistants handled users' personal data. Echo's release surprised consumers because there were no launch events or detailed descriptions of how it worked (Tsukayama 2014). Voice assistants activate after hearing trigger words, worrying consumers about how much they listen to and store on their servers.

Privacy advocates seek to limit tech companies' control over personal data. Their voices make consumers more cognizant of their privacy. Since 2018, several states have introduced legislation concerning data collection. Privacy advocates are making progress in their efforts, but they need more immediate progress to keep up with the growing smart home market.

Review of Research

The most controversial case of personal data collection in the US came from the National Security Agency. In 2013, former NSA employee Edward Snowden leaked several documents describing mass surveillance of American citizens. Weinstein (2014) scrutinizes how his leaks affected international views of US cyber power. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act) created the US Department of Homeland Security and granted them the power to collect electronic communications to aid in the

War on Terror. Siegler (2006), argues that the Patriot Act's emphasis on physical and digital surveillance violates constitutional rights and makes legal defense more difficult.

Data collection from foreign tech giants prompted action from the US government. The National Intelligence Law of the People's Republic of China requires that "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of" (China Law Translate 2017). Fearing that Chinese telecommunications company Huawei would comply by sending user information to the Chinese government over 5G networks, the Trump administration issued a full ban on their devices in 2019. Waldron (2020) investigates whether Huawei poses a significant threat to US national security and if less extreme methods could have been used to address it. ByteDance, the Chinese company who owns the popular app TikTok, was banned from conducting transactions with US companies for similar reasons. Ryan, Fritz, and Impiombato (2020) found that TikTok's engineers were able to find American users' names, birthdays, home addresses, phone numbers, emails, passwords, PayPal account information, contact lists, private videos, direct messages and more.

In some countries, the government mandates personal data retention. The EU Data Directive requires Internet Service Providers to keep records of electronic communications in case law enforcement needs to access them. The Electronic Frontier Foundation, along European Digital Rights, AK Vorrat, and other civil society advocates, argue that mandatory data retention violates civil rights and increases the vulnerability of personal data to interception from hackers (Rodriguez et al.). Several cases have been brought up with the Court of Justice of the European Union regarding this regulation.

Pajcic (2018) discusses the conflicts of interest data retention presents introduces between public safety and privacy and outlines the struggles lawmakers have in finding a balance between the two.

The struggle for control of personal data is still a work in progress. More research will become available on this subject in the future, so periodic progress checks are recommended.

The people

Privacy isn't the top priority of most consumers. A survey by Consumers International and the Internet Society showed that 63 percent of respondents believe connected devices are "creepy" and 75 percent see good reason for concern over how collected data is used by tech companies (Consumers International et al. 2019). However, 70 percent of survey respondents still own connected devices. Even those who chose not to buy smart home devices do so mostly for other reasons. Privacy concerns were the main deterrent for 28 percent of survey respondents who didn't buy smart home devices – the same percentage as those deterred by price. Acquisti, Taylor, and Wagman (2016) describe privacy as an economic value entailing tradeoffs with other values, such as utility. Secure alternatives to smart home devices don't exist, so consumers see loss of privacy as a necessary cost. Americans do little to limit their data collection even with available resources. A 2014 survey by the Pew Research Center found that only 10 percent of Americans encrypt their phone calls, text messages, and email, and only 9 percent browse the internet anonymously (Madden et al., 2015). Despite indifference to data collection, Americans expect changes to current policy. The same survey found that

around 50 percent of Americans hope for limits on the amount of time online records of usage data are kept by corporations and the government. Although privacy isn't the top priority of the average American consumer, they're aware of it and hope for more regulation.

Those who prioritize privacy are passionate. Stanley (2017) from the American Civil Liberties Union views digital assistants and other Internet of Things (IoT) devices as a "triple threat to privacy: from government, corporations, and hackers". He fears that audio files kept for too long will be used to send ads to users, taken by the government without a warrant, or stolen by nefarious third parties. He says this triple threat can be stopped if voice assistants retain audio for only a minimal necessary period, don't share recordings without a warrant, and don't use audio data for other purposes.

Privacy advocates regularly communicate with the government. The Electronic Privacy Information Center sought to make Data Protection a platform in the 2016 election in the US (EPIC 2016). They asked congressional candidates for their viewpoints on strong encryption, privacy legislation, etc., and asked for greater enforcement against identity theft, financial fraud, and data breaches. The Consumer Technology Association works to educate lawmakers on improving product security and fostering market incentives for more secure IoT products (CTA). Their legislative priorities, which have been sent to Congress, focus on risk, establishing standards, maintaining freedom, and following principles. CTA developed the Industry Consensus on IoT Device Security Baseline Capabilities, an initiative to outline security capabilities to properly secure the IoT sector, in partnership with the Council to Secure the Digital Economy. Echo Kids Privacy (2019) took issue with how Alexa interacts with children, believing it's in

violation of the Children's Online Privacy Protection Act (COPPA). They argue that Alexa lacks necessary parental control or consent options and keeps children's personal information much longer than necessary. Deleting information collected from children is currently too difficult, requiring parents to search through every single audio interaction and delete their child's recording manually. They don't believe Alexa provides children enough protections from third-parties who may have access to their data. Their concerns were submitted to the Federal Trade Commission in a formal complaint, asking them to "hold Amazon accountable for blatantly violating children's privacy law and putting kids at risk" (CCFC).

How tech companies handle data

Amazon, Google, and Apple, the creators of the three most popular voice assistants, claim to store personal data on their servers to improve product functionality (Fowler 2019). Voice assistants rely on audio data to train their artificial intelligence. Audio interactions are stored on Amazon's servers until manual deletion, regardless of whether they were intended for Alexa (Amazon). Google only keeps data when prompted by users (Google). Apple does the same, while also giving unique identifiers to audio recordings in order to separate them from individuals (Apple). All companies employ humans to listen to audio data to improve speech technology (Tasca 2019). Whether tech companies sell personal data is unknown, and they never provide a clear answer. Many assume that voice recordings factor into more personalized advertisements for users (Tsukayama 2015).

There are cases where tech companies have sought to keep personal data in the hands of their users. In 2016, following a mass shooting in San Bernardino, CA, Apple refused pressure from the FBI to create a software update allowing them to view the shooting suspect's personal text messages. Apple CEO Tim Cook believed this would set a dangerous precedent, citing that the "implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge" (Cook 2016). The ACLU and many other privacy advocates expressed their support for Apple (ACLU 2016). Amazon, with the help of the ACLU, sued the North Carolina Department of Revenue in 2010 after they requested data linking customers to their purchases (ACLU 2010). A federal judge sided with Amazon, ruling that this practice "violated Internet users' rights to free speech, anonymity and privacy".

Many believe tech companies don't do enough to keep their devices secure from bad actors, making them weary of how long personal data is stored online. Smart speakers allow developers to create small apps, called "Actions" on Google home and "Skills" on Amazon Alexa, to expand their functionality. For example, the ESPN skill for Alexa allows users to hear hourly score updates and listen to live ESPN radio (Amazon). While experimenting with Google Home and Amazon Alexa, Bräunlein and Frerichs (2019) of Security Research Labs discovered that Actions and Skills can eavesdrop on users and conduct phishing attacks. The pair called on Amazon and Google to better

police the third-party apps they allowed on their web stores. Barda, Zaikin, and Shriki (2020), researchers for Check Point, tested Alexa's defense against code-injections, exposing vulnerabilities which allowed attackers to quietly install and uninstall skills and gain access to a victim's voice history and personal information. They note that smart home devices are inherently vulnerable, making them attractive to bad actors.

Policymaker action

Some policymakers and federal agencies stand alongside privacy advocates. Senator Ed Markey (D-MA), the original author of COPPA, and Congressman Joe Barton (R-TX), have always held children's privacy in high regard. They worked together on the "Do Not Track Kids Act of 2011", an amendment to COPPA with updated provisions to the "collection, use and disclosure of children's personal information" (Senator Ed Markey 2011). After Echo Dot Kids Edition was released, they wrote a letter to Amazon CEO Jeff Bezos asking 12 questions about how the Echo protects privacy rights and complies with COPPA (Markey et al., 2018). Senator Chris Coons (D-Del.), wrote a similar letter to Bezos following a report that Amazon may still keep text transcripts of audio recordings after users manually delete them (Ng 2019). In it he asked what Amazon does with users' voice records and data. Sen Coons (2019) stated that the "American people deserve to understand how their personal data is being used by tech companies, and I will continue to work with both consumers and companies to identify how to best protect Americans' personal information". The National Institute of Standards and Technology released a document in early 2020 with some voluntary cybersecurity practices for companies to implement in their IoT devices (Fagan et al.

2020). NIST asks IoT device makers to identify expected customers and expected use cases, reach customer cybersecurity goals, determine how to address customer goals, and work on "reducing the prevalence and severity of IoT device compromises".

States recently began regulating the control of personal data. California was the first state to pass legislation for data privacy (California Consumer …, 2018). The state's act grants consumers the ability to request businesses to delete any personal data they've collected (with some exceptions), and businesses must notify consumers of their right to request data deletion. In 2019, the California State Assembly's privacy committee introduced the Anti-Eavesdropping Act, requiring makers of smart speakers to get consent from users before storing recordings (Information privacy … 2020). Assemblyman Jordan Cunningham (R), the sponsor of the bill, said tech companies "are giving us false choices. We can have these devices and enjoy their functionality and how they enhance our lives without compromising our privacy" (Fowler 2019). Illinois passed the Keep Internet Devices Safe Act that same year with the same requirements (SB1919). Other states with similar laws include Nevada (Nevada Senate …, 2019), Maine (An Act …, 2019), and Vermont (Vermont Senate …, 2020). Several other states have bills in progress. Nevada and Vermont's laws are similar to California's Consumer Privacy Act but Maine puts responsibility on internet service providers, not voice assistant makers (An Act …, 2019). Maine's law requires internet service providers to receive consent from their users before disclosing personal data. While this law may keep tech giants from seeing personal data, there's no requirement for them to honor requests for deletion.

The response

Amazon's response to Markey and Barton's letter was not well received. It focused on FreeTime Unlimited, their service for kid-friendly books and ad-free radio stations (Yurieff 2018). An Amazon spokesperson said they "believe one of the core benefits of FreeTime and FreeTime Unlimited is that the services provide parents the tools they need to help manage the interactions between their child and Alexa as they see fit". Frustrations with this response birthed Echo Kids Privacy, which Sen Markey and a few other members of Congress supported. Amazon's immediate response to EKP's complaint was "FreeTime on Alexa and Echo Dot Kids Edition are compliant with the Children's Online Privacy Protection Act (COPPA)" while directing customers to their privacy page (St. John 2019). Amazon now requires verifiable parental consent to collect children's personal data under COPPA and makes parental controls more powerful and easier to navigate (Amazon 2020). However, they still do not provide protections against third party services, instead putting responsibility on users. In response to Sen Coons' letter, Huseman (2019) said "customer trust is our highest priority, and we know we must get privacy right in order to meet our customers' high expectations". Coons was not impressed with the response, saying it did show a "commitment to protecting users' personal information," but noting that it "leaves open the possibility that transcripts of user interactions with Alexa are not deleted from all of Amazon's servers" (Coons 2019).

Apple and Google originally stored all audio recordings on their servers, but switched to opt-in programs to store them after public pushback. Google still has outside contractors review audio recordings, but on a much smaller scale (Tasca 2019). Apple features an additional opt-in for humans to review audio recordings, and limits reviewers

to only its own employees (Apple 2019). Amazon, after facing pressure from recent legislation, now allows users to have voice recordings automatically deleted after three or 18 months, or they can choose for audio recordings to be deleted immediately after every interaction (Amazon). Alexa still defaults to storing all audio interactions indefinitely.

Six weeks after publishing their experiment, Bräunlein and Frerichs checked if Amazon or Google took action to combat their exploits, which they did not (Bräunlein et al. 2019). When asked about the exploit, an Amazon spokesperson said "We have mitigations in place to detect this type of skill behavior and reject or take them down when identified. SR Labs contacted us late last week with new research and skills they developed, which we identified and blocked. We are currently reviewing the research, but can confirm we identified and took down all the new phishing skills before they were reported to us using our existing mitigations and monitoring tools. We will develop any necessary additional mitigations following our review" (O'Donnell 2019). Karsten Nohl, managing director at Security Research Labs, said Amazon's mitigations were "comically ineffective". Google did not respond to questions about the exploit. After hearing about the vulnerabilities found by Barda, Zaikin, and Shriki at Check Point, an Amazon spokesperson said "We appreciate the work of independent researchers like Check Point who bring potential issues to us. We fixed this issue soon after it was brought to our attention, and we continue to further strengthen our systems" (Grzeszczak 2020). Amazon's fix was confirmed by Check Point.

EFF legislative counsel Ernesto Falcon said California's privacy bill "improves on the existing privacy law so that consumers can control who gets access to their data and how the data is being used" (EFF 2019). 14 other privacy advocacy groups expressed

their support for California's law, including the ACLU, Common Sense Kids Action, Consumer Federation of America, and Privacy Rights Clearinghouse. Although privacy advocates are happy with new state regulations, they would like action from the federal government. EPIC, along with several other privacy advocacies, sent a letter with lessons learned from the California Consumer Privacy Act to Congress in hopes of the rest of the US following suit (Consumer and Privacy Organizations 2018). Their desired provisions included baseline federal data protection legislation, more robust enforcement, and a federal data protection agency.

Despite pushback and regulations, tech companies don't see much incentive to enhance privacy features. People are still buying smart home products. As of spring 2020, 60 million Americans, or 24 percent of the population, own a smart speaker (Edison Research …, 2020). By 2023, the number of smart home devices expected to break 300 million worldwide with a value of over 141 billion dollars (Tankovska 2020). 40 percent of that revenue is expected to come from North America. Voice assistants are no longer limited to expensive smart speakers – Google sells 5 different types of smart speakers for a minimum of 50 dollars (Google), and Amazon currently sells over 100 Alexa enabled smart devices, from their latest echo smart speakers to a 25-dollar voice controlled smart plug (Amazon).

Conclusion

Privacy advocates made progress towards keeping personal data private in the last decade, but tech companies have been slow to change. With precedents set by states with their own regulations, privacy advocates must focus their efforts on the federal

government for quick action. Rapid market growth may outpace their legislative goals, but more smart home owners means more support for privacy advocates. Data collection practices and lackluster cybersecurity measures will become less acceptable when they affect a majority of Americans. Privacy advocates face an uphill battle, but as their voices grow louder tech companies will be forced to do more to answer their demands.

References

ACLU. (2016, March 2). American Civil Liberties Union. ACLU Filing Brief Supporting Apple Against Order to Help IPhone. https://www.aclu.org/press-releases/aclu-filing-brief-supporting-apple-against-order-help-unlock-iphone.

ACLU. (2010, October 26). American Civil Liberties Union. Federal Court Upholds Amazon Users' Privacy and Free Speech Rights. https://www.aclu.org/press-releases/federal-court-upholds-amazon-users-privacy-and-free-speech-rights.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54(2)*, 442-492. Jstor

Amazon. (2015, June 23). Amazon Echo Now Available to All Customers. https://press.aboutamazon.com/news-releases/news-release-details/amazon-echo-now-available-all-customers

Amazon. Amazon Echo & Alexa Devices. Amazon.com. https://www.amazon.com/smart-home-devices/b/?ie=UTF8&node=9818047011&ref_=sv_devicesubnav_1

Amazon. Children's Privacy Disclosure. (2020, July 8). https://www.amazon.com/gp/help/customer/display.html?nodeId=202185560

Amazon. Common Questions About Alexa Privacy. Amazon.com. https://www.amazon.com/Alexa-Privacy-Hub/b?ie=UTF8&node=19149165011

Amazon. ESPN. Amazon.com. https://www.amazon.com/ESPN/dp/B074JCPM4M

An Act To Protect the Privacy of Online Customer Information. S.P.275-L.D.946. (2019). https://www.mainelegislature.org/legis/bills/display_ps.asp?ld=946&PID=1456&snum=129

Apple. (2011, October 4). Apple launches iPhone 4S, iOS 5 & iCloud. https://www.apple.com/newsroom/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud/

Apple. (2019, August 28). Improving Siri’s privacy protections. https://www.apple.com/newsroom/2019/08/improving-siris-privacy-protections/.

Apple. Privacy. Apple.com. https://www.apple.com/privacy/.

Barda, D., Zaikin, R., & Shriki, Y. (2020, August 13). Keeping the GATE locked on your IoT DEVICES: Vulnerabilities found on Amazon's Alexa. Check Point. https://research.checkpoint.com/2020/amazons-alexa-hacked/

Bräunlein, F., & Frerichs, L. (2019, December 17). Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping. Security Research Labs. https://srlabs.de/bites/smart-spies/

Benjamin, G. (2020, January 21). Amazon Echo's privacy issues go way beyond voice recordings. The Conversation. https://theconversation.com/amazon-echos-privacy-issues-go-way-beyond-voice-recordings-130016.

California Consumer Privacy Act of 2018. SB-1121. (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

CCFC. (2019, May 8). Campaign for Commercial Free Childhood. Advocates Demand FTC Investigation of Echo Dot Kids Edition. https://commercialfreechildhood.org/advocates-demand-ftc-investigation-echo-dot-kids-edition/.

China Law Translate. (2017, June 27). National Intelligence Law of the P.R.C. (2017). https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Consumer and Privacy Organizations. (2018). Draft Framework for Data Protection in the United States. https://epic.org/testimony/congress/CPOs-to-SCC-US-Data-Protection-Framework-Oct2018.pdf.

Consumers International & Internet Society. (2019). The trust opportunity: Exploring Consumers' Attitudes to the Internet of Things. Internet Society. https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf

Cook, T. (2016, February 16). A Message to Our Customers [Letter to Apple Customers]. Apple, Cupertino, California

CTA. Privacy and security. https://www.cta.tech/Advocacy/Issues/Privacy-and-Security

Edison Research & National Public Radio. (2020). The Smart Audio Report. National Public Media. https://www.nationalpublicmedia.com/uploads/2020/04/The-Smart-Audio-Report_Spring-2020.pdf

EFF. (2019, February, 27). Electronic Frontier Foundation EFF Supporting California's Privacy For All Bill, Which Puts People, Not Tech Companies, in Control of Personal Data. https://www.eff.org/press/releases/eff-supporting-californias-privacy-all-bill-which-puts-people-not-tech-companies

EKP (2019, May 9). Echo Kids Privacy. Echo Dot Kids Edition Violates COPPA. https://www.echokidsprivacy.com

EPIC. (2016). Electronic Privacy Information Center. Data Protection 2016. http://dataprotection2016.org

Fagan, M., Megas, K. M., Scarfone, K., & Smith, M. (2020). Foundational Cybersecurity Activities for IoT Device Manufacturers (NIST Interagency or Internal Report (NISTIR) 8259, Rep.). National Institute of Standards and Technology. doi:https://doi.org/10.6028/NIST.IR.8259

Fowler, G. (2019, May 08). Perspective | Alexa has been eavesdropping on you this whole time. Washington Post. https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time

Google. Assistant Privacy & Security Features - Google Safety Center. safety.google. https://safety.google/intl/en_us/assistant/?utm_source=google.

Google. Compare smart speakers and displays. Google Store. https://store.google.com/magazine/compare_nest_speakers_displays?toggler2=nest_hub&toggler3=nest_hub_max&toggler6=nest_hub&toggler4=home_mini

Grzeszczak, J. (2020, August 13). *Is Amazon Alexa safe? Cybersecurity researchers uncover serious privacy issues*. Newsweek. https://www.newsweek.com/amazon-alexa-safe-cybersecurity-researchers-uncover-serious-privacy-issues-1524888.

Huseman, B. (2019, June 28). Response to Concerns over Amazon's privacy and Data Collection Practices [Letter to Christopher A. Coons]. United States Senate, Washington, District of Columbia.

Information privacy: other connected device with a voice recognition feature. AB-1395. (2020). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1395

Keep Internet Devices Safe Act. SB1719. (2021). https://ilga.gov/legislation/billstatus.asp?DocNum=1719&GAID=15&GA=101&DocTypeID=SB&LegID=118965&SessionID=108

Madden, M., & Rainie, L. (2020, August 17). Americans' attitudes about privacy, security and surveillance. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Markey, E. J., & Barton, J. (2018, May 10). Amazon Echo Dot Kids Edition [Letter to Jeffrey Bezos]. Congress of the United States, Washington, District of Columbia

Nevada Senate Bill 220. NV SB220. (2019). https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Overview

Ng, A. (2019, May 09). Amazon Alexa transcripts live on, even after you Delete Voice records. https://www.cnet.com/home/smart-home/amazon-alexa-transcripts-live-on-even-after-you-delete-voice-records/

O'Donnell, L. (2019, December 17). *Alexa, Google Home Eavesdropping Hack Still Exists*. Threatpost English Global threatpostcom. https://threatpost.com/alexa-google-home-eavesdropping-hack-not-yet-fixed/151164/.

Ryan, F., Fritz, A., & Impiombato, D. (2020). TikTok and WeChat: Curating and controlling global information flows (pp. 36-42, Rep.). *Australian Strategic Policy* Institute. doi:10.2307/resrep26120.7

Rodriguez, K., Sheehan, K., Carlson, K., & O'Brien, D. Mandatory data retention. https://www.eff.org/issues/mandatory-data-retention

Siegler, A. (2006). The Patriot Act's Erosion of Constitutional Rights. *Litigation, 32*(2), 18-72. http://www.jstor.org/stable/29760549

Stanley, J. (2017, January 13). The Privacy Threat From Always-On Microphones Like the Amazon Echo [Web log post]. https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo

Senator Chris Coons. (2019, July 3). Amazon responds to Sen. Coons' concerns about consumer privacy practices for Alexa devices. https://www.coons.senate.gov/news/press-releases/amazon-responds-to-sen-coons-concerns-about-consumer-privacy-practices-for-alexa-devices

Senator Ed Markey (2011, October 14). Oct. 14, 2011: Markey to Amazon: Don't Hold a Kindle Fire Sale on Privacy. https://www.markey.senate.gov/news/press-releases/oct-14-2011-markey-to-amazon-dont-hold-a-kindle-fire-sale-on-privacy.

St. John, A. (2019, May 9). Amazon Echo Dot Kids Violates Privacy Rules, Advocates Claim. Consumer Reports. https://www.consumerreports.org/privacy/amazon-echo-dot-kids-violates-privacy-rules-advocates-claim/.

Tankovska, H. (2020). Smart home - Statistics & Facts. Statista. https://www.statista.com/topics/2430/smart-homes/

Tasca, N. (2019, September 23). Doing more to protect your privacy with the Assistant [web log]. https://www.blog.google/products/assistant/doing-more-protect-your-privacy-assistant/.

Tsukayama, H. (2014, November 11). How closely is Amazon's Echo Listening? https://www.washingtonpost.com/news/the-switch/wp/2014/11/11/how-closely-is-amazons-echo-listening/

Vermont Senate Bill 110 (Act 89). S.110. (2020). https://legislature.vermont.gov/bill/status/2020/S.110

Waldron, K. (2020). (Rep.). R Street Institute. doi:10.2307/resrep27015

Weinstein, D. (2014). Snowden and U.S. Cyber Power. *Georgetown Journal of International Affairs*, 4-11. http://www.jstor.org/stable/43773644

Yurieff, K. (2018, May 11). Lawmakers write letter to CEO Jeff Bezos with concerns about Amazon's Echo Dot for kids. CNNMoney. https://money.cnn.com/2018/05/11/technology/amazon-echo-dot-kids-lawmaker-concerns/index.html.