Internet-Connected Video Doorbells: Ethical, Privacy, and Legal Concerns

Robert Hosbach
MIDS W231: Behind the Data: Humans and Values

April 21, 2021

Contents

1 Introduction

Over the past decade, smart homes have transitioned from a distant dream to a current reality for many people. A variety of definitions for "smart home" exist; but, generally, a smart home is a home that contains devices meant to automate certain tasks. Due to the high level of Internet connectivity in homes, most of these automation devices connect to the Internet either individually or through a home automation system (the devices are sometimes referred to as Internet-of-things, or IoT, devices).

In 2012, roughly 1.5 million home automation systems were installed in the United States (ABI Research, 2012). These automation systems use centralized hubs as well as a variety of Internet-connected devices to monitor and control a home's climate, lighting, and appliances, among other things. Since then, companies have developed multitudes of new Internet-connected smart home devices, and the market penetration of smart home devices has grown substantially and will continue to grow for the foreseeable future (Verified Market Research, 2020). A 2020 report indicates that nearly 25% of American adults already own a home smart speaker (*e.g.*, Amazon Echo) (NPR & Edison Research, 2020). Additionally, the U.S. Department of Energy forecasts that residential connected LED lights and luminaires will grow from roughly two million systems in 2017 to over 600 million systems by 2035 (Navigant Consulting, Inc., 2019, pg. 25). But, smart speakers and connected lighting are not the only smart home devices that are rapidly becoming commonplace in U.S. households.

Current estimates suggest that over 20 million U.S. households, or one in seven homes, have an Internet-connected video doorbell (ICVD) (Business Wire, 2020; U.S. Census Bureau, 2020). ICVDs are typically installed near the front door of a home (like a typical doorbell), and common functionality across ICVDs includes: high-definition video capture and recording, night vision, motion detection, wide field of view (generally in excess of 90 degrees), two-way audio capture and recording, and Wi-Fi connectivity (Ring, 2020c; SimpliSafe, 2021b). The Ring Video Doorbell came to market in 2014, and it represents the first ICVD to gain significant market penetration (Ring, 2020a). Since then, many other companies—including Google, Vivint, and SimpliSafe—have brought products to this burgeoning market. However, Ring, which was acquired by Amazon in 2018, still holds the bulk of the U.S. video doorbell market share (Weinschenk, 2020). As with the smart home device market as a whole, ICVDs are poised for continued growth.

In this report, the ethical, privacy, and legal concerns of ICVDs in the United States are discussed. While these concerns exist for other smart home devices, ICVDs are an interesting case study due to their primary purpose of capturing video (and sometimes audio) of people outside the home. The Ring ICVD will provide

the basis for much of the content in this report due to Ring's popularity and media coverage. Moreover, the focus on the United States is not because ethical, privacy, and legal concerns for ICVDs do not exist in other locations, but because the United States forms the social and legal context the author is most familiar with.

The following section contains a discussion on the current perception of ICVDs by consumers and then provides a summary of recent news stories involving ICVDs. The next section of the report looks at the ethical, privacy, and legal concerns of ICVDs. ICVDs are evaluated using several well-regarded ethical and privacy frameworks, then the existing legal environment that ICVDs operate in is considered. Finally, recommendations are provided for mitigating the key ethical, privacy, and legal concerns identified for ICVDs, and the application of an existing framework for assessing a product's level of data privacy and security to ICVDs is considered.

2 Consumer Perceptions and Recent News

ICVDs are a popular commodity right now. But, how does the general public perceive these doorbells? What are the pros and cons of installing such a doorbell in one's home? In this section, I will discuss the pros and cons of ICVDs as expressed by consumers through surveys. Then, I will provide a sampling of high-impact news articles about ICVDs. Taken together, the findings in this section will provide helpful background information before I discuss privacy and ethical harms and legal concerns in the subsequent section.

2.1 Consumer Perceptions of Internet-Connected Video Doorbells

Despite the popularity of ICVDs, few publicly-available surveys provide insight into how users perceive these devices. Of the surveys that companies have conducted on ICVDs, one can still gain some general insights. One survey of 950 Amazon Ring owners in the U.S. showed that most respondents said "they were aware of hacks, but that benefits of Ring, like convenience and a sense of 'peace of mind,' outweighed security concerns" (Holmes, 2020). The same source cited affordability—popular ICVDs typically cost under $200 and do not require professional installation—as another benefit of ICVDs. Another survey of 1,500 Americans indicated that respondents generally felt safer with ICVDs, but 93% of respondents indicated that they would not purchase an ICVD if the company was collecting and selling their personal data (Covington, 2021). While not a result of a survey, some insurance companies offer discounts on homeowners insurance

for homes equipped with ICVDs (American Family Insurance, 2021). At a high level, Table 1 provides a summary of user perceptions of the pros and cons of ICVDs based on these findings.

Table 1: User-perceived pros and cons of ICVDs

Pros	**Cons**
Peace of mind / sense of security	Collecting/selling of personal data
Convenience	Potential for hacking
Affordability	
Insurance discounts	

Table 1 is certainly not exhaustive; but, given the rapid market growth of ICVDs, it follows that the list of benefits that users perceive would outweigh the list of cons. As the one survey found, consumers often find that the added convenience and peace of mind provided by ICVDs take precedence over any security or privacy concerns. Nevertheless, a montage of news stories from the past few years has shined a light on some of the potential drawbacks of ICVDs.

2.2 Recent News Stories of Internet-Connected Video Doorbells

News outlets strive to produce catchy, polarized content to attract and retain an audience. ICVDs are prime candidates for headline news due to their popularity and ability to create debate over privacy and security issues. On one side, proponents of ICVDs argue that the devices make places safer and, if used properly, only record video footage of places that are not considered private (*e.g.*, porches, public streets, and sidewalks). In contrast, others hold serious concerns for ICVDs with respect to privacy and the ethics involved in the use of captured video and audio of non-consenting persons. This type of debate makes great fodder for the news.

I have provided a listing below of news headlines regarding ICVDs in the U.S. going back to 2019, sorted in reverse chronological order. All of the articles come from well-respected outlets, and each of the headlines points to some ethical, privacy, legal, or security concern related to ICVDs. While there are many positive news articles in support of ICVDs, I have selectively chosen headlines for this list that raise the types of ethical, privacy, and legal concerns that form the focus of the rest of this report. The Amazon Ring features prominently in these headlines, which is likely due to its position as the current market leader as well as Ring's partnership with law enforcement agencies (this will be discussed in more detail later on). However, this does not mean that other ICVD products do not have similar concerns.

- "Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments" (Lyons, 2021)
- "Home-security cameras have become a fruitful resource for law enforcement — and a fatal risk" (Harwell, 2021)
- "Los Angeles police 'wanted Amazon Ring BLM protest footage'" (BBC News, 2021)
- "Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs" (Paul, 2020)
- "Nest Doorbell safety fears arise as Google Nest Hub shows stranger's cam" (Tambini, 2020)
- "Amazon's Ring logs every doorbell press and app action" (Kelion, 2020)
- "Your Doorbell Camera Spied on You. Now What?" (Chen, 2020)
- "Amazon's Ring could tighten privacy after accusations it shares data with Facebook" (Reichert, 2020)
- "Man Captured on Doorbell Camera Footage Confessing to Murder" (Fortin, 2020)
- "Police can keep video from Ring doorbells indefinitely, adding to privacy concerns" (Masunaga, 2019)
- "Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns" (Harwell, 2019) [1]

From these headlines spanning 2019 to 2021, one can catch a glimpse of how ICVDs are making their mark on society, as well as the variety of ethical, privacy, and legal concerns news outlets have brought before the public.

3 Ethical, Privacy, and Legal Considerations

The highlights of the previous section may appear inconsistent at first glance. While consumers have expressed concern over data sharing and the potential for hacking, the strong market growth of ICVDs indicates that, in general, consumers implicitly place more value on the convenience, sense of security, and affordability of ICVDs (Rao, 2018). Despite this inconsistency, ICVDs raise several ethical, privacy, and legal concerns that I will discuss in detail in this section.

[1] When compared to the first (most recent) article in this list, this headline provides an indication of how quickly Ring is gaining new partnerships with law enforcement agencies and fire departments.

3.1 Ethics: Belmont Principles

The Belmont Report, published in 1979 by the U.S. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, provides three key principles for ethical research involving human subjects: respect for persons, beneficence, and justice (The National Commission for the Protection of Human Subjects of & Biomedical and Behavioral Research, 1979). These three principles form a consistent, useful framework for evaluating the ethical considerations of not only proposed human subjects research projects, but also devices like ICVDs that collect, use, and store personal data.

Respect for persons involves two aspects: individuals should have autonomy and those with inhibited autonomy should be protected. Practically, autonomy means that participation is voluntary, participants comprehend what they are volunteering for, and participants are therefore able to give informed consent. This principle is relevant to ICVDs in two primary ways: 1) the amount and types of data that are collected and how those data are used by the company, and 2) the innocent passersby who are recorded without their explicit consent.

As with any Internet-connected technology, the company's privacy policy (and sometimes terms of service) plays a key role in any discussion of informed consent for the consumer. Every manufacturer of an ICVD will have an associated privacy policy that consumers must agree to in order to use the product. However, according to a 2019 Pew Research Center survey of Americans, 81% of respondents claimed they are asked to agree to at least one privacy policy each month, while only 22% of respondents claimed to "always" or "often" read the privacy policies they are presented with (Auxier et al., 2019). This implies that the majority of Americans agree to privacy policies without a true understanding of what data the company collects and how those data are used, shared, and potentially sold by the company. While consumers might consider much of the data ICVD manufacturers typically collect commonplace (*e.g.*, billing information and captured video recordings), sometimes manufacturers collect and use data in ways that many consumers may not anticipate. For instance, Ring will obtain "the geolocation of your mobile device if you consent to the collection of this data" and "information we obtain from third-party social media services (e.g., Facebook) or payment services (e.g., PayPal) if you choose to link to, create or log into your Ring account through these services (including when you share Ring videos or content via your social media account)" (Ring, 2021b). In short, Ring's smart phone application will track a user's location if the user consents to it, and anytime a user makes any connection between Ring and a social network, Ring can pull in information about the user from that social network. These statements come directly from Ring's privacy policy, which all Ring owners

implicitly agree to when they begin using the ICVD. However, one can argue that a long and often-unread privacy policy fails to provide the fully informed consent that the principle of respect for persons requires.

In addition to product consumers, respect for persons also applies to any passersby who are recorded by a consumer's ICVD. The privacy policies for ICVDs explicitly state that the consumer is responsible for ensuring they have a legal right to install and operate an ICVD at their residence, and in some cases signage may be required to notify the public that an ICVD is operating in the vicinity. However, even if signage is provided (and this is not a typical requirement), most passersby will have no recourse to prevent being recorded. For instance, ICVDs may capture vehicles that drive by, neighbors that live next door or walk down the street (including children), and package deliverers. In these cases the person(s) involved would have no choice but to be recorded. It is also important to consider the blind and those with poor eyesight who, even with signage, would be unaware that they are being recorded. In some cases, conscious persons may see signage or become aware of ICVDs in the vicinity and have the ability to take a different route; but, these cases are exceptional. Ultimately, the ability of ICVDs to record people in public places without their consent and sometimes even without their awareness of being recorded goes against the respect for persons principle. These people are not consenting to be recorded, and they have no recourse (in most cases) to prevent being recorded by someone's ICVD.

The second principle from the Belmont Report is beneficence. Beneficence involves not causing harm, and maximizing the benefit to participants and society as a whole while minimizing potential risks. As previously discussed, surveyed respondents generally listed convenience, affordability, and a sense of security as the key benefits for ICVDs. This is unsurprising because these are exactly the benefits that ICVD manufacturers are aiming to provide to their customers. However, the manufacturers' collection and handling of user data may undermine the aspect of minimizing potential risks to the users. In particular, when manufacturers collect data that are unnecessary for the operation of the product (*e.g.*, collecting GPS data from users' smartphones) and share or sell those data with third parties for analytical, advertising or other reasons, the potential risks for the users begin to amass. Moreover, any IoT device has the potential to be hacked, which exacerbates the risk of extraneous data collection (*i.e.*, not only might user data be shared with third parties for ostensibly legitimate purposes, but nefarious hackers may obtain the data for decidedly illicit purposes, such as extortion or blackmail). For ICVDs, which capture video footage and sometimes audio recordings, it is therefore imperative that strong security systems are in place, both at the device level as well as at the content storage level (*i.e.*, in the cloud).

The final principle from the Belmont Report is justice. Justice focuses on fair procedures and selection of subjects, along with understanding who stands to benefit the most and who stands to lose the most. One application of the justice principle with respect to ICVDs is to consider who is "left out" of the ICVD market. While ICVDs are not grossly expensive, they are out of the price range for people with little disposable income. As a result, it is likely that affluent populations will install significantly more ICVDs than low-income populations. Ironically, the affluent populations generally have less need for a "sense of security" than those living in impoverished, underserved areas. Another aspect of justice to consider is how the ICVD manufacturers may use the data that are captured and stored. For instance, will the manufacturer use the data solely to improve the product (which benefits both the manufacturer and the user), or will the data be shared, sold, or used in ways that benefit the manufacturer disproportionately more than the user. Another aspect that relates to justice is the possibility for ICVD manufacturers to implement facial recognition algorithms into their products. This will be discussed at length in a subsequent section, but here it is worth briefly noting that research has shown that facial recognition algorithms perform disproportionately worse on people with darker skin tones than on lighter-skinned individuals. Moreover, facial recognition systems have been found to perform best on White men and worst on Black women. In a situation where an ICVD has a feature to alert the homeowner to a suspicious-looking person at the front door, one can easily envision a situation where minorities and traditionally-marginalized groups may be disproportionately classified as "suspicious" by the algorithm. Such a situation would cause unjust harm to these individuals.

The Belmont principles of respect for persons, beneficence, and justice provide a good framework for analyzing the merits and drawbacks of ICVDs. Another framework that proves useful for this purpose is the matrix of domination.

3.2 Ethics: Matrix of Domination

The matrix of domination is a sociological construct based on the idea that race, class, gender, ethnicity, and other categories used to ostracize groups of people are "interlocking systems of oppression," rather than stand-alone systems that act in a vacuum relative to each other (Collins, 1990). In this construct, a White woman might be seen as privileged due to her skin tone, yet oppressed due to her gender. With respect to the matrix of domination, facial recognition technology and law enforcement's use of ICVD footage are central concerns that will be discussed in this section.

There are concerns that the use of ICVDs to flag suspicious-looking individuals, or for law enforcement to use ICVDs with embedded or third-party facial-recognition algorithms, would exacerbate the marginalization of minorities and under-privileged groups. For instance, Ring provides the Neighbors app, in which Ring customers can notify people in their neighborhood of suspicious-looking individuals (Ring, 2021a). On one hand, this is a feature that could drive down crime in a neighborhood outfitted with numerous ICVDs. On the other hand, one can imagine a situation where minorities, or even poorly-dressed individuals become the subjects of these postings for no reason other than walking through a neighborhood in which they are viewed as suspicious. Moreover, in these cases it is likely that police would be called in to interrogate these individuals to ensure they mean no harm. It is not difficult to see, given the history of law enforcement with minorities in the United States, how such situations could escalate quickly.

Ring is currently partnered with over 2,000 police and fire departments across 48 states (Lyons, 2021). Using Ring's Neighborhood app, users can submit content recorded on their Ring ICVDs directly to law enforcement agencies either voluntarily or in response to a request by an agency (for instance, if the police believe an ICVD may have captured footage of a crime or suspected criminal). As the tagline of a 2019 article from Vice stated, "Neighbors, a social media crime-reporting app owned by Amazon, creates a digital ecosystem in which you are encouraged to assume the worst about your neighbors—and people of color are once again being harmed" (Haskins, 2019). The article goes on to discuss how such platforms can perpetuate racism by creating an environment in which minority neighbors are virtually ostracized, racist descriptions are posted, and video posts of suspicious persons most commonly contain people of color. One high-profile instance of the controversial relationship that law enforcement has with Ring ICVD owners is when the Los Angeles police department (LAPD) was found to have requested video footage of Black Lives Matter (BLM) protests against police violence that occurred during 2020 (BBC News, 2021). This stands as a particular instance of surveillance against predominantly colored individuals exercising their right as citizens to peacefully protest. (While it is true that some BLM protests resulted in violence and destruction of property, the vast majority of the protests were peaceful in nature (Mansoor, 2020).)

The next section will take this discussion a step further to discuss the potential ethical and privacy harms with the use of facial recognition algorithms.

3.3 Ethics and Privacy: Facial Recognition Algorithms

Buolamwini and others have produced a body of research demonstrating the shortcomings of facial recognition algorithms (see, for example, (Buolamwini & Gebru, 2018; Cavazos, Phillips, Castillo, & O'Toole, 2021; Raji et al., 2020)). These algorithms present an important concern for ICVDs due to the relative ease with which technology companies (especially the likes of Amazon and Google) can incorporate such algorithms into their ICVDs. Currently, popular ICVDs like the Nest Hello ICVD (associated with Google) and the Kami Doorbell Camera incorporate facial recognition technology (Kami, 2021; Nest, 2021). However, Ring filed a patent in 2018 that was approved in January 2021 for facial recognition technology (Siminoff, 2021). This indicates that such technology may soon be available for Ring doorbells as well.

As previously discussed, the ethical concerns with facial recognition algorithms are manifold. A documentary entitled "Coded Bias" was recently produced that talks about these issues in detail (*CODED BIAS*, 2020). In particular, the documentary follows Buolamwini's discovery that facial recognition algorithms are biased against women and people of color, and her push for the first United States legislation to combat algorithmic bias. Part of the documentary tracks law enforcement use of facial recognition technology in the United Kingdom, where people are misidentified by the algorithm as threats or terrorists, confronted by law enforcement in public, interrogated, and eventually released. This type of scenario could play out anywhere facial recognition algorithms are deployed by law enforcement. This is a key reason underlying the uproar that privacy and ethics advocates have raised in response to Ring's partnership with over 2,000 police and fire departments in the United States.

A recent New York Times article entitled "Your Face Is Not Your Own" discusses potential misuses of facial recognition technology while providing an exposé of ClearView AI, an American company that provides propriety facial recognition technology to private companies and law enforcement agencies (Hill, 2021). At one point the article states, "[Facial recognition technology] could galvanize countless name-and-shame campaigns, allow the police to identify protesters and generally eliminate the comfort that comes from being anonymous as you move through the world." These are serious ethical concerns that American society is currently wrestling with in the case of ICVDs as well as other video-recording technologies.

Analyzing ICVDs through the ethical lenses of the Belmont principles, the matrix of domination, and concerns around facial-recognition algorithms uncovers a range of ethical and privacy quandaries for this technology. However, in addition to ethical concerns and the privacy concerns brought about by facial-recognition technology, ICVDs raise a number of other privacy issues as well.

3.4 Privacy: Solove's Taxonomy of Privacy Harms

ICVDs pose a variety of privacy issues that will be explored in this section using Solove's Taxonomy of Privacy Harms. Solove's Taxonomy, created by leading privacy researcher Daniel J. Solove, provides a concise and practical framework that focuses on "specific activities that pose privacy problems" (Solove, 2006, pg. 482). The taxonomy consists of four primary components—information collection, information processing, information dissemination, and invasion—that each contain specific forms of privacy harm that may occur (see Figure 1). The four primary components will be applied to ICVDs in turn.

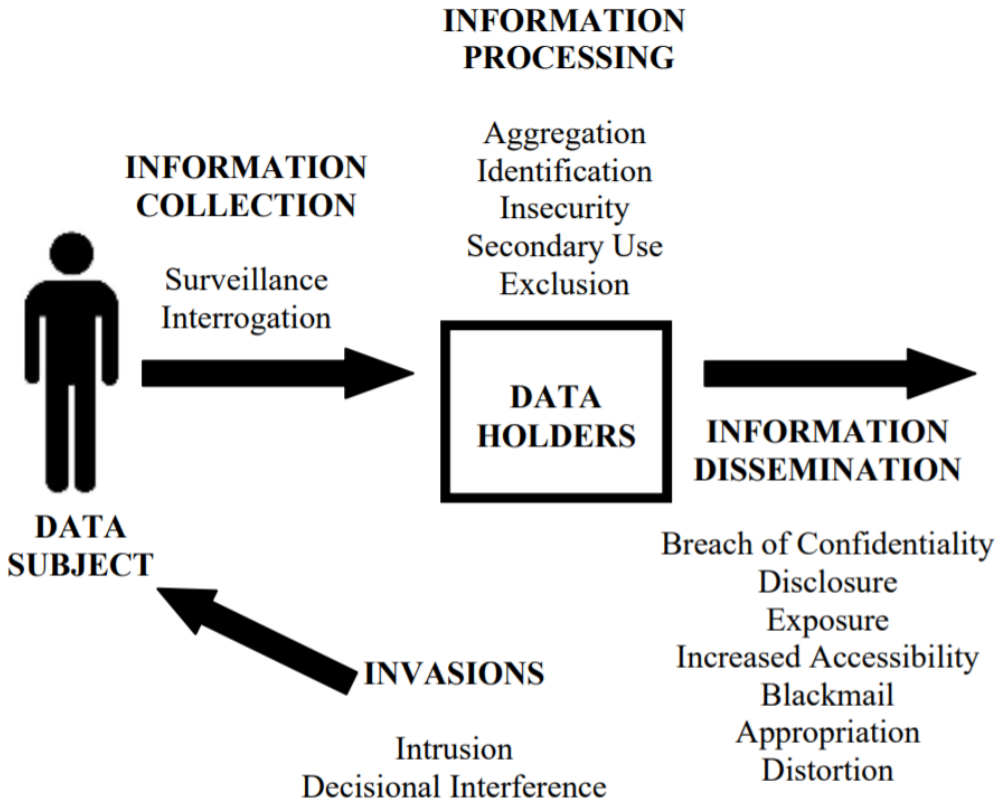

Figure 1: Visual depiction of Solove's Taxonomy of Privacy Harms (source: Solove, 2006)

Information collection, the first of the primary components of Solove's Taxonomy, contains privacy harms associated with surveillance and interrogation. While interrogation is not an obvious privacy harm for ICVDs, surveillance clearly is. According to Solove, surveillance is "the watching, listening to, or recording of an individual's activities," which is exactly what ICVDs do (Solove, 2006, pg. 490). Indeed, the provided news headlines and previous discussion on the ethics of ICVDs already covered surveillance concerns in some detail. As a refresher, thousands of police and fire departments are now partnered with Ring in an effort to

make neighborhoods safer. Despite the apparent altruism of these partnerships, one glaring outcome is that law enforcement agencies are given access to a vast network of video footage which, among other things, could be used to surveil certain populations. This, in fact, has already occurred with the LAPD attempting to access Ring doorbell footage of the 2020 BLM protests. Beyond law enforcement's use of ICVD footage for potential surveillance, there are also concerns that programs such as Ring's Neighbors app could create a sort of virtual "Neighborhood Watch." One 2018 article from the British Journal of Criminology argues that this type of surveillance encourages stigmatization, ethnic profiling, and excessive social control, especially for safer, more affluent neighborhoods" (Lub, 2017).

The next primary component of the Taxonomy, information processing, includes aggregation, identification, insecurity, secondary use, and exclusion. All five of these privacy harms apply to ICVDs. Aggregation, or the act of combining disparate data sources together in order to create a more complete "picture," is a serious privacy threat for ICVDs on multiple levels. First, ICVD manufacturers have the ability to gather and potentially aggregate vast amounts of information on their users from web and smartphone apps, connected social media accounts, as well as the footage collected from the ICVD itself (some of this was previously discussed). But, another aggregation harm exists in the potential for neighborhoods or law enforcement to have ICVD footage aggregated in the name of safer communities. This means that personal ICVD footage from multiple households could potentially be viewed and analyzed by multiple people, for no reason at all other than to "keep the peace." With law enforcement agencies already partnering with Ring, in some instances this may already be the case. Identification is a related concern that involves not only collected personal information on ICVD users (*e.g.*, from purchases and linked social media accounts), but also the ability for facial recognition algorithms to identify people that walk through an ICVD's camera view. Insecurity is a privacy harm that applies to any IoT device, because the device itself is susceptible to hacking. Hacked information and security vulnerabilities are not uncommon for ICVDs, and the problem is intensified by the type of data hackers could potentially obtain (Wroclawski, 2019). For example, video and audio footage of one's family and neighbors could be compromised. Finally, secondary use and exclusion are potential privacy harms as well that relate more to an ICVD manufacturer's use of user data. Secondary use might involve the manufacturer using collected data for research purposes or for sharing with targeted advertisers without the user providing informed consent. Although related to secondary use, exclusion occurs when a person is unable to find out what personal data has been recorded, how those data are being used, or when the person has no recourse to edit or amend incorrect information. Generally, ICVD manufacturers collect vast amounts of data from their users, including purchasing data, installation and location specifics for the

ICVD, as well as data collected from web and smartphone apps. If ICVD consumers are not provided with proper notification of the specific types of information collected on them, exclusion becomes an issue.

The third primary component is information dissemination, which contains seven distinct privacy harms that "all involve the spreading or transfer of personal data or the threat to do so" (Solove, 2006, pg. 491). In this case, rather than stepping through each of the privacy harms individually, the information dissemination harms will be considered collectively. It is again not only the amount of data collected on the ICVD consumers and passersby, but the types of data that makes information dissemination an important category of privacy harm for ICVDs. On the consumer side, purchasing data, installation location data, as well as audio and video of the home's inhabitants are all data types that, if compromised or transferred without the informed consent of the consumer, could cause serious harm by way of breach of confidentiality, disclosure (of truthful information about a person that said person does not want disclosed), exposure ("revealing another's nudity, grief, or bodily functions"), and blackmail (Solove, 2006, pg. 491). On the other hand, disclosure, exposure, and blackmail all apply to passersby who are captured in audio and video recordings as well. In brief, most of the data collected by ICVDs pose serious information dissemination privacy harms for both the ICVD consumers and those who are recorded by others' ICVDs without their consent.

The last primary component of Solove's Taxonomy, invasions, includes intrusion and decisional interference. According to Solove, intrusions are acts that "disturb one's tranquility or solitude," and decisional interference "involves the government's incursion into the data subject's decisions regarding her private affairs" (Solove, 2006, pg. 491). ICVDs can present intrusion harms by their susceptibility to hackers gaining access to the ICVD and viewing and talking through your ICVD (this is related to the insecurity privacy harm) as well as by recording audio and video of passersby (and perhaps even the household's inhabitants) who do not wish to be recorded. Both of these instances represent intrusions into one's privacy. For decisional interference, Solove's construct involves the government interfering in one's decisions and private life. A prime example of this privacy harm is law enforcement's use of ICVD data either via partnerships with ICVD manufacturers or through obtaining footage to surveil populations (such as the LAPD's request to obtain Ring ICVD footage of the BLM protests). This example is related to the concept of surveillance, but the government's central role and the impact it may have on the actions and decisions one makes while under surveillance allow this example to be categorized as a decisional interference harm as well.

Solove's Taxonomy provides a concise and practical means to evaluate privacy harms for ICVDs. By using this framework, a variety of distinct privacy harms were identified. In the following subsection, the

discussion moves away from privacy in order to provide a glimpse into the legal environment in which ICVDs operate.

3.5 Legal: Existing Regulations

Along with ethical and privacy considerations, ICVDs are interesting to analyze from a legal perspective. As one article states, "A patchwork of federal, state, county, and local laws controls video and audio recording. Federal law is generally silent on the matter of video surveillance, instead addressing audio eavesdropping and surveillance" (Wallender, 2019). What does this mean for ICVDs?

The guiding principle regarding the legality of home *video* recording is to look for an infraction against reasonable expectation of privacy. A 2018 summary report from the National Association of Realtors (NAR) claims that most states that "criminalize nonconsensual videotaping of a person require that the person be in an area in which that person has a reasonable expectation of privacy," such as in their home (*State Audio and Visual Surveillance Laws*, 2018, pg. ii). In general, this means that video recording from ICVDs does not pose legal concerns because the ICVD is nearly always capturing footage of property where no privacy should be expected (*e.g.*, public sidewalks and streets and home entryways). The report also notes that Alaska, Arizona, the District of Columbia, Florida, and New York exempt video security surveillance systems from their video recording laws, but only if proper signage is provided to inform passersby that they are being recorded. This is a likely explanation for why the privacy policies for Ring and SimpliSafe explicitly note that users may need to provide proper signage in their homes to comply with applicable laws (Ring, 2021b; SimpliSafe, 2021a). Outside of Federal and State laws, homeowners associations (HOAs) may also have specific requirements regarding ICVDs; but, these requirements would be HOA-specific.

Another aspect of video recording from ICVDs is the collection of biometric data (*i.e.*, data related to human features, such as facial contours and fingerprints), especially in the use of facial recognition algorithms. In 2008 Illinois passed its Biometric Information Privacy Act (BIPA) to regulate the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information" (*Biometric Information Privacy Act*, 2008) Illinois was the first state to pass this type of law, but since then other states have been following suit, including Texas, Washington, California, New York, and Arkansas. Over 200 BIPA lawsuits were filed in 2018 and 2019, which is suggestive of the impacts these laws are having on the biometrics industry (Prescott, 2020). In 2020, a class-action lawsuit that invoked the Illinois BIPA was brought against Ring. The lawsuit claims that Ring broke privacy laws by collecting biometric data (in

this case, facial features) without consent and sharing the data with the police (White, 2020). Ring asserts that it does not use facial recognition technology and also does not share or sell facial recognition technology to law enforcement; but, there are other ICVD manufacturers that are currently using facial recognition technology (Ring, 2020b). As more ICVDs begin using facial recognition technology, one can only expect a steady stream of BIPA lawsuits to follow.

While video recording is generally not of legal concern for ICVDs, *audio* recording can be. RecordingLaw.com provides a map summarizing the consent requirements for call recording in the United States (see Figure 2) (*United States Recording Laws*, 2020). While there are some exceptions, 12 states[2] require all parties in the communication to consent to having audio recorded, and the remaining 39 states (including the District of Columbia) require single-party consent. According to the NAR report, in the 39 states requiring single-party consent, the requirement is generally met if the person recording the audio is part of the conversation or if one person in the conversation had previously consented to the recording (*State Audio and Visual Surveillance Laws*, 2018).

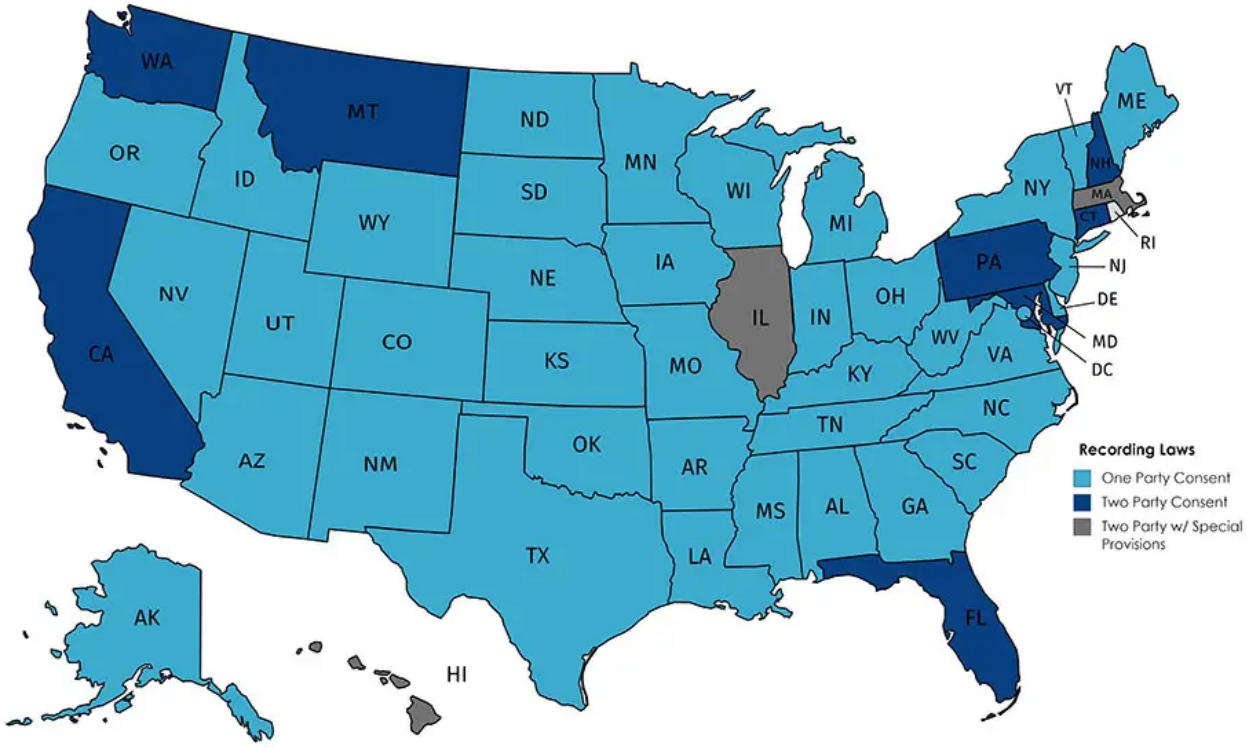

Figure 2: Summary map of legal audio recording consent requirements by state in 2018 (source: *United States Recording Laws*, 2020)

[2]This includes Michigan and Oregon, which RecordingLaw.com listed as "One Party Consent" states to err on the side of caution due to the special provisions in these states.

One recent legal challenge to ICVD audio recordings came from New Hampshire, where a prosecutor asked a judge to admit audio recording evidence from a Ring doorbell in a case involving two brothers, one of which shot the other in the arm with a gun. The defendant's public defender argued that such recordings violate the state's wiretapping law, and therefore should not be admissible as evidence (Feathers, 2020). However, the judge ruled against this argument, ultimately allowing recorded audio from a Ring doorbell to be used as evidence because it did not, in the judge's opinion, violate the state's wiretapping law (Haas, 2020).

In summary, the legal framework that regulates ICVDs is composed of at least three main parts: video data regulation, audio data regulation, and biometric data regulation. Each of these parts is distinct from the others, and as is the case with most advanced technologies, the law is trying to catch up with the rapidly-evolving ICVD market to ensure privacy rights are properly protected.

4 Recommendations

The previous section contained ethical, privacy, and legal analyses of ICVDs, in which a variety of concerns were uncovered. This section will provide suggestions for mitigating some of the key concerns, and also discuss how an existing framework for measuring consumer privacy and security can be applied to ICVDs.

4.1 Mitigating Identified Concerns

Table 2 provides a summary of the key ethical, privacy, and legal concerns that were discussed in the previous section.

Table 2: Summary of ethical, privacy, and legal concerns for ICVDs

Ethical	**Privacy**	**Legal**
Facial recognition algorithms and BIPA laws		
Lack of truly informed consent for consumers / Secondary use of collected data		Audio collection / wiretapping laws
No/minimal recourse for passersby (especially the visually-impaired)	Surveillance	Video recording
Collection of unnecessary data	Data aggregation (leading to potential identification)	Signage requirements
Collection of personal content	Data security	
Low-income may be "left out"	Information dissemination	
Law enforcement partnerships	Intrusion / hacking	

There are a variety of concerns expressed in Table 2. However, many of these concerns may be lessened or mitigated, if they are acknowledged and properly addressed. Following is a list of recommendations, each of which addresses one or more of the concerns listed in Table 2.

Forego facial recognition technology. Current facial recognition algorithms are flawed, and their use in ICVDs could disproportionately harm minorities. Moreover, these algorithms are essentially unregulated right now, both in their implementation and potential use (*e.g.*, for law enforcement purposes). Facial recognition also involves collecting and storing peoples' "faceprints," which are valuable pieces of identifying data that could be compromised by hackers. Currently, the benefit to consumers of being able to know exactly which family member or neighbor is at their door based on facial recognition algorithms is far outweighed by the plethora of potential harms to individuals and broader communities that these algorithms propagate. Until the algorithms are improved, robust safeguards are established, and laws are in place (*e.g.*, BIPA laws) to effectively regulate the use of facial recognition technology, ICVDs should not provide this feature.

Better inform consumers. All ICVD manufacturers have a privacy policy that consumers agree to prior to using the ICVD. However, in many cases these policies detail how companies collect large amounts of extraneous data, share or sell consumer data to third-parties, use opt-out rather than opt-in policies, and/or have no data retention policy. One might argue that these policies do not elicit truly informed consent from the consumer. Given the amount and types of data collected by ICVDs, ICVD manufacturers should establish procedures to better ensure consumers know what data are being collected and how those data are being used. This might be achieved by providing timely pop-up information/consent windows, or even providing a short test at the end of the privacy policy to ensure consumers understand key points they are agreeing to.

Minimize data collection. An important tenet of data privacy is to minimize data collection, only collecting what is actually required for your device or service to function properly. Between the ICVD manufacturers and the ICVDs themselves, vast amounts of personal, private data are collected. ICVD manufacturers would do well to limit how much data they collect and store, as well as how long they store those data, especially given the large number of ICVDs that have already been hacked.

Give consumers control over their data. The Digital Standard conducted a study of 24 ICVDs in 2020 and found that many of the manufacturers did not provide consumers with a means to request and see their data, or even a means to have their data deleted (**?**). These are important controls that ICVD manufacturers should be providing to their consumers.

Secure the data well. The 2020 Digital Standard study also found that most ICVDs they tested lacked two-factor authentication at the time; but, five of the 11 ICVD manufacturers who did not provide two-factor authentication indicated that by the end of 2020 their ICVDs would have this feature (**?**). Nevertheless, two-factor authentication is a security feature that should have been widely adopted by 2020. Given the amount and types of data collected by ICVD manufacturers, as well as the hacks that have already occurred on ICVDs, ICVD manufacturers must keep their security practices updated.

Maintain well-trained staff. Employees of ICVD manufacturers who have access to consumer data should be trained, not only on the requisite privacy laws, but on good privacy and ethical practices. Additionally, part of this training should explicitly educate employees on the dangers that data aggregation poses to the ICVD consumers.

Establish community guidelines. For ICVD manufacturers that provide a neighborhood-connection app (*e.g.*, Neighbors for the Ring ICVD), strong community guidelines and moderation must be established to prevent ostracism, racial profiling, and other related injustices.

Limit law enforcement's reach. Ring is currently partnered with over 2,000 law enforcement agencies and fire departments. This creates the possibility for a network of ICVDs that may be surveilled in real time, at any time. Therefore, it is imperative that ICVD manufacturers that engage with law enforcement agencies have proper policies in place to prevent overreach by law enforcement agencies (*e.g.*, the LAPD requesting Ring video footage of the BLM protests).

Evaluate using The Digital Standard. The Digital Standard provides a testing framework to evaluate Internet-connected products (and the manufacturers that produce them) in four categories: security, privacy, ownership, and governance. ICVD manufacturers should avail themselves of this framework, or others like it, to help ensure their products meet high-level security, privacy, ownership, and governance standards.

The following section will provide more detail on The Digital Standard, and what aspects the framework evaluates.

4.2 The Digital Standard

The Digital Standard is an open-source, "community-led effort to build a framework to test and rate products and services on the basis of privacy, security, and data practices" that was originally developed by Consumer Reports and other agencies (TheDigitalStandard, 2021). Table 3 provides a listing of the high-level types of

evaluations The Digital Standard currently provides (most of the categories listed in Table 3 contain multiple sub-evaluations).

Table 3: The Digital Standard v1.2.1 Evaluation Categories

Security	**Privacy**	**Ownership**	**Governance**
- Build quality	- Access and control	- Ownership	- Business model
- Data security	- Data use and sharing	- Permanence	- Human rights and corporate social responsibility
- User Safety	- Data retention	- Right to repair	- Open
	- Overreach		- Privacy policy and terms of service
			- Transparency

Given this framework's emphasis on privacy and security specifically for IoT devices, it represents an ideal evaluation template for ICVDs. In fact, The Digital Standard provides a case study on ICVDs that was conducted in 2020. This case study evaluated 24 ICVDs from 16 manufacturers on build quality, data security, access and control, data use and sharing, and transparency (**?**). Highlights from the case study include: 1) ICVDs from Eufy, GoControl, LaView, and Netvue had severe security vulnerabilities; 2) Most doorbells lacked two-factor authentication; and 3) Most manufacturers collected more data than they needed, did not provide users control over their data, and did not provide a data retention policy (Wroclawski, 2020).

The findings from this case study provide evidence that The Digital Standard can be effectively applied to ICVDs. Moreover, because The Digital Standard is affiliated with Consumer Reports, case studies like the one from 2020 are likely to be published and widely disseminated, which can incentivize ICVD manufacturers to employ better data privacy and security practices.

5 Conclusion

Internet-connected video doorbells (ICVDs) are popular commodities in the U.S. Roughly 20 million households have already installed one, and the market for ICVDs continues to grow. While these devices are popular for their ease of use, affordability, and the peace of mind they provide, ICVDs have also been the subject of a variety of high-profile news articles over the past few years that collectively highlight their ethical, privacy, and security concerns.

ICVDs were analyzed according to the Belmont Principles, the Matrix of Domination, and Solove's Taxonomy of Privacy Harms. Additionally, existing laws regulating ICVDs were discussed, and special

consideration was given to the use of facial recognition algorithms in ICVDs. Analyzing ICVDs in these ways uncovered a variety of concerns, including collecting too much data, sharing data with third parties, surveillance, security, facial recognition implications, and law enforcement partnerships (see Table 2 for a more complete summary).

After understanding the concerns regarding ICVDs, specific recommendations were made to mitigate some of these concerns. Key recommendations include foregoing facial recognition technology, minimizing data collection, ensuring consumers provide actual informed consent, and giving consumers control over their data. Finally, The Digital Standard, a framework for assessing a product's level of data privacy and security, was discussed. In particular, highlights from a case study conducted by Consumer Reports in 2020 that used The Digital Standard on ICVDs were discussed.

There are myriad ethical, privacy, and legal concerns associated with ICVDs. But, this does not mean that ICVDs are inherently "bad" products that should be banned from the market. Rather, this means that it is incumbent (ethically, if not legally) upon ICVD manufacturers to do everything in their power to protect their users' privacy and ensure their products are not being used in unethical ways. Moreover, lawmakers must work to ensure a proper legal framework is established and frequently updated to govern the use of these devices in a way that protects the rights of citizens while simultaneously allowing ICVD manufacturers to remain in business.

References

ABI Research. (2012, November). *1.5 Million Home Automation Systems Installed in the US This Year.* Retrieved 2021-04-15, from https://www.abiresearch.com/press/15-million-home-automation-systems-installed-in-th/

American Family Insurance. (2021). *Safe, Secure, Smart Home Discount.* Retrieved 2021-04-15, from https://www.amfam.com/insurance/home/discounts/safe-secure-smart-home-discount

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November). *4. Americans' attitudes and experiences with privacy policies and laws.* Retrieved 2021-02-19, from https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/

BBC News. (2021, February). Los Angeles police 'wanted Amazon Ring BLM protest footage'. *BBC News*. Retrieved 2021-04-15, from https://www.bbc.com/news/technology-56099167

Biometric Information Privacy Act. (2008, October). Retrieved 2021-04-15, from https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Buolamwini, J., & Gebru, T. (2018, 23–24 Feb). Gender shades: Intersectional accuracy disparities in commercial gender classification. In S. A. Friedler & C. Wilson (Eds.), *Proceedings of the 1st conference on fairness, accountability and transparency* (Vol. 81, pp. 77–91). New York, NY, USA: PMLR. Retrieved from http://proceedings.mlr.press/v81/buolamwini18a.html

Business Wire. (2020, February). *Amazon's Ring Leads Google's Nest As 16% Of US Homes Adopt Video Doorbells: Strategy Analytics.* Retrieved 2021-04-15, from https://www.businesswire.com/news/home/20200213005824/en/Amazon%E2%80%99s-Ring-Leads-Google%E2%80%99s-Nest-As-16-Of-US-Homes-Adopt-Video-Doorbells-Strategy-Analytics

Cavazos, J. G., Phillips, P. J., Castillo, C. D., & O'Toole, A. J. (2021). Accuracy comparison across face recognition algorithms: Where are we on measuring race bias? *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *3*(1), 101-111. doi: 10.1109/TBIOM.2020.3027269

Chen, B. X. (2020, February). Your Doorbell Camera Spied on You. Now What? *The New York Times*. Retrieved 2021-04-15, from https://www.nytimes.com/2020/02/19/technology/personaltech/ring-doorbell-camera-spying.html

CODED BIAS. (2020). Retrieved 2021-04-15, from https://www.codedbias.com

Collins, P. H. (1990). Black Feminist Thought in the Matrix of Domination. In *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment* (pp. 221–238). Boston: Unwin Hyman. Retrieved 2021-04-15, from http://www.hartford-hwp.com/archives/45a/252.html

Covington, T. (2021, April). *Ring the Alarm: 87% of Americans Don't Know How Their Doorbell Camera Data Is Being Used.* Retrieved 2021-04-15, from https://www.thezebra.com/resources/home/doorbell-camera-survey/

Feathers, T. (2020, January). *Do Ring Cameras Violate Wiretapping Laws? New Hampshire Is About to Find Out.* Retrieved 2021-04-15, from https://www.vice.com/en/article/3a8k79/do-ring-cameras-violate-wiretapping-laws-new-hampshire-is-about-to-find-out

Fortin, J. (2020, January). Man Captured on Doorbell Camera Footage Confessing to Murder. *The New York Times*. Retrieved 2021-04-15, from https://www.nytimes.com/2020/01/02/us/Michael-Egwuagu-confession-doorbell-camera.html

Haas, K. (2020, March). Judge: Audio from Ring doorbell can be used as evidence in Rochester shooting case. *Union Leader*. Retrieved 2021-04-15, from https://www.unionleader.com/news/crime/judge-audio-from-ring-doorbell-can-be-used-as-evidence-in-rochester-shooting-case/article_ee1ddcd1-b193-5ec9-ad9b-08c22fbcdc2f.html

Harwell, D. (2019, August). Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns. *The Washington Post*. Retrieved 2021-04-15, from https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/

Harwell, D. (2021, March). Home-security cameras have become a fruitful resource for law enforcement — and a fatal risk. *The Washington Post*. Retrieved 2021-04-15, from https://www.washingtonpost.com/technology/2021/03/02/ring-camera-fears/

Haskins, C. (2019, February). *Amazon's Home Security Company Is Turning Everyone Into Cops.* Retrieved 2021-04-15, from https://www.vice.com/en/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops

Hill, K. (2021, March). Your Face is Not Your Own. *The New York Times*. Retrieved 2021-04-15, from https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html

Holmes, A. (2020, January). *We Surveyed Hundreds of Amazon Ring Owners: Here Are 4 Takeaways.* Retrieved 2021-04-15, from https://www.businessinsider.com/amazon-ring-owners-survey-4-takeaways-2020-1

Kami. (2021). *Kami Doorbell Camera.* Retrieved 2021-04-15, from https://kamihome.com/kami-doorbell/

Kelion, L. (2020, March). Amazon's Ring logs every doorbell press and app action. *BBC News*. Retrieved 2021-04-15, from https://www.bbc.com/news/technology-51709247

Lub, V. (2017, October). Neighbourhood Watch: Mechanisms and Moral Implications. *The British Journal of Criminology*, *58*(4), 906–924. Retrieved 2021-04-15, from https://doi.org/10.1093/bjc/azx058 doi: 10.1093/bjc/azx058

Lyons, K. (2021, January). *Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments.* Retrieved 2021-04-15, from https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras

Mansoor, S. (2020, September). *93% of Black Lives Matter Protests Have Been Peaceful, New Report Finds.* Retrieved 2021-04-15, from https://time.com/5886348/report-peaceful-protests/

Masunaga, S. (2019, November). Police can keep video from Ring doorbells indefinitely, adding to privacy concerns. *Los Angeles Times*. Retrieved 2021-04-15, from https://www.latimes.com/business/story/2019-11-20/ring-doorbell-video-data-privacy (Section: Business)

Navigant Consulting, Inc. (2019, December). *Energy Savings Forecast of Solid-State Lighting in General Illumination Applications* (Tech. Rep.). Washington, D.C.: U.S. Department of Energy: Office of Energy Efficiency & Renewable Energy. Retrieved 2021-04-14, from https://www.energy.gov/sites/prod/files/2020/02/f72/2019_ssl-energy-savings-forecast.pdf

Nest. (2021). *Nest Hello.* Retrieved 2021-04-15, from https://store.google.com/null

NPR, & Edison Research. (2020, April). *The Smart Audio Report* (Tech. Rep.). Retrieved 2021-02-18, from https://www.nationalpublicmedia.com/uploads/2020/04/The-Smart-Audio-Report_Spring-2020.pdf

Paul, K. (2020, December). *Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs.* Retrieved 2021-04-15, from http://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats (Section: Technology)

Prescott, N. A. (2020, January). *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020.* Retrieved 2021-04-15, from https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020

Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2020). Saving face: Investigating the ethical concerns of facial recognition auditing. In *Proceedings of the aaai/acm conference on ai, ethics, and society* (p. 145–151). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3375627.3375820 doi: 10.1145/3375627.3375820

Rao, S. (2018, September). In today's homes, consumers are willing to sacrifice privacy for convenience. *Washington Post*. Retrieved 2021-02-19, from https://www.washingtonpost.com/lifestyle/style/in-todays-homes-consumers-are-willing-to-sacrifice-privacy-for-convenience/2018/09/11/5f951b4a-a241-11e8-93e3-24d1703d2a7a_story.html

Reichert, C. (2020, February). *Amazon's Ring could tighten privacy after accusations it shares data with Facebook.* Retrieved 2021-04-15, from https://www.cnet.com/home/smart-home/amazons-ring-to-tighten-privacy-after-accusations-it-shares-data-with-facebook/

Ring. (2020a, May). *The Original Ring Video Doorbell, Reimagined – The Ring Blog.* Retrieved 2021-04-15, from https://blog.ring.com/2020/05/06/the-original-ring-video-doorbell-reimagined/

Ring. (2020b, August). *Ring's Stance on Facial Recognition Technology.* Retrieved 2021-04-15, from https://blog.ring.com/about-ring/rings-stance-on-facial-recognition-technology/

Ring. (2020c). *Video Doorbell: 2020 Release.* Retrieved 2021-04-15, from https://ring.com/products/video-doorbell-v2

Ring. (2021a). *Neighbors App by Ring | Real-Time Crime & Safety Alerts.* Retrieved 2021-04-15, from https://ring.com/neighbors

Ring. (2021b, February). *Privacy Notice.* Retrieved 2021-04-15, from https://ring.com/privacy-notice

Siminoff, J. (2021, January). *Generating composite images using audio/video recording and communication devices* (No. US10885396B2). Retrieved 2021-04-15, from https://patents.google.com/patent/US10885396B2/en

SimpliSafe. (2021a, March). *SimpliSafe Privacy Policy.* Retrieved 2021-04-16, from https://simplisafe.com/privacy

SimpliSafe. (2021b). *Video Doorbell Pro.* Retrieved 2021-04-15, from https://simplisafe.com/video-doorbell-pro

Solove, D. J. (2006, January). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3). Retrieved 2021-02-10, from https://papers.ssrn.com/abstract=667622

State Audio and Visual Surveillance Laws (Tech. Rep.). (2018, October). National Association of Realtors. Retrieved 2021-04-14, from https://www.nar.realtor/sites/default/files/documents/2018-NAR%20Surveillance-Survey-Update.pdf

Tambini, O. (2020, May). *Nest Doorbell safety fears arise as Google Nest Hub shows stranger's cam.* Retrieved 2021-04-15, from https://www.techradar.com/news/nest-doorbell-safety-fears-arise-as-google-nest-hub-shows-strangers-cam

The National Commission for the Protection of Human Subjects of, & Biomedical and Behavioral Research. (1979, April). *The Belmont Report* (Final). Department of Health, Education, and Welfare. Retrieved 2021-04-15, from https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf

TheDigitalStandard. (2021, April). *TheDigitalStandard.* The Digital Standard. Retrieved 2021-04-15, from https://github.com/TheDigitalStandard/TheDigitalStandard (original-date: 2017-01-03T00:42:02Z)

United States Recording Laws. (2020, October). Retrieved 2021-04-15, from https://recordinglaw.com/united-states-recording-laws/

U.S. Census Bureau. (2020). *U.S. Census Bureau QuickFacts: United States.* Retrieved 2021-04-15, from https://www.census.gov/quickfacts/fact/table/US/VET605219

Verified Market Research. (2020, November). *Smart Home Market Worth $207.88 Billion, Globally, by 2027 at 13.52% CAGR: Verified Market Research.* Retrieved 2021-02-19, from https://www.prnewswire.com/news-releases/smart-home-market-worth--207-88-billion-globally-by-2027-at-13-52-cagr-verified-market-research-301165666.html

Wallender, L. (2019, November). *The Home Security Laws You Need to Know.* Retrieved 2021-04-15, from https://www.thespruce.com/home-security-laws-to-know-4767353 (Section: The Spruce)

Weinschenk, C. (2020, February). *Video Doorbell Research: Amazon Ring Tops in Market Share with 16% of Households Opting In - Telecompetitor.* Retrieved 2021-04-15, from https://www.telecompetitor.com/video-doorbell-research-amazon-ring-tops-in-market-share-with-16-of-households-opting-in/

White, B. (2020, September). *Ring Video Doorbells Class Action Alleges Privacy Law Violations.* Retrieved 2021-04-15, from https://topclassactions.com/lawsuit-settlements/privacy/ring-class-action-lawsuit-says-video-doorbells-violate-privacy-law/

Wroclawski, D. (2019, December). *3,000 Ring Doorbell and Camera Accounts May Be Vulnerable to Hackers.* Retrieved 2021-04-15, from https://www.consumerreports.org/hacking/ring-doorbell-accounts-may-be-vulnerable-to-hackers/

Wroclawski, D. (2020, August). *Data Security and Privacy Gaps Found in Video Doorbells by Consumer Reports' Tests.* Retrieved 2021-04-15, from https://www.consumerreports.org/video-doorbells/data-security-data-privacy-gaps-found-in-video-doorbells/