

Developing a Measure of Social, Ethical, and Legal Content for Intelligent Cognitive Assistants

Clovia Hamilton
SUNY Korea

William Swart
East Carolina University

Gerald M. Stokes
SUNY Korea

We address the issue of consumer privacy against the backdrop of the national priority of maintaining global leadership in artificial intelligence, the ongoing research in Artificial Cognitive Assistants, and the explosive growth in the development and application of Voice Activated Personal Assistants (VAPAs) such as Alexa and Siri, spurred on by the needs and opportunities arising out of the COVID-19 global pandemic. We first review the growth and associated legal issues of the of VAPAs in private homes, banks, healthcare, and education. We then summarize the policy guidelines for the development of VAPAs. Then, we classify these into five major categories with associated traits. We follow by developing a relative importance weight for each of the traits and categories; and suggest the establishment of a rating system related to the legal, ethical, functional, and social content policy guidelines established by these organizations. We suggest the establishment of an agency that will use the proposed rating system to inform customers of the implications of adopting a particular VAPA in their sphere.

Keywords: data privacy, AI ethics, intelligent cognitive assistants, voice activated personal assistants, VAPA, Alexa

INTRODUCTION

In February 2019, an Executive Order was issued to maintain American leadership in artificial intelligence (Executive Order 13859, 2019). This order was supported by the National Science Foundation (NSF) who had already conducted two workshops, one in 2016 and one in 2018, realizing that pressing and long-term problems on the horizon would require new forms of computational analysis and human-computer collaboration to make effective progress toward solving these problems. These new forms, referred to as Intelligent Cognitive Assistants (ICAs), should embody intelligent architectures and capabilities endowed with common sense knowledge and reasoning which, if applied appropriately, could fundamentally enable humanity to address these challenges in the foreseeable future (Oakley, 2018; SRC, 2016).

The 2016 workshop reached a consensus that ICAs should “complement, rather than replace, human capabilities. ICAs must respond and change flexibly to changing environmental and usage conditions, consider the human life course in their application, facilitate ‘natural’ interactions involving ‘common sense’ toolkits and intuitive interfaces, and ultimately cultivate trust in relations between humans and machines. They should leverage models of the intentions and goals of the people they are supporting. There is a great opportunity to leverage detailed models of human cognition, including and understanding of biases in judgement, and models of attention, memory, perception, and comprehension.”

The workshop then posited the application of ICAs throughout at various stages of the human life span: (1) early development and education; (2) group activities and working environment; and (3) eldercare. At the time, no one foresaw that the world would be engulfed in a pandemic during 2020. Imagine if there was an ICA to personalize everyone’s learning by providing what was needed, in the form needed, at the time needed, and where needed in order to optimize individual learning. Imagine if there was an ICA that can facilitate virtual team effectiveness through its understanding of individual and group psychology and team dynamics so that it can engender trust, facilitate interactions and incorporate interdisciplinary perspectives. And imagine if there was an ICA that could gently work with the elderly to assist them with specific tasks or needs as their abilities gradually wane. Clearly, with such ICAs, we would be able to much better weather the disruptions caused by COVID.

The above paragraphs illustrate the strategic importance of artificial Intelligence to the nation and the visions that exist for combining it with inspirations from psychology, cognitive science, and neuroscience to form ICAs that can achieve conceptual learning, fast instance learning, and lifelong learning. There is a sense that we are on the precipice of creating Cognitive Artificial Intelligence which will enrich the lives of humans over their entire lifespan, from cradle to grave. Enhancing human physio-cognitive capabilities, while respecting social, ethical, and legal concerns, is a main goal (Oakley, 2018).

While scientists and researchers may view us as being on the precipice of their creating amazing ICAs, the common man is living in a world ubiquitous with precursors to ICAs – namely Voice Activated Personal Assistants (VAPAs). While they may not satisfy the scientists’ definition of intelligent, they are intelligent enough to engage with users conversationally by reacting and responding to the users’ oral requests (Mallat, 2017). Nearly half of US adults say they use VAPAs; 14% use them on computers and 8% use them on stand-alone devices (Pew Research Center, 2017). These interactions result in the users assigning agency to device which is the cognitive phenomenon of anthropomorphism (Burkett, 2018). Besides the term VAPA, they are also called digital voice enabled assistants, virtual personal assistants, smart speakers, conversational agents, chatbots, intelligent personal assistants (Cowan, 2017); and robo-advisors (Sabharwal, 2018). Voice software has “colonized smartphones, car dashboards and the living room” (Day, 2019a). They have also seen use in private homes, healthcare facilities, banks, K-12 classrooms, and in institutions of higher learning.

The rise of the current global COVID-19 pandemic has given new impetus to the development and adoption of new VAPA technologies and applications. Amazon’s *Alexa* unit reports a huge increase in the use of *Alexa* in and out of the home and its skill’s usage up 65% worldwide. It has also populated the *Alexa* data base with corona-virus related questions with information from a number of sources, including the CDC (Soper, 2020). The government ordered lockdown in the United Kingdom is leading more than half of VAPA owners to increase their use of technology and that 40% plan to increase their use of VAPAs even after the lockdown ends. In all, 60% of VAPA users said that their VAPAs were helping them during isolation and more than half said that their VAPAs had become part of the family during lockdown (Schwartz, 2020).

Being considered part of the family has led to the building of relationships between *Alexa* and users. *Alexa* has received over a million marriage proposals and compliments of love from its “family members” (Soper, 2020). While this may have its humorous side, it points out that *Alexa* may receive volumes of personal information from users which, if not safeguarded, may lead to compromising situations in the wrong hands. The explosive development and use of VAPAs in all arenas, but particularly in private homes, healthcare, banking and education as a result of the COVID-19 global pandemic has led to a new urgency in providing consumers of VAPAs with some measure as to their ability to safeguard privacy.

The objectives of this paper are to lay out the framework for the development of such a measure. To do so, we will first examine the current situation regarding privacy issues that have and are arising through the use of VAPAS. This is followed by a review the policy guidelines developed by six diverse organizations covering the development of such devices. Next, we analyzed these policy guidelines and summarized their content into a set of categories which, together, embody the guidelines for the development of future ICAs so that they can indeed avoid disrespecting some of the legal, ethical, social and functional concerns arising through their use. Finally, we use these categories to suggest the development of measures that can be used to rate new and existing VAPAs and ICAs as to the extent they satisfy those guidelines and, hence, allow the consumer to make an informed decision as to their procurement and use in their sphere.

To gain an understanding of VAPA user perceptions of privacy, we examine literature related to privacy issues with their current use in: (1) private homes, (2) healthcare facilities, (3) banks, (4) K-12 classrooms and (5) higher education. First, we explore what the expressions of concerns are in current affairs. This will be followed by a discussion of what policy guidelines are calling for.

CURRENT AFFAIRS

VAPA Use in Private Homes

“The moment when a digital assistant surprises a user with “The chemist is nearby – do you want to buy more hemorrhoid cream, Steve?” could be when many may choose to reassess the trade-off between amazing new services and old-fashioned privacy.”

– The Economist (Economist, 2017)

The ongoing COVID-19 pandemic and associated lockdowns has found that a majority (77%) of adults in the U.S. have changed their routine. Among the changes is their use of VAPAs. Being at home more simply creates more opportunity to use a VAPA. More than half of VAPA owners are using voice commands at least once a day. The rate at which VAPA use is increasing suggests a positive feedback loop. The more you use your VAPA, the more you will use it (Schwartz, 2020). VAPAs, through the power of voice, can access information sources from media to recipes for cooking, can order groceries, send and receive e-mails and, more importantly, maintain communication with relatives and friends. Thus, VAPAs provide users with a sense of presence that can lead to them being considered as trusted friends and confidants sharing their owner’s homes (Sheerman et al., 2020). The increased and increasing use of VAPAs combined with the increased socialization between the device and the user will result in more private and personal information being captured in the Cloud and potentially accessible to anyone with a “good” pretext. This will challenge the concept of the home as being a private space.

The home is a private space where a person has a right to retreat and be free from unreasonable governmental intrusion (Silverman v. United States, 1961). What a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. In *Katz v. United States*, the court created a two-part test by holding that the determination of whether a search is reasonable depends on: (1) whether a person is required to have manifested an actual subjective expectation of privacy, and (2) whether this expectation is one that society is prepared to recognize as reasonable (*Katz v. United States*, 1967). The Fourth Amendment of the US Constitution protects people from warrantless searches of places, seizures of people and seizures of objects (US Const., 1791). If both parts of the Katz two-part test are met, the government has taken an action that violates the Fourth Amendment. The third-party doctrine is also relevant. In *United States v. Miller*, the court held that when a bank depositor reveals his private affairs to another person, the information can be revealed to the government by that third party (*United States v. Miller*, 1976).

In 1979, the Supreme Court ruled that the government could install a pen register in a robbery suspect’s office to create a record of phone numbers dialed by the robber. The robber made threatening phone calls to his victim who was able to identify a vehicle she believed he drove. The government found that the alleged robber was calling the robbery victim, got a warrant to search his home, found evidence of the calls

to the victim and arrested him. The court held that there is no legitimate expectation of privacy in information voluntarily turned over to third parties (Smith v. Maryland, 1979). These two cases comprise the third-party doctrine (Villasenor, 2013).

In 2012, the government lost a Supreme Court case related to physically intruding onto private property without a warrant to attach a GPS tracking device to a suspect's car. Justice Sotomayor wrote that the third-party doctrine may be ill suited to the digital age. Since people reveal a lot of information in public social media platforms for limited purposes, should they be disentitled to Fourth Amendment protections? (United States v. Jones, 2012).

What is deemed a reasonable expectation of privacy has changed over time given social media networking (Bedi, 2013). Regarding information sharing devices such as VAPAs, when data is shared voluntarily with companies like Google, the user may not be concerned about the limited purpose. However, government access may be concerning, and the user may expect privacy for their different access purposes. It has been argued that the third-party doctrine needs to be updated to better reflect modern life (Haslag, 2018).

Therefore, although data collected by smart home devices is stored by third parties, it is intended to be private since it is collected inside the home. The collected data should receive the same privacy protection as telephone calls. When hearing cases that involve VAPAs in the home and the third-party doctrine, the Court should apply the reasonable expectation of privacy test (Haslag, 2018). There is a need for a more modern application of the third-party doctrine. It has been argued that *Alexa* data is analogous to the private papers in personal diaries. Some members of American society may not have knowingly consented to sharing this information; and it is possible for individuals to be unknowingly recorded by *Alexa*. Further, besides the use of *Alexa*, more and more citizens 'need' to use third-party digital services such as e-mail, cell phones, credit cards, and online news platforms. It is unlikely that users intend for their intimate conversations to be accessed by government law enforcement without warrants. The third-party doctrine "needs to be reconsidered as it becomes harder to function in the political, economic and social world without sharing electronic data" (Shackleton, 2019).

In addition, regarding freedom of speech, if users know that the intimate details of their conversations are collected, shared and can be acquired by law enforcement, then the user would clam up. Feeling the need to clam up thwarts Americans' freedom of speech. There is an 'essentialist' argument that the data has constitutionally protected value as speech. There is the argument that data is property and strong data privacy protection would reduce liberty by constraining consensual market exchange. Companies like Amazon that argue they need to collect data in order to improve their algorithms view the data as knowledge. The collection and processing of data "promotes greater scientific and commercial understanding of individual behavior and desires" (Cohen, 2000). Arguably, data privacy protections and the control of personal data can be turned over to individuals. It can be done by creating "a limited right against certain kinds of commercial collection and use of personally-identified information" (Cohen, 2000).

In 2018, the US Supreme Court held that merely turning on a cell phone creates location data and that act is exempt from the third-party doctrine. Each time a cell phone connects to a nearby tower, a person's movements can be tracked with the use of cell site location information (CSLI). The court ruled that this information is not subject to the third-party doctrine (Carpenter v. United States, 2018). Thus, perhaps the Supreme Court is moving in the direction of limiting the use of the third-party doctrine to reflect the modern, digital age we live in.

The magazine *The Economist* released a statement that "allowing always-on microphones into people's pockets and homes amounts to the further erosion of traditional expectations of privacy" (Economist, 2017). One report stated that about one quarter of US homes have smart speakers like the Amazon Echo (National Public Media, 2020). Another stated that 4% of smart speaker users own more than one (Nielsen, 2018). *Alexa* can identify individual voices and Amazon could choose to inform users who had not previously consented that they were being recorded. However, Amazon does not warn unregistered users that it is creating voice recordings of their *Alexa* interactions (Romano, 2019).

Google Home and Amazon *Alexa* are VAPAs that have recordings of everything everyone in the home says. This includes information about the times in which dwellers ask for lights to be turned on and off and

music that they listen to (Bubar, 2018). Sciuto et al (2018) gathered history logs of 75 *Alexa* users and interviewed them about how they integrated *Alexa* into their lives. Participants were asked about their joys and frustrations; how they socially interacted with the devices; how their home environments influenced their use; and when they questioned their privacy (Sciuto, 2018). The devices were used to control lamps, lights, fans, televisions and speakers. They were used in living rooms, bedrooms, kitchens, family rooms, dining rooms, dens and offices. Surprisingly, many home owners owned many devices and placed them throughout their homes (Sciuto, 2018).

Amazon and Google keep a copy of everything that their devices, *Alexa* and Apple Siri respectively, records (Fowler, 2019). For *Alexa*, the data is stored on Amazon's servers and can be accessed any time by the *Alexa* owner's Amazon account (Melancon, 2018). These companies claim they need the data to improve their artificial intelligence systems (AI/S). There is merit to this because in order to train and optimize AI/S, machine learning algorithms require vast quantities of data (OECD, 2019: 88). This begs the question of why these companies are not soliciting volunteers or offering to pay individuals for their private data (Lynskey, 2019). Perhaps VAPA developers like Amazon want the benefit of spontaneity in the recordings of what users say. Amazon, for example, claims that it annotates a small sample of *Alexa* voice recordings in order to improve customer experience (Romano, 2019).

In the wake of Facebook's CEO Mark Zuckerberg's testimony before the US Senate regarding more than 87 million Facebook users' private information being used by Cambridge Analytica in relation to the 2016 US Presidential election, US Senators Klobuchar and Kennedy introduced a bill that would require websites to provide users with a copy of the data that is being collected about them and a list of entities has access to the data. US Senators Blumenthal and Markey introduced the bill S. 2639 called the 'Consent Act' that would force companies to get consent to share or sell personal data. So far, the bill was read twice and referred to the Committee on Commerce, Science and Transportation (2018b; Bubar, 2018).

Andy Rubin owns a VAPA for home company called Henry Products LLC. This company developed a smart home VAPA called *Essential*. This device uses an operating system that scans data, learns home dwellers' routines (at home and on the go), predicts their needs, gets dozens of gadgets cranking and controls the home environment. It is a suite of always-on listening devices that tracks home dwellers. However, Rubin believes that his device is not a threat to privacy because it does not send data to the cloud. His company does not sell the data or want it. They simply sell the product (Pierce, 2017). So, VAPA developers' use of data could be limited to AI/S improvement rather than being sold to marketing agencies and other organizations.

The European Union's General Data Protection Regulation (GDPR) went into effect May of 2018 (EU GDPR, 2018). It is a strict regulation that requires that companies like Amazon and Google explain in simple language how they plan to use and share people's personal information. These companies must obtain users' consent and authorization for data. A comparison between US laws and the EU GDPR has been conducted. The US does not have a comparable GDPR. Instead, individual states have enacted some of the related privacy laws (Garrison, 2019).

In 2015, Amazon was asked to provide police authorities with Echo smart speaker recordings related to a murder case in Bentonville, Arkansas. The murdered victim was found dead in a hot tub at the defendant's home. The defendant voluntarily agreed that Amazon could release the data (Flynn, 2018; McLaughlin, 2017; Pfeifle, 2018). In March 2017, Amazon agreed to turn over the requested data (Pfeifle, 2018). In 2018, Amazon was ordered to provide police authorities with Echo smart speaker recordings related to a double murder case in New Hampshire. An adult male was charged with killing his girlfriend and her friend in his home (Anderson, 2018; Flynn, 2018).

Since 1990, the Electronic Frontier Foundation (EFF) has fought against injustice and stand for freedom related to the use of digital technology. They were founded at the time of the early use of the Internet. Their primary concerns include censorship, corporate and government surveillance and efforts to thwart innovation (EFF, 2020). An example of EFF's efforts is the 2015 Amazon case. The EFF applauded Amazon for pushing back on the request for Amazon Echo data (EFF, 2017). This advocacy organization promotes that the microphones and cameras used in VAPAs should not be trusted because they can be hacked, exploited and used by law enforcement agencies (EFF, 2019).

Again, the Fourth Amendment to the US Constitution prohibits unreasonable searches and seizures; and protects the sanctity of the home (Pfeifle, 2018). Courts are trying to figure out if this applies to VAPAs. In 2017, the Electronic Privacy Information Center (EPIC) sent a letter to the US Department of Justice and the Federal Trade Commission (FTC) requesting an investigation of whether VAPAs violate federal laws against warrantless electronic surveillance (Smith, 2017). It has been argued that the First Amendment Right to Free Speech is the best option for protecting a customer's VAPA data rather than the Fourth Amendment (Melancon, 2018).

Surveillance intermediaries are VAPA developers like Apple, Google and Facebook that dominate digital communications and data storage. Government and law enforcement surveillance relies on them. These companies' incentive to resist government requests for user data is financial and ideological. These intermediaries exercise minimum compliance with requests for data and aggressive litigation. They also design products and services to make surveillance harder. In addition, they rally legislation and public opinion against government surveillance. Intermediaries construct policies by helping "society identify and minimize tradeoffs between security and competing values like privacy and economic competitiveness". However, the unintended consequences are that they likely force government to surveil more invasively and allow themselves to collect more user data. Besides this frontier construction, there is also frontier selection whereby they select policies (Rozenshtein, 2018).

The primary concern is over what happens to data after it is collected and for what purpose will it be used. In the home, use of the Amazon Echo is not automatically protected by the Fourth Amendment given the Katz vs. US two-part test. Further, what a person knowingly exposes to the public is not given Fourth Amendment protections. Since anything that VAPAs pick up and get stored in cloud storage is exposed to the public, it is unlikely that this data will receive Fourth Amendment protection (Allen, 2018). There must be a way for people to give notice about what they seek to preserve as private.

Some scholars purport that since users of VAPAs treat these anthropomorphized devices and applications as assistants who are persons, the law should treat them as if they are people. Legal scholar Christopher Burkett argues that the US Congress and courts should limit the government's ability to use the technology against its users. The communications recorded and stored on these devices should receive special maximum privacy protection in homes (Burkett, 2018). This "raises questions about what it means to be human. AI researchers insist that their machines do not think like people, but if they can listen and talk like humans, what does that make them? As humans teach ever more capable machines to use language, the once-obvious line between them will blur" (Economist, 2017).

Professor Pedro Lopes designed a bracelet which jams signals from any microphones on VAPAs and prevents voice recognition (Savva, 2020). The development of technology to limit the always-on feature of VAPAs would be beneficial. Perhaps companies should engineer privacy into their devices (Pfeifle, 2018). Existing technical measures include pseudonymization, anonymization and encryption. "Privacy and security will soon be expected 'by design and by default' – and with this regulatory turn, comes a raft of responsibilities". The human computer interface (HCI) community should make privacy and data protection an integral part of broader system design which meet end-users' privacy goals (Luger, 2015).

In 2012, the FTC's report on Protecting Consumer Privacy in an Era of Rapid Change presented data security, data collection limits, sound retention practices and data accuracy advocacy. The FTC recommended that companies provide consumer choice at the time of data collection and use, limit data sharing with third parties, obtain affirmative consent before collecting sensitive information, and provide a Do Not Track mechanism (FTC, 2012). Regulations must address how big data, digital technologies acts on society and collects information that get to know everyone inside and out (Pan, 2016). Thus, besides requiring privacy by design, tech companies can be incentivized to be privacy conscious. They should also adopt the opt-in model required in the GDPR adopted in 2019 (Manheim, 2019).

However, some people do not care about invasions of privacy. It helps to gain an understanding of privacy theory related to the "tradeoff" between having privacy and benefiting from the use of these devices (Cohen, 2000). Although worried about privacy, people are willing to give up privacy in return for convenience (Thomas, 2018). The tradeoff idea is that users do not have to use VAPAs. According to

Georgia Tech's Mobile Robot Lab's robot ethicist scholar Dr. Ronald Arkin, when they make the concerted choice to use VAPAs, they allow potential violations of their privacy (Carroll, 2015).

Sun Microsystem's CEO Scott McNealy once said: "You have zero privacy anyway. Get over it" (Springer, 1999). This was essentially a call for 'privacy resignation'. Lau et al (2018a) interviewed 17 users and 17 non-users of VAPAs. These researchers found concerning evidence that some VAPA users showed signs of 'privacy resignation' which can lead to 'privacy avoidance'. There was a lack of privacy seeking behavior. The researchers suspect that this is because of what a user might find if they were aware of privacy risks, educated themselves about data practices and controls, and made more careful informed decisions. The research team recommended that VAPA designers design privacy notices with privacy resigned users in mind. The new design would prompt users to make privacy decisions that they might otherwise avoid (Lau, 2018a, b).

VAPA Use in Healthcare Facilities

The current COVID-19 pandemic has created unprecedented opportunities for VAPAs. They can hear and respond in a natural language to questions and present concise information from credible sources and thus help prevent a "misinfodemic": the spread of a disease facilitated by misinformation. Amazon found it impossible to vet the credibility of skill developers and thus removed all the skills related to the virus from the *Alexa* store and put a stop to adding new ones. However, they relented when the Mayo Clinic, in partnership with software developer Orbita, was able to convince them about the credibility of the information contained in their skill. However, Amazon's concerns about misinformation still limits the Mayo Clinic skill to the U.S. (Schwartz, 2020).

VAPAs may be uniquely well suited for symptoms screening because people with stigmatized conditions often avoid seeking health care and education and are more willing to disclose sensitive personal information to VAPAs than to humans. If effectively designed and deployed, VAPAs can help to mitigate the long-term impact of pandemic-related isolation, trauma, and depression. To provide these opportunities, corporations such as Amazon, Apple, and Google have developed COVID-19 focused VAPAs on platforms available to billions of users (Miner et al., 2020). This explosive growth in health-related applications of VAPAs, however, also carry a risk of misdiagnosis (can a VAPA be responsible for malpractice?) as well new and novel challenges on how to comply with Health Insurance Portability and Accountability Act (HIPAA) requirements.

The Carnegie Mellon University and University of Pittsburgh have a Quality-of-Life Technology Center for developing various quality of life technologies. These technologies require the collection and sharing of personal information. Microsoft rolled out a HIPAA and GDPR compliant healthcare VAPA that includes a symptom checker, medical content, healthcare facility testing location assistance, appointment scheduler and answers to non-medical questions (Hale, 2019). A decade prior to this, a study was conducted of disabled and nondisabled adults' use of recordings with video, sound and sensors for sharing personal information with healthcare providers, insurance companies, researchers and government. Using a survey instrument, participants were asked for information is focused on end-user health related behavior and functioning such as toileting, taking medications, cognitive ability and mobility. The researchers measured concerns about the importance of privacy, security and specific information. The researchers found that user privacy concerns are a potential barrier to the adoption of technology. This study provided empirical evidence of the implicit tradeoffs between privacy and the benefit of potentially improved health among older and disable adults (Beach, 2009).

The researchers found that individuals reporting disability had more positive attitudes towards sharing information than those not reporting disability. Those with disabilities were more likely to accept infringements on their privacy when using quality of life technological applications. The benefits of using the applications outweighed the possible cost of diminished privacy. This suggests that the greater a person needs help, the more privacy the person may be willing to relinquish (Beach, 2009).

Older, nondisabled elderly people were slightly more accepting of sharing and recording privacy information. Interestingly, both the less educated and the most educated among participants had more positive attitudes about the sharing and recording of their health information. The researchers opined that

perhaps the less educated had more trust in government and insurance institutions. Further, people with lower socio-economic status may not have the luxury to be concerned about privacy issues. So, this is a phenomenon that merits further study (Beach, 2009).

Overall, the study participants had positive attitudes about using technology that shared their privacy information since the technology made their lives easier, more comfortable, safer and convenient. Participants that had concerns about the security of information released to web sites and medical institutions were less accepting of using the technological applications. The private use of their toilets was contentious since private affairs like this is embedded in our culture. The researchers stated that the gathering of this type of very personal data needs to be made less highly visible with unobtrusive technology such as sensors rather than surveillance cameras (Beach, 2009).

In 2014, researchers published a systematic review regarding older adults' perceptions of technologies focused on falls prevention, detection and monitoring. All of the studies revealed that control over privacy was very important to patients in regard to any video imagery activated after a fall. Patients were fine with imagery in their living room but not in their bedroom or bathroom. If they did not use a technology, it was due to breach of privacy. Cameras and visual surveillance were not desired in relation to robotic devices, fall detectors and home automation systems (Hawley-Hague, 2014). While VAPAs are not known for camera or videotaping features, it is considered a surveillance and monitoring device which records voices. Hawley-Hague (2014) stated that “[g]iven the differing results in studies included in [their] review, further research into the relationship between perceived breach of privacy and the potential benefits of technology is needed”.

In a literature review of ethical implications of the use of assistive technology in elderly care homes, researchers found that the implementation of specific monitoring devices, ethical values of privacy, autonomy and independence appeared to be at risk. Loss of autonomy and privacy is heightened in nursing homes. The authors recommend that the concept of obtrusiveness needs to be disentangled from underlying ethical considerations (Zwijssen, 2010). Research has been done on user perception of obtrusiveness in relation to privacy, physical invasion, human interaction and other factors (Hensel, 2006).

Situational factors are broad dimensions of the characteristics of a situation. These characteristics can be used to describe and compare any situation (Rauthmann, 2017). Researchers have examined the use of VAPAs by the blind (Abdolrahmani, 2018). They found that the impact of situational factors played a role in the ways that users interact with VAPAs due to privacy issues.

Another research project involved 14 blind participants and individuals who are blind and hearing impaired. The primary privacy concern was eavesdropping by others nearby. On a daily basis, these study participants were concerned about their private financial and medical information. There is a need for a way for these individuals to monitor their surroundings and know whether someone is in earshot. From interviews, it was discovered that these users' concerns about using assistive devices was that they were too expensive, hard to learn, too time consuming, not user friendly and did not work well for them. The researchers recommended that devices such as Google Glass would reduce the cost and complexity (Ahmed, 2015). In 2009, the Pitt-CMU Quality of Life Technologies research team stated that they would focus on studying the use of “inside-out” vision technology. This is a device worn by a patient that captures what is going on in the environment around them. The privacy concern includes the patient's attitude about having their family and friends monitored and recorded (Beach, 2009).

Health chatbots “could potentially increase access to healthcare, improve doctor-patient and clinic-patient communication, or help to manage the increasing demand for health services such as via remote testing, medication adherence monitoring or teleconsultations” (Nadarzynski, 2019). Alison Darcy, clinical research psychologist at Stanford University, built the chatbot *Woebot* to help depressed patients. It chats with users in Facebook Messenger. Darcy studied 70 young adult users and discovered that they experienced lower incidents of depression and anxiety after two weeks of chatting with *Woebot* (Thompson, 2018). Besides *Woebot*, there is AI/S robot therapy conducted with chatbots such as *Tess*, *Sara* and *Wysa*. Interestingly, although these VAPAs serve to provide a way for patients to get low-threshold interventions in the “privacy” of their homes or on the go, clear standards for confidentiality, information “privacy”, and data security are needed. There needs to be transparency. Patient autonomy relates to “when and how

consent is required and how best to deal with matters of vulnerability, manipulation, coercion and privacy”. Guidance on how to implement applications in a way that respects patient autonomy needs to be developed (Fiske, 2019). It has been advocated that the field of psychology “champion new legislation to ensure the confidentiality, privacy, security, liability, competency, and even the licensure of overseeing clinicians [because] [e]ven if these chatbots aren’t the virtual therapists of tomorrow, you may soon see them in clinical decision support, data processing or entry, and even in managing the clinic’s schedule” (Vaidyam, 2019).

Chatbots *Woebot*, *7Cups* and *Koko* provide psychological and psychoeducational materials. *Koko* is a mobile application designed to promote emotional resilience (Morris, 2018). Morris et al (2018) studied 37,169 *Koko* users and found the responses from the chatbot to be rated favorably and were well received. However, these researchers found that users rated responses less favorably when they were told that the responses came from an assistive agent chatbot rather than a peer. Interestingly, all of the responses were written by peers (Morris, 2018).

Nadarzynski et al (2019) interviewed 29 students on the University of Southampton campus were interviewed to assess their attitudes toward new digital technologies in healthcare. They were asked about digital privacy, the accuracy of health information online, the preference for face-to-face interaction and trust in advice from a health chatbot. The researchers found that although students were not familiar with the use of health chatbots, the students appreciated the mainstream chatbots such as *Alexa* or Google Home for information searches. Students were also ‘AI hesitant’ about the quality, trustworthiness and accuracy of health chatbots (Nadarzynski, 2019).

VAPA Use by Banks

Some banks have made the development and application of VAPAs part of their long-term strategy. Bank of America received approximately 160 patents relating to Artificial Intelligence in 2018. *Erica*, its virtual financial assistant, has 24 of those patents associated with it. Since its launch, *Erica* has attracted eight million users on the mobile app and has handled more than 55 million client requests. Other banks are following Bank of America’s lead. NatWest, a British bank, recently ran a pilot for handling banking using Google Assistant and FIVE, a platform created by a group of credit unions working together to enable members to transfer funds and pay down loans through Amazon *Alexa* and Google Assistant (Schwartz, 2019). The COVID-19 pandemic could be the most serious challenge to financial institutions in nearly a century. Institutions that are at the forefront in the development and applications of VAPAs are better positioned to deal with the COVID issues than their less technology driven peers. But the less technology driven peers can still position themselves to better deal with COVID imposed issues by increasing their IT development teams to automate routine work in back-office operations. Intelligent automation tools may let them automate simple to moderate tasks at both branch and corporate levels within several weeks. And, to offset the surge in call volume, the use of VAPAs can help to process as a significant number of requests without live intervention. However, the issues dealing with privacy are still considerable as will be discussed below (Yousufani, 2020).

Wells Fargo uses a Facebook Messenger chatbot robo-advisor (Sabharwal, 2018). Swedish bank Svenska Enskilda Banken (SEB) uses a VAPA called *Aida*; Nordea Bank uses *Nova*; and Swedbank uses *Nina* (Hansson, 2018). Another ‘bank bot’ is HDFC Bank’s *AVA* (Vajradhar, 2020). Financial institutions including USAA, Capital One and American Express are using *Alexa*. Users can ask for their account balances, spending habits and financial advice. Darius Jones, Assistant Vice President of USAA Labs stated that account data is kept secure with a three-way trust between USAA and Amazon using OAuth 2.0. OAuth is a popular standard for tokenized authentication and connection to third party applications. By requiring a voice PIN, USAA claims that it prevents random persons from asking *Alexa* for another person’s banking information (Crosman, 2017c).

Although other banks expressed security concerns, USAA claims that they partnered with Amazon to ensure legal compliance, security and privacy. But data is shared with Amazon. USAA states that they exercise transparency and notify users about the data that is shared with Amazon. By 2017, USAA had completed the development of a secure model to conduct money transfers using *Alexa* (Crosman, 2017a).

“Chatbots can be invaluable where millions of customers reach out to organizations every day with their queries and the need for assistance”. Chatbots can decrease response time and scale up operations (Rakheja, 2018).

In 2017, when Bank of America was developing the VAPA *Erica* and were looking into integrating VAPAs such as *Alexa*, *Siri* or *Google Home*, the bank was concerned about privacy and data ownership issues related to such an integration. They were careful not to rush implementation because of the high risk of public relations nightmares. One reason was that in 2001, in response to such public relation nightmares, Microsoft discontinued the *Clippit* (aka “*Mr. Clippy*”) office assistant that popped up as a paper clip to provide helpful hints. Users were angered and annoyed by it. Users felt it was invasive and interfered with work because it would ask: ‘Are you writing a letter? May I read it?’ (Cozens, 2001). To make matters worse, in 2016, Microsoft launched a chatbot called *Tay* that spouted offensive and racist comments (Crosman, 2017b; McCollum, 2017; Wakefield, 2016).

Bank of America rolled out *Erica* in 2018 and still considered the protection of consumer privacy a challenge. The bank’s chief technology and operations officer stated that the device does not eavesdrop on conversations like the Amazon’s *Alexa* device. The user has to enter their mobile banking account and start the *Erica* session therein (Crosman, 2018). The virtual financial assistant *Erica* can answer user questions and provides notices to users about their credit score changes, refund confirmations, bill reminders, account balances, duplicate charges, recurring charges, and spending (Bank of America, 2020).

When VAPAs and machine learning are used in financial services, they need to be carefully designed to address regulatory compliance. The areas of measuring credit risk for lending charges and lending decisions is a particular concern regarding possible discrimination on the bases of race, sex and marital status. Larry Wall of the Federal Reserve Bank of Atlanta noted that on the one hand, these applications can significantly improve discriminatory practices. However, the modeling would need to be transparent so that the algorithms could be monitored to ensure that they are not programmed to violate regulations (Wall, 2018). Three (3) ethical dilemmas in the use of artificially intelligent financial services include: (1) unintended consequences like the problem with Microsoft’s *Tay* chatbot; (2) the potential for changing human thought processes and methodologies such as in the valuation of start-ups; and (3) the fact that AI/S applications are unable to explain decisions in a way that meets regulatory requirements. “[C]ompanies cannot avoid liability by claiming ‘my robot did it’” (Fourie, 2019).

It is also interesting to note that besides the value that banking VAPAs bring to customer support, they can also be useful to the banks. They can be used for the purpose of lead generation to encourage or assist customers with learning about and selecting bank products. They can also give banks valuable feedback and to identify suspicious or fraudulent activity (Vajradhar, 2020). A well designed one would be able to remember customer preferences, deliver information quickly, machine learn from customer feedback, provide easy to understand graphics, widgets and text; can interpret a number of languages; work on the web or in mobile applications; and work round the clock (Vajradhar, 2020). With regard to designing chatbots using best practices in interaction design methods, short and easy tasks were met with more positivity than longer and complex tasks (Duijst, 2017). Careful formatting, use of language and gamification for entertainment are key to providing a good user experience (Hansson, 2018). The better banks get at this, the more widespread the use of these VAPAs will likely become.

VAPA Use in K-12 Classrooms

The COVID-19 pandemic has impacted over 1.2 billion students in 186 countries. In 2019, global investment in educational technology was estimated at \$18.66 billion and was estimated to reach \$350 billion by 2025. The pandemic has accelerated the rate of investment to support the shift to remote learning on digital platforms. While many bemoan this shift to online learning, research suggests that on average, students retain 25-60% more material when learning online compared to only 8-10% in a classroom. They also require 40-60% less time to learn than in a traditional classroom because they can learn at their own pace, going back and re-reading, skipping, or accelerating through concepts as they choose. This will not happen if online learning is designed to replicate what happened in a classroom. Since children are more easily distracted, there needs to be a concerted effort to make online learning fun and effective which can

be achieved through the clever integration of games that will engage the young learner and make them fall in love with learning (Li and Lalani, 2020). Education oriented VAPAs will play a central role in making this happen, but only if they can assure privacy and confidentiality to parents, teachers, and schools (Suprenant, 2020).

There are start-up companies such as Aparna and Deepak Ramanathan's "Ask my class" that are refining *Alexa* functions to make them more appropriate for children (Boccella, 2019). VAPAs are helping teachers in the classroom. They can be used to: (1) conduct learning drills, (2) play music, (3) play games, (4) ask and answer student questions, (5) promote mindfulness, (6) read to the class, (7) time activities, (8) facilitate peer editing and reading for questions that come up during peer editing, (9) take attendance and (10) track participation points (Penn State University, 2017). In addition, a new VAPA called *EVA* was developed by the start-up Voicea for notetaking (Herold, 2019).

Some benefits are that VAPAs are good for timid students (Davis, 2018). Students are corrected without feeling judged. VAPAs in classrooms also benefit students in low income areas whose parents cannot afford to buy such devices (Desai, 2019; Fredericks, 2019). Teachers have reported that students enjoy having a robot in the classroom (Penn State University, 2017). When done well, students can learn great critical thinking skills. However, when used poorly, technology in the classroom can detract from learning because students get distracted and classroom management becomes difficult (Fohner, 2019).

Amazon sells an Echo Dot Kids version. Northern Idaho University experimented by placing 90 Echo Dots in their schools. One benefit was shared by a special education teacher. A student on the autism spectrum began to ask *Alexa* questions and the VAPA helped teach this student how to interact (Pfannenstiel, 2019).

Students' privacy interests are undervalued by education policymakers when they release policies stating that students, employees, visitors and other users are to have no expectation of privacy in anything they create, store, send, delete, receive or display when using a school system's network, device or Internet access (Fedders, 2019). There is concern about students managing their own privacy settings. It is recommended that schools stop requiring only one e-safety class each year or a once yearly presentation from a policeman. More interactive ways to provide e-safety lessons is with gaming in education (BESA, 2018a). In addition, teachers should have a voice on school edu-technology committees that promulgate school district regulation and policies on the use of technology in the classrooms (Brown, 2018). It is also recommended that there be awareness of privacy issues; classroom use policies; and alerts and conversations with parents about the use of VAPAs in the classroom (Crist, 2019; Davie, 2018; Knutson, 2018).

VAPAs are surveillance instruments because they "must be listening at all times so that they can respond to users" (Hoy, 2018). The use of cameras in the classrooms has been debated. These are known as smart classrooms. In smart classrooms, sensors are used to track where teachers look, where students look, how many times they speak up or raise their hands, and how much time teachers leave for student responses after questions are asked. The issues to address are: (1) who has access to this data, (2) what will they do with it, and (3) who can benefit from it. There are benefits such as: (1) students could access the data and reflect on the level and extent of their in class engagement; (2) parents could access the data to better understand their student's progress; and (3) teachers' performance could be assessed (Ogan, 2019). Another question is: "What steps will administrators take to secure student data and ensure the privacy of this information?" (Pierce, 2018).

Interestingly, at the 2019 International Society for Technology in Education (ISTE) conference, an Amazon representative stated that Amazon's VAPAs were not intended for the classroom (Tate, 2019). Earlier, in June 2018, an Amazon representative stated that the products *Alexa* and *Dot* pose compliance and privacy issues. When this was tweeted by the privacy expert Bill Fitzgerald, it got 40 retweets and 100 likes (Nazerian, 2018).

Teachers in the Greylock Regional School District in Massachusetts use Amazon's *Alexa* device in their classrooms. One teacher was concerned that although she turned *Alexa* off, it stayed on awaiting a keyword to activate it. Teachers were found to not understand privacy laws and how noncompliance impact students, teachers and the school district. Eileen Belastock, the Chief Technology Officer of the Greylock

Regional School District stated that there is a need for policies to be developed regarding use of VAPAs in classrooms. Belastock stated that she did not believe VAPAs should be in the classrooms because there are other AI/S tools available. Further, the devices “circumvent any school filtering and firewall”. Application providers like Amazon are not soliciting parents’ permission to disclose personally identifiable information (Brown, 2018). Thus, with regard to risk management, school administrators may incur unforeseen legal liability if they hastily adopt practices involving surveillance in violation of student privacy interests (Fedders, 2019; Zeide, 2016).

Contrary to Belastock, Superintendent Kenneth Eastwood of the Enlarged City School District of Middletown New York says that although legal compliance is a real issue, he is of the opinion that VAPAs should be tested to acquire lessons learned (Horn, 2018). RAND’s K-12 senior policy researcher Robert Murphy advises that before new tech is adopted, educators need to address specific questions on what problems they are hoping to solve, for which students, and under what circumstances (Herold, 2019).

Fifth grade teacher Rayna Freedman uses the Google Home VAPA in her classroom. She claims that she uses a “clean” Google account that is blank with no link to her identity, billing information or student data. She also crafted a responsible use policy. She claims that their conversations are protected because the students unplug the device (Crist, 2019). This is concerning since the device has wireless capabilities and need not be plugged in. Also, users may think that programmatically they are their account name and login credentials when they use AI/S devices. But, in fact, the system’s algorithm is building an identity of the user(s) over time and creating a rough portrait that is a proxy (Gajendar, 2019). Users are not likely to be aware of this.

To function, the Amazon Echo device must be permanently switched on, connected to the Internet and awaiting the wake word command. However, there are security concerns (Davie, 2018; Simpson, 2017; Wueest, 2017). VAPAs require cloud computing to analyze requests and personalize responses. When users click “I agree to the terms and conditions of use”, they give consent to the use of their personal data. They give consent to third party use. It has been argued that this type of consent does not require much attention and that users do not likely fully understand that they are giving away their personal data in an on-going manner. The current consent mechanisms cannot meet VAPA challenges such as the developers’ desire to store, study and perhaps sell user recordings. There is a need for new consent mechanisms and software developer tools that encourage and reflect human values such as justice, autonomy, privacy, trust and freedom of choice (Hong, 2004; Kaye, 2018; Luger, 2013).

The information technology team at the Metropolitan School District of Wayne Township in Indianapolis claims that data is secure because their *Alexa* device is connected to a separate WIFI network that does not cross data with servers that contain sensitive information. This school district claims that they check the voice recordings regularly to monitor how they are being used (Crist, 2019). Here, the school district is protecting credit cards and social security numbers. But what about personal information that the children share in the classroom? What about the property rights in the children’s voices that get recorded? The bottom line is that the school district has absolutely no control over what Amazon does with the voice recordings and cannot monitor how Amazon uses the recordings.

The prominent laws that govern the rights of children and their personally identifiable information include the: (1) United Nations Convention on the Rights of the Child; (2) Family Educational Rights and Privacy Act (FERPA) ; (3) Children’s Internet Protection Act (CIPA) ; and (4) Children’s Online Privacy Protection Act (COPPA) (COPPA, 1998).

Since 1990, Article 16 of the United Nations Convention on the Rights of the Child gives children a right to privacy. This ruling states that: “(1) no one shall be subjected to arbitrary or unlawful interferences with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation; and (2) the child has the right to the protection of the law against such interference or attack” (United Nations, 1989). In addition, since 1974, the Family Educational Rights and Privacy Act (FERPA) has protected the privacy of students’ records that are maintained by schools. Schools must have written permission from a parent or eligible student in order to release any information from a student’s education record. There are exceptions. For example, schools can disclose a student’s name, address, telephone number, date and place of birth, honors, awards and dates of attendance. This is known as school directory

information. The school must notify the parent about the release and give parents enough time to request that this information not be disclosed.

The nine (9) FERPA exceptions which do not require consent include giving student information to: (1) school officials who have a legitimate educational interest in the information; (2) other schools that a student is transferring to; (3) specified officials for audit or evaluation purposes; (4) appropriate parties in connection with financial aid to a student; (5) organizations conducting certain studies for or on behalf of the school; (6) accrediting organizations; (7) compliance with a judicial order or lawfully issued subpoena; (8) appropriate officials in cases of health and safety emergencies; and (9) juvenile justice system state and local authorities in compliance with specific state laws.

Since 2000, the Children's Internet Protection Act (CIPA) has required that schools that benefit from the E-rate program (for affordable communications services and programs to schools and libraries) have internet safety policies. The US Federal Communications Commission (FCC) has issued rules to implement the CIPA. The goal is to address concerns about minor students' access to obscene and harmful content over the Internet. Schools are to (1) monitor and block harmful content; and (2) educate minors about appropriate online behavior. Schools that do not comply may not receive the E-rate program discounts.

The 1998 Children's Online Privacy Protection Act (COPPA) requires that website operators and online services get parental consent for the collection of personal information of children under the age of 13. Companies making applications, websites and online tools for kids under the age of 13 must have a clear and comprehensive privacy policy; get parental consent before collecting information about kids; and not use kids' data for marketing-related purposes (COPPA, 1998). In 2002, the Federal Trade Commission (FTC) released results from a survey on compliance with COPPA. They found that 89% of websites that collected personal information had privacy policies (FTC, 2002).

Quite frankly, if parents' permissions were solicited and one or more parent did not give permission, the classroom would be difficult to manage. Students whose parents did not give permission would not be able to speak to the VAPA device. How would a teacher be able to silence that student? Students would have to be separated into permitted and non-permitted classroom spaces. This might not be practical.

Under the GDPR, children are afforded specific protection regarding their personal data. They are considered a vulnerable population because they are likely less aware of personal data sharing risks, safeguards and consequences (BESA, 2018b).

In a poll of 500 students, some worried that robots acting as teachers could be hacked and produce false information or discover the students' personal information (Davis, 2018). The concern over potential hacking is not unfounded. A German VAPA user listened to his archive and discovered 1,700 audio files from a person he did not know. Amazon dismissed it as a case of mere human error (Shaban, 2018a). Also, in 2018, Senators Flake and Coons who lead the Judiciary subcommittee on privacy, technology and the law, asked Amazon's CEO Jeff Bezos for answers related to the smart speakers' listening habits. A family discovered that their Echo had recorded a private conversation and sent it to a random person in their contacts (Shaban, 2018c).

In addition, there have been privacy concerns raised by the American Civil Liberties Union (ACLU) over the recordation of children's voices and data sent to Amazon's computing cloud (Boccella, 2019). The ACLU questions whether students should be required to submit themselves to always-on voice tracking and other third-party surveillance (Herold, 2018). According to a staff technologist at the ACLU, VAPAs are computers with microphones and speakers connected to networks and they can be used for surveillance. They are entering deeply into our lives without close examination of how they can malfunction (Shaban, 2018b).

In April 2019, although it was reported that human listeners review *Alexa* voice recordings at Amazon, the company stated that it complies with COPPA (Day, 2019a). Recordings do not provide users' full names and addresses. They do include users' first names, device serial numbers and user account numbers (Day, 2019b).

In May 2019, the US Federal Trade Commission (FTC) filed a complaint against Amazon alleging that Amazon's collection of voice recording transcripts and personal information in this youth-oriented version is illegal. The claim alleges that this device only deletes information if a parent explicitly requests that it be

deleted. If a parent does not contact customer service to make this request, Amazon retains the personal information. This form of parental control is allegedly flawed because parents are confused by this privacy policy and the storage of information is not transparent (Brown, 2019; Garcia, 2019a, b).

Alexa collects the name, birthdate, contact information, voice, photos, videos, location, activity, device information and identifiers of users. Collecting information requires parental consent. It has been argued that *Alexa*'s agreement states that "you" accept their terms. However, "you" is not defined as the household or classroom group who is in the vicinity of the *Alexa* device talking (Romano, 2019). Two advocacy groups discovered that the device enables children to easily divulge their name, home addresses, social security numbers and other intimate information. Further, it is cumbersome for parents to delete these personal details; and Amazon fails to get parental consent for the information (Singer, 2019).

US Senators Markey, Blumenthal, Durbin and Hawley signed a letter sent to the FTC stating that there are serious concerns about whether this device complies with laws (Brown, 2019). The Senators state that Amazon Echo Dot Kids does not comply with COPPA because it does not meet the parental consent requirements and Amazon does not disclose what information the device collects and how it is used (Garcia, 2019a). Amazon has stressed that it has strict guidelines in place to protect family security and privacy. They have a service for *Alexa* users called Amazon FreeTime that helps parents manage the ways their kids interact with technology including limiting screen time and parents can review and delete kids' voice recordings at any time via an app or Amazon's website (Garcia, 2019a). But, what about when *Alexa* and Echo speakers are used in the classrooms without parental consent and involvement?

Mattel abandoned plans to build a VAPA called *Aristotle* after complaints were raised that the device would be invasive of children's privacy. The product was to be based on the Amazon *Alexa* technology and was to launch in 2018. A petition with 15,000 signatures from members of child advocacy groups, lawmakers and parents urged that the device was led by the Campaign for a Commercial-Free Childhood and the Story of Stuff Project. Concerns included the psychological bonds that children would form with the data-collecting devices and the in-depth profiles of children and their family that Mattel could collect (Rabkin Peachman, 2017).

Gajendar (2019) argues that when technology companies remind users that they can control their privacy and security settings, the information is too complex. This "control has meaning only when it's contextualized within the activities and goals" users pursue. "Control has purpose when it's made emotionally relevant within a dialogue and with stories" that invite users to take actions to make things as the user desires them to be. User control needs to be respected and enabled in a way that is personally valuable. The question becomes "[h]ow can an intelligent app/ service stage that kind of conversation with human actors using modes of interaction?" (Gajendar, 2019).

With regard to the surveillance features in VAPAs, it has been recommended that: (1) to the extent that pervasive surveillance conveys messages of mistrust, minimizing surveillance will help students value their privacy; (2) schools should have a policy of notice and transparency to help students and their parent protect their privacy interests; and (3) information obtained should not be maintained indefinitely (Fedders, 2019). Although many argue that stakeholders in the use of AI/S need transparency, "some scientists consider the task of transparency too difficult to achieve" because complex AI/S algorithms are too hard to understand. Thus, transparency is illusory because even if we can see what the system is doing, we cannot understand it. Instead of human regulation there should be regulation by a "guardian" algorithm to make sure autonomous devices stay within parameters (Firth-Butterfield, 2017). With this argument, VAPAs would be programmed to perhaps stop the transmission of certain recordings from devices like *Alexa* to its developer Amazon.

VAPA Use in Higher Education

Ongoing advances in hardware, software, telecommunication systems, instructional systems, instructional design models and academic management systems have been harbingers of change in the higher education system (Saba & Shearer, 2016). Teaching via lectures in a classroom is inefficient and ineffective and ignores research that indicates that students learn faster and retain more via online learning (Li and Lalani, 2020). This reality was widely discarded by an academic establishment that had given little

thought to digital literacy and digital pedagogies. When COVID-19 appeared, it became the catalyst that drove the worldwide move to online learning. But online learning is the beginning, not the end of the technological transformation of higher education. As educational technologies continue to advance, they will bring us closer to the holy grail of personalized learning in which properly crafted Adaptive Learning Systems (ALS) will allow learners to match their own personal traits with instructional treatments (Saba & Shearer, 2016). A key factor in personalized learning systems will be VAPAs, which will provide individual students with personalized interventions (Saiz-Manzanares et al., 2020). This will require the sharing of personal and, in some cases, health related information. Thus, VAPAs used to support student learning in general and personalized learning in particular, must be able to conform to HIPAA and FERPA requirements.

Besides VAPAs, there are smart classrooms that include virtual assistant technologies. Whiteboards contain several tools including natural language virtual assistants, video cameras that can recognize gestures and motions, and microphones that capture speech. This classroom technology is capable of recording and processing the natural actions of teachers and students, discern their activities and elicit responses to assist the professor. This is known as ambient intelligence (Carlos Augusto, 2009).

In compliance with federal regulations that mandate strict requirements over the safeguard of stored social security and credit card numbers, university officials write policies and conduct periodic reviews of the encryption of sensitive data (Botelho, 2018). But how can a university control data that gets sent to Amazon's servers when the Amazon Echo is used in a classroom or dorm? With such smart devices, author Stefanie Botelho wrote that "[a] complete computer policy would inform students how much and what kind of data the university gathers from the technology" (Botelho, 2018). However, the university is not gathering this data. Amazon, Google and other device developers are.

Emerson University students use an app called *Em* which is accessed by an Amazon *Alexa* enabled device. It helps students find rooms and offices, determine when to drop or add classes, and obtain other information. Arizona State University uses a VAPA to help students complete projects. Park University's students access the Canvas learning management system and retrieves audio lecture, course announcements and assignment deadlines with a VAPA. San Diego University uses a VAPA to access classroom presentation equipment to assist a handicap instructor who is wheelchair bound and has difficulty accessing equipment (Rowh, 2019). Utah State University has deployed *Alexa* devices to 11 classrooms to support the student teacher interface.

It has been argued that mere online learning will be replaced with computing and that VAPAs such as Siri, Cortana and *Alexa* can deliver interactions with affective computing (Skiba, 2016). With respect to this prediction, Blackboard is rolling out a Blackboard Learn Skill for *Alexa*. It serves to allow access to coursework information (Marder, 2019). Amazon created the *Alexa* Fund Fellowship to engage 18 universities educating PhD and post-doctoral students in the area of using AI/S in education; and in planning coursework and conversational AI/S curriculum (TechCrunch, 2018). Arizona State University will use their fellowship to inspire and enable student start-ups by helping student innovators build their new venture concepts in ASU's Entrepreneurship and Value Creation course (Stoneman, 2018).

Further, besides the classroom, Saint Louis University became the first university in the USA to bring Amazon *Alexa*-enable devices into every student resident hall room and student campus apartment. The university believes that if students can use these devices to save time on searching for information, they can spend more time focused on their education (Saint Louis University, 2018). They installed nearly 2,300 units. Staff deliver university specific information to the students and respond to student requests (Rowh, 2019).

POLICY GUIDELINES

There is fear that AI tools like VAPAs will begin to act on their own behalf. However, since humans are most intelligent when they act collectively and cooperatively, AI will also be at its best when functioning in partnership with humans. Thus, "AI is more of an ancillary intelligence (A*I) [rather] than an artificial intelligence (AI)" (Stokes, 2020) In light of the fears, the development of policy guidelines is imperative.

An early guideline for robotics was written by Isaac Asimov in his three laws of robotics: 1) that robots may not injure a human being, or through inaction, allow a human being to come to harm; 2) a robot must obey the orders given it by human beings except where such orders would conflict with the First Law; and 3) a robot must protect its own existence as long as such protection does not conflict with the First or Second Law (Asimov, 1950). And perhaps “there should be a fourth law that states: Every robot must have a human being that is responsible and accountable for its actions” (Stokes, 2020).

Considering the fears, the design and use of VAPAs is not going unmonitored. Today, in several organizations, there are initiatives to build AI/S around principles of ‘privacy by design’ and ‘privacy by default’. They use and adapt privacy guidelines. “To date, AI policy initiatives feature ethics, fairness and justice prominently” (OECD, 2019: 89). This section gives a short overview of six (6) prominent organizations that provide resources to policy makers on issues relevant to VAPAs. The 6 organizations include: (1) the Partnership on AI/S founded by five of the leading high technology companies in the USA; (2) the OECD Global Partnership on Artificial Intelligence which operates at the country-level worldwide; (3) the charitable outreach organization Future of Life Institute; (4) the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems focused on providing ethical standards to designers; (5) the British Standards Institution (BSI) which published the British Standard (BS) 8611 for the ethical design and application of robots and robotic systems; and (6) the Privacy Coalition.

Partnership on AI

In 2016, Facebook, Amazon, Google, IBM and Microsoft formed the ‘Partnership on AI’. The purpose of the partnership is to provide a formal structure for communication between these companies, academics, researchers, ethicists and other interested parties to discuss advancements in AI/S, conduct research and promote best practices (Mannes, 2016). The partnership aims to be a resource for the exploration of the consequences of certain AI/S; and to policymakers for the development and use of AI/S. The partnership’s 6 pillars include: (1) making sure that when AI/S is used to supplement or replace human decision-making, it is safe, trustworthy and ethical; (2) developing fairness, transparency and accountability methods to detect and correct errors and biases in data; (3) finding best approaches to minimizing potential disruptions to the distribution of jobs and nature of work; (4) provide clarity about the understandings and confidence AI/S have about situations and problem solving (i.e. assistance is only as good as the algorithms are programmed); (5) promote thoughtful collaboration and open dialogue; and (6) collaborate to address society’s most pressing challenges (Partnership on AI, 2020).

In 2019, the Partnership on AI published a framework for responsible product and tool design and policy development involving human-AI interaction. Case studies were included in the publication and addressed the nature of collaboration, nature of the situation, AI/S characteristics and human characteristics. The cases relevant to VAPAs included the use of virtual assistants, mental health chatbots, intelligent tutoring systems. They did not provide a case related to banking (Partnership on AI, 2019).

The nature of VAPAs is that the AI/S evolves over time with model updates and continual interaction. There is active ongoing collaboration between the AI developers and the AI systems. The AI/S serves to help the user and the user seeks help from the device. So, their goals are aligned. Although the goal of the human-AI collaboration is clear, there are goals that users may weigh differently. These goals are knowledge based such as with information gathering; or motivational. The goal could be physical such as with task management.

There may be third parties involved since several people can talk to VAPAs at once. VAPAs require consent before interacting with the AI/S. Consequences of AI/S failure was noted as moderate. An example is where a person asks a VAPA to tell them their flight information or other appointment, and they miss the event. However, “[c]ertain types of sensitive information could lead to grave consequences depending on the response”. VAPAs free up time and provide users with convenience. The significance of their benefits simply depends on who you ask (Partnership on AI, 2019).

OECD Global Partnership on Artificial Intelligence

Founded in 1961, the Organization for Economic Cooperation (OECD) is a research and policy making body with 34 member countries that develop standards. Since 1980, the OECD has provided privacy guidelines. The guidelines were revised in 2013, provide a consensus on international standards and are used by many countries in their privacy laws (OECD, 2013). In 2019, the OECD published a report entitled “Artificial Intelligence in Society” which includes several public policy considerations. The goal is to ensure that AI/S are trustworthy and human centered (OECD, 2019).

In 2020, a new Global Partnership on AI/S was launched and is hosted by the OECD. This partnership’s goal is to ensure that AI/S is used responsibly, respects democratic values and human rights. They plan to convene working groups of experts from industry, governments and academia to address responsible AI/S, data governance, the future of work, innovation and technology commercialization. Members of this partnership are at the country level and include 15 founding members (Australia, Canada, European Union, France, Germany, India, Italy, Japan, Korea, Mexico, New Zealand, Singapore, United Kingdom and the United States) (Moltzau, 2020).

The *OECD AI in Society* report advocates five (5) key priorities for human centered AI/S: (1) inclusiveness, equity, well-being and the advancement of the UN sustainability goals in areas such as education and health; (2) respect for human-centered values and fairness; (3) transparency in the use and operation of AI/S; (4) robust safety; and (5) accountability for the results of AI/S predictions and decisions (OECD, 2019). AI/S is concentrated in a few companies and developed nations. AI/S can perpetrate biases. Of concern is the disparate impact on the less educated, low skilled, women, elderly and low to middle income countries.

Regarding human-centered values and fairness, there are international laws that protect human rights. Human rights include the right to equality, nondiscrimination, freedom of privacy, right to an education and to health. While AI/S can fulfill human rights, it can also create new risks for intentional and accidental human rights violations. Examples of human rights violations is where AI/S is used to predict recidivism and has undetected bias; or where AI/S restricts rights to free expression. The key is to identify risks of harm and vulnerable groups. “[I]n the regulation of expression on social networks, human rights jurisprudence helps demarcate hate speech as a red line” (OECD, 2019: 86).

Since 1980, the OECD has defined personal data as data that can be identified or is an identifiable data subject. OECD members are to ensure there is no discrimination against data subjects. The AI/S challenge is that ‘non-personal data can be correlated with other data and matched to specific individuals, becoming personal ... [and] can increasingly be used to re-identify individuals.’ Further it is becoming hard to distinguish between sensitive and non-sensitive data because some algorithms can infer sensitive information from non-sensitive data (OECD, 2019: 88).

Regarding transparency in the use and operation of AI/S, the focus is on how decisions, recommendations and predictions are made; who participates in the process; and factors used to make decisions. Another area of concern that is more technical is how and whether to allow people to understand how an AI/S is developed, trained and deployed. Approaches to transparency include: (1) giving theoretical guarantees about an AI/S backed by proof; (2) providing empirical evidence that measures a system’s overall performance, demonstrate value or demonstrate system harm; or (3) use humans to explain the computer logic for how a set of inputs reaches a conclusion (OECD, 2019: 92). However, providing transparency may conflict with proprietary trade secrets and other intellectual property rights and need for secrecy.

Future of Life Institute

The Future of Life Institute (FLI) is a charity and outreach organization based in Boston, Massachusetts in the USA that works to ensure that future technologies are beneficial for humanity. They focus on powerful technologies such as nuclear weapons, synthetic biology and AI/S. Their mission is to support research that safeguards life and discover positive ways for humanity to consider new technologies and challenges. They have compiled a listing of 14 areas of concern for the safe and beneficial development of

AI/S and created a website that includes examples of existing policy principles and recommendations (Future of Life Institute, 2020).

One of the areas of concern is entitled ‘surveillance, privacy and civil liberties.’ The principles and recommendations that the FLI has advocated include the Asilomar AI principles, the British Standard on Robots, and the Charlevoix Common Vision for the Future of AI in 2017, the FLI organized the Asilomar Conference on Beneficial AI in Pacific Grove, California. At the conference, the Asilomar AI Principles were created. They are 23 guidelines for the research and development of AI (Future of Life Institute; Sterling, 2018).

The first 5 guidelines are related to research issues. First, the goal of AI/S research should be to create not undirected intelligence, but beneficial intelligence. Second, investments in AI/S should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:

- How can we make future AI/S highly robust, so that they do what we want without malfunctioning or getting hacked?
- How can we grow our prosperity through automation while maintaining people’s resources and purpose?
- How can we update our legal systems to be more fair, efficient, to keep pace with AI/S, and to manage the risks associated with AI/S?
- What set of values should AI/S be aligned with, and what legal and ethical status should it have?

Third, there should be constructive and healthy exchange between AI/S researchers and policymakers. Fourth, the AI/S research culture should be a culture of cooperation, trust, and transparency should be fostered among AI/S researchers and developers. The fifth guideline is called ‘race avoidance’ and advocates that teams developing AI/S should actively cooperate to avoid corner cutting on safety standards.

The next 13 guidelines are related to Ethics and Values. AI/S should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible. If an AI/S causes harm, it should be possible to ascertain why. This is called ‘failure transparency’. With respect to ‘judicial transparency’, any involvement by an autonomous system in judicial decision making should provide a satisfactory explanation auditable by a competent human authority. Designers and builders of advanced AI/S are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications. Highly autonomous AI/S should be designed so that their goals and behaviors can be assured to align with human values throughout their operation. In addition, AI/S should be designed and operated to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.

Regarding personal privacy, people should have the right to access, manage and control the data they generate, given AI/S’ power to analyze and utilize that data. The application of AI/S to personal data must not unreasonably curtail people’s real or perceived liberty. AI/S technologies should benefit and empower as many people as possible. The economic prosperity created by AI/S should be shared broadly, to benefit all of humanity. There needs to be human control over AI/S. Humans should choose how and whether to delegate decisions to AI/S, to accomplish human-chosen objectives. The power conferred by control of highly advanced AI/S should respect and improve, rather than subvert, the social and civic processes on which the health of society depends. Although not relevant to the use of VAPAs, the Future of Life Institute advocates that an arms race in lethal autonomous weapons should be avoided.

The last 5 guidelines are related to longer-term Issues. Strong assumptions regarding upper limits on future AI/S capabilities should be avoided. Advancing AI/S is important. It could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources. Risks posed by AI/S, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact. AI/S that is designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject

to strict safety and control measures. Lastly, superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization.

The FLI also advocates the commitments made at the 2018 G7 Summit in Charlevoix, Quebec, Canada. The summit produced nine documents. One of these was entitled the Charlevoix Common Vision for the Future of Artificial Intelligence (Kirton, 2018). It urges AI/s designers to respect and promote applicable frameworks for privacy and personal data protection. Privacy should be safeguarded through appropriate legal regimes, investments in cybersecurity, enforcement of privacy legislation, communication of enforcement decisions, and informing people about how their personal data may be used by AI/S. Further, promoting research and development in safety, assurance, data quality and data security, privacy protection and transparency.

The G7 leaders made the following 12 commitments to:

1. Endeavour to promote human-centric AI/S and commercial adoption of AI/S, and continue to advance appropriate technical, ethical and technologically neutral approaches by: safeguarding privacy including through the development of appropriate legal regimes; investing in cybersecurity, the appropriate enforcement of applicable privacy legislation and communication of enforcement decisions; informing individuals about existing national bodies of law, including in relation to how their personal data may be used by AI/S; promoting research and development by industry in safety, assurance, data quality, and data security; and exploring the use of other transformative technologies to protect personal privacy and transparency.
2. Promote investment in research and development in AI/S that generates public trust in new technologies and encourage industry to invest in developing and deploying AI/S that supports economic growth and women's economic empowerment while addressing issues related to accountability, assurance, liability, security, safety, gender and other biases and potential misuse.
3. Support lifelong learning, education, training and reskilling, and exchange information on workforce development for AI/S skills, including apprenticeships, computer science and STEM (science, technology, engineering and mathematics) education, especially for women, girls and those at risk of being left behind.
4. Support and involve women, underrepresented populations and marginalized individuals as creators, stakeholders, leaders and decision-makers at all stages of the development and implementation of AI/S applications.
5. Facilitate multi-stakeholder dialogue on how to advance AI/S innovation to increase trust and adoption and to inform future policy discussions.
6. Support efforts to promote trust in the development and adoption of AI/S with attention to countering harmful stereotypes and fostering gender equality. Foster initiatives that promote safety and transparency and provide guidance on human intervention in AI/S decision-making processes.
7. Promote the use of AI/S applications by companies, in particular small and medium-sized enterprises and companies from non-tech sectors.
8. Promote active labor market policies, workforce development and reskilling programs to develop the skills needed for new jobs and for those at risk of being left out, including policies specifically targeting the needs of women and underrepresented populations in order to increase labor participation rates for those groups.
9. Encourage investment in AI/S technology and innovation to create new opportunities for all people, especially to give greater support and options for unpaid caregivers, the majority of whom today are women.
10. Encourage initiatives, including those led by industry, to improve digital security in AI/S and developing technologies, such as the Internet of Things and cloud services, as well as through the development of voluntary codes of conduct, standards or guidelines and the sharing of best practices.

11. Ensure AI/S design and implementation respect and promote applicable frameworks for privacy and personal data protection.
12. Support an open and fair market environment including the free flow of information, while respecting applicable frameworks for privacy and data protection for AI/S innovation by addressing discriminatory trade practices, such as forced technology transfer, unjustified data localization requirements and source code disclosure, and recognizing the need for effective protection and enforcement of intellectual property rights (Kirton, 2018).

IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems

The Institute of Electrical and Electronics Engineers (IEEE) *Global Initiative on Ethics of Autonomous and Intelligent Systems* has developed a treatise of ethical principles, key issues and practical recommendations called “Ethically Aligned Design”. It was written for the general public, academics, engineers, policy makers and manufacturers of autonomous and intelligent systems (A/IS). The goal of this initiative is to bring values-driven ethics into action in businesses at the beginning of the development process for innovations (IEEE, 2020). The eight (8) general principles of ethically aligned design include: 1) human rights, 2) well-being, 3) data agency, 4) effectiveness, 5) transparency, 6) accountability, 7) awareness of misuse and 8) competence. Recommendations for creators of A/IS tools are provided.

In 2005, John Ruggie was appointed as the Special Representative (SRSG) on Business and Human Rights under Kofi Anan in the United Nations (UN). In June 2008, Ruggie proposed a policy framework for better managing business and human rights challenges (United Nations, 2008a,b). It is based on the following pillars: (1) the state has a duty to protect against human rights abuses by third parties, including businesses; (2) corporations’ responsibility is to respect human rights; and (3) there is a need for greater access by victims to effective judicial and non-judicial remedies. The Human Rights Council operationalized this policy framework on business and human rights (2008). The policy framework is known as the ‘Ruggie Principles’. Ruggie Principles provide the internationally recognized legal framework for human rights standards and accounts for the impact of technology on individuals while also addressing inequalities, discriminatory practices, and the unjust distribution of resources. IEEE applies the Ruggie Principles. IEEE advocates that A/IS national policies and business regulations be founded on a rights-based approach using the Ruggie Principles. These include: 1) responsibility, 2) accountability, 3) participation, 4) nondiscrimination, 5) empowerment, and 6) corporate responsibility.

The first issue is how to ensure that A/IS supports, promotes, and enables internationally recognized legal norms. Responsibility involves identifying entities that hold rights and that have duties to other entities. The duty bearers have an obligation to fulfill all human rights. Accountability is defined as requiring duty bearers to behave responsibly, represent the greater public interest, and to be open to public scrutiny of their A/IS policies. In addition, there should be a high degree of participation from duty bearers, rights holders, and other interested parties.

The practice of A/IS should be underlined with the principles of nondiscrimination, equality, and inclusiveness. Particular attention must be given to vulnerable groups such as minorities, indigenous peoples, or persons with disabilities. Rights holders should be empowered to claim and exercise their rights. Regarding corporate responsibility, companies are responsible in A/IS development when they comply with the rights-based approach that do not lead to human rights violations.

The second issue is related to the development of government expertise in A/IS. Policy makers should support the development of expertise required to create a public policy, legal, and regulatory environment that allows innovation to flourish while protecting the public and gaining public trust. IEEE advocates that technologists spend extended time in political offices; or that policy makers work with organizations that operate at the intersection of technology policy, technical engineering, and advocacy. This will enhance the technical knowledge of policy makers, strengthen ties between political and technical communities, and contribute to the formulation of effective A/IS policy.

There is also a need for the cross-border sharing of best practices around A/IS legislation, consumer protection, workforce transformation, and economic displacement stemming from A/IS-based automation.

This can be done through governmental cooperation, knowledge exchanges, and by building A/IS components into venues and efforts surrounding existing regulation, e.g., the GDPR.

Because A/IS involve rapidly evolving technologies, there is a need for both workforce training in A/IS areas and long-term STEM educational strategies, along with ethics courses, are needed beginning in primary school and extending into university or vocational courses. These strategies will foster A/IS expertise in the next generation of many groups, e.g., supervisors of critical systems, scientists, and policy makers.

The third issue is how to ensure that governance and ethics are core components in A/IS research, development, acquisition, and use. IEEE recommends that national and international standards for A/IS be developed in a manner that enables the efficient and effective public and private sector investments. Nations should consider their own ethical principles and develop a framework for ethics that each country could use to reflect local systems of values and laws. Governments should prioritize funding A/IS research that identify approaches and A/IS governance challenges. There is a need for research that results in identifying national and global models of A/IS governance, their benefits and the adequacy of how they address A/IS societal needs.

IEEE advocates that the standards development process include the participation of a diverse set of stakeholders. Standards should address A/IS issues such as fairness, security, transparency, understandability, privacy, and societal impacts of A/IS. A global framework for identification and sharing of these and other issues should be developed. The standards should incorporate independent mechanisms to properly vet, certify, audit, and assign accountability for the A/IS applications.

The fourth issue is how to create policies for A/IS to ensure public safety and responsible A/IS design. The governance and safe deployment of policies and regulations for A/IS should be developed by nations using a process that is based on informed input from a range of expert stakeholders, including academia, industry, NGOs, and government officials. A/IS policies should foster the development of economies able to absorb A/IS. In addition, there is a need to address the effect of A/IS on employment and income and how to ameliorate certain societal conditions. New models of public-private partnerships should be studied. Policies for A/IS should remain founded on a rights-based approach. Policy makers should be prepared to address issues that will arise when innovative and new practices enabled by A/IS are not consistent with current law.

The fifth issue is how to educate the public on the ethical and societal impacts of A/IS. IEEE recommends that an international multi-stakeholder forum be created. It should include commercial, governmental, and other civil society groups to determine the best practices for using and developing A/IS. The proposed forum's deliberations into international norms and standards. There is a need for increased funding for interdisciplinary research and communication on topics ranging from basic research on intelligence to principles of ethics, safety, privacy, fairness, liability, and trustworthiness of A/IS. Societal aspects should be addressed both at an academic level and through the engagement of business, civil society, public authorities, and policy makers. Educational outreach also needs to be conducted to inform the public on A/IS research, development, applications, risks and rewards, along with the policies, regulations, and testing that are designed to safeguard human rights and public safety. A broad range of A/IS educational programs need to be developed to ensure that lawyers, legislators, and A/IS workers are well informed about issues arising from A/IS. This includes the need for measurable standards of A/IS performance, effects, and ethics, and the need to mature the still nascent capabilities to measure these elements of A/IS.

Further, there are eight (8) principles that include: 1) human rights, 2) well-being, 3) data agency, 4) effectiveness, 5) transparency, 6) accountability, 7) awareness of misuse and 8) competency. Regarding the first principle, to best respect *Human Rights*, society must assure the safety and security of A/IS so that they are designed and operated in a way that benefits humans. Governance frameworks, such as standards and regulatory bodies, should be established to oversee processes which ensure that the use of A/IS does not infringe upon human rights, freedoms, dignity, and privacy, and which ensure traceability. This will contribute to building public trust in A/IS. There is a need for a way to translate existing and forthcoming legal obligations into informed policy and technical considerations. Such a method should allow for diverse

cultural norms as well as differing legal and regulatory frameworks. A/IS should always be subordinate to human judgment and control. A/IS should not be granted rights and privileges equal to human rights.

Regarding the second principle, A/IS should prioritize human *Well-being* as an outcome in all system designs. The third principle of *Data Agency* is achieved when individuals specify their online agent for case-by-case authorization decisions as to who can process what personal data for what purpose. Thus, individuals should be empowered with the ability to access and securely share their data; and maintain control over their identity. For minors and those with diminished capacity to make informed decisions, current guardianship approaches should be viewed to determine suitability.

The fourth Principle of Effectiveness necessitates that A/IS creators and operators provide evidence in the form of metrics or benchmarks of the effectiveness and fitness for purpose, meeting objectives, and adhering to standards and remaining within risk tolerances. The evidence should be readily obtainable by all interested parties including users, safety certifiers, and regulators. There is also an important need for guidance on how to interpret and respond to the metrics generated by the systems. To the extent possible, industry associations or other organizations, e.g., IEEE and ISO, should work toward developing standards for the measurement and reporting on the effectiveness of A/IS.

The fifth principle of *Transparency* refers to the need for A/IS decisions to be always discoverable. The mechanisms for transparency include providing users with a “why-did-you-do-that” button which, when pressed, causes the robot to explain the action it just took. Validation or certification agencies can have access to the algorithms underlying the A/IS and how they have been verified. Accident investigators should have access to secure storage of sensor and internal state data comparable to a flight data recorder or black box.

The sixth principle of *Accountability* involves creating and operating A/IS to provide an unambiguous rationale for decisions made. To best address issues of responsibility and accountability. Legislatures and courts should clarify responsibility, culpability, liability, and accountability for A/IS, where possible, prior to development and deployment so that manufacturers and users understand their rights and obligations. Further, A/IS developers should remain aware of, and consider, the diversity of existing cultural norms among the groups of users of these A/IS. Multi-stakeholder ecosystems should be developed to help establish norms where they do not exist because A/IS-oriented technology and their impacts are too new. These ecosystems would include, but not be limited to, representatives of civil society, law enforcement, insurers, investors, manufacturers, engineers, lawyers, and users. The norms can mature into best practices and laws.

Systems for registration and record-keeping should be established so that it is always possible to find out who is legally responsible for a particular A/IS. Creators, including manufacturers along with operators, of A/IS should register key, high-level parameters, including: 1) intended use, 2) training data and training environment, 3) sensors and real-world data sources, 4) algorithms, 5) process graphs, 6) model features, 7) user interfaces, 8) actuators and outputs, and 9) optimization goals, loss functions, and reward functions.

The seventh principle of *Awareness of Misuse* is where creators safeguard against all potential misuses and risks of A/IS in operation. Raising public awareness of potential misuse includes providing ethics education and security awareness that sensitizes society to the potential risks of misuse of A/IS. It is important to give notice in data privacy warnings that some smart devices will collect their users’ personal data. Delivering ethics education; and educating government, lawmakers, and enforcement agencies about these A/IS issues are important so citizens can work collaboratively with these agencies to understand safe use of A/IS. For example, the same way police officers give public safety lectures in schools, they could provide workshops on safe use and interaction with A/IS.

The eighth principle is that there needs to be creator and operator *Competence* to ensure the safe and effective operation of A/IS. Creators of A/IS should specify the types and levels of knowledge necessary to understand and operate A/IS applications. Integrated safeguards are necessary and include notifications, warnings to operators in certain conditions, limiting functionalities for different levels of operators (e.g., novice vs. advanced), system shut-down procedures in potentially risky conditions, any preconditions for their effective use, who is qualified to operate them, what training is required for operators, how to measure A/IS performance, and what should be expected from the A/IS.

British Standards Institute

The British Standards Institution (BSI) published the British Standard (BS) 8611 for the ethical design and application of robots and robotic systems (British Standards Institute, 2016). BS 8611 identifies potential ethical harms and provide guidelines on the safe design of robots. It defines ethical harm as anything that compromises psychological and/or societal environmental well-being. This includes stress, embarrassment, anxiety, addiction, discomfort, deception, humiliation, and being disregarded. These issues may be in relation to factors such as gender, race, religion, age, disability and/or poverty.

BS 8611 provides an ethical risk assessment that includes ethical issues, hazards and risks. The issues are societal, application, financial and environmental. The societal issues include loss of trust, intentional or unintentional deception, anthropomorphizing, privacy and confidentiality, lack of respect for cultural diversity and pluralism, robot addiction, and employment. The application issues are misuse, unsuitable divergent use, the dehumanization of humans in relationship with robots, a robot gaining inappropriate trust in human, and self-learning systems exceeding their remit. Ethical assessments need to be undertaken with regards to various human-robot interaction scenarios. The scenarios include unauthorized use, reasonably foreseeable misuse, the uncertainty of situations to be dealt with, psychological effects of failure in the control system, possible reconfiguration of the system and ethical hazards association with specific robot applications.

Norms of robots need to be considered when designing and building robots. These include that robots should not be designed solely or primarily to kill or harm humans, that humans and not robots are responsible agents, and that they should be secure and not deceptive. Other norms include privacy by design. Roboticists are encouraged to work responsibly by engaging with the public, addressing public concerns, demonstrating commitment to best practices, working with experts from other disciplines and the media and providing clear instructions.

Privacy Coalition

The Privacy Coalition is sponsored by the Electronic Privacy Information Center (EPIC). Since 1994, EPIC has served as a public research center located Washington, DC in the USA. EPIC draws public attention to privacy and civil liberties issues, the protection of privacy, freedom of expression and democratic values (EPIC, 2020). The Privacy Coalition is a nonpartisan coalition of more than 50 consumer, civil liberties, educational, family, library, labor and technology organizations that agreed to a Privacy Pledge and have held meetings since 1995. The Privacy Pledge notes the Fourth Amendment rights of people to be secure in their persons, houses, papers and effects from unreasonable searches and seizures. Members are to pledge to their constituents and to the American people that they support a privacy framework that safeguards the rights of Americans in the information age. “The framework includes:

1. the Fair Information practices: the right to notice, consent, security, access, correction, use limitations, and redress when information is improperly used,
2. independent enforcement and oversight,
3. promotion of genuine Privacy Enhancing Technologies that limit the collection of personal information and legal restrictions on surveillance technologies such as those used for locational tracking, video surveillance, electronic profiling, and workplace monitoring, and
4. a solid foundation of federal privacy safeguards that permit the private sector and states to implement supplementary protections as needed” (Privacy Coalition, 2020).

Table 1 summarizes the features advocated by each of the six organizations discussed above.

ANALYSIS OF THE POLICY GUIDELINES

We have analyzed the AI/S policy guidelines of the six prominent organizations referenced above and placed them in five categories. The categories contained a minimum of 2 traits and a maximum of 7 traits. There was a wide variability in categories and traits articulated by these organizations. The Privacy Coalition’s policy covered two categories with a total of three traits while the IEEE policy covered all

categories and 20 traits. The only trait that was included in all the organization’s policy statements was that AI/S’s must be Safe and Secure.

We defined the five categories covered by the guidelines as *Mastery*, *Justice*, *Human Rights*, *Confidentiality* and *Reliability*. An AI/S possesses *Mastery* when it can apply or use a set of related knowledge, skills, and abilities required for it to successfully perform the tasks it was designed to perform in its intended work setting. We have subdivided AI/S *Mastery* into five traits: It must be competent; it must be effective – e.g., it must be able to accomplish its intended task; it must have minimum potential to disrupt jobs and the nature of work; it must have a registration system; and, it must have a record keeping system. While all these are included in the IEEE policy document, none were included in the OECD, FLI, or Privacy Coalition’s guidelines, perhaps reflecting the difference in mindset between technical and non-technical organizations.

An AI/S must function with *Justice*. While it is reasonable to argue that artificial systems will treat all users equally, *Justice* means that AI/S’s must be able to detect when particular users need different treatment to derive the same benefit from their use as others. We have divided this category into five traits: A just AI/S must be non-discriminatory by design; it must be fair; it must be able to detect and correct biases; it must contain provisions to handle pluralism, inclusiveness and cultural diversity, and it must be equitable. At least one of these traits was included in every organization’s policy document.

TABLE 1
SUMMARY OF FEATURES ADVOCATED AMONG THE SIX SETS OF
POLICY GUIDELINES

AI/S features	Partnership on AI	OECD	BS 8611	FLI	IEEE	Privacy Coalition
Safe/secure	✓	✓	✓	✓	✓	✓
Trustworthy	✓		✓	✓	✓	
Ethical	✓		✓		✓	
Nondiscriminatory		✓	✓			
Fair	✓	✓		✓	✓	✓
Transparent	✓	✓		✓	✓	
Accountable	✓	✓			✓	
Effective					✓	
Competent					✓	
Detect & Corrects Biases	✓	✓				
Privacy			✓	✓	✓	✓
Minimum Potential to disrupt jobs & nature of work	✓		✓		✓	
Registration System					✓	
Record Keeping System					✓	
Reflects Clear Understanding & confidence about situations and human control	✓			✓	✓	
Reflects Thoughtful collaborations/ open dialogue in R&D	✓			✓	✓	

Aligned with human values				✓		
Responsible		✓	✓	✓	✓	
Public Awareness/ educational outreach					✓	
Respects democratic values		✓				
Respects human rights		✓		✓	✓	
Provisions for pluralism, inclusiveness & cultural diversity		✓	✓		✓	
Equitable		✓		✓	✓	
Well-being		✓	✓	✓	✓	

As discussed in this paper, a frequent use of AI/S’s is to serve as Voice Activated Personal Assistants in the home, in healthcare, in banks, and in education. People develop relationships with their VAPAs and make them part of their families and trust what they are told by them. Consequently, VAPAs in particular and AI/S’s in general must be designed so as to not provide advice that will knowingly lead their users to violate the *Human Rights* of others. *Human Rights* may be viewed as a set of moral principles that apply to everyone and countries often incorporate human rights into their own national, state and local laws (The Advocates for Human Rights). We have subdivided this category into five traits that AI/s’s must possess: They must align with human values; they must reflect a clear understanding and confidence about situations and human control that may indicate a violation of human rights; they must respect human rights; they must be designed to support democratic values (or their violation); and they must be designed to promote human well-being. The Privacy Coalition’s guideline did not stipulate any human rights traits in their guidelines, while the Partnership on AI only included “Reflects clear understanding and confidence about situations and human control” in their guidelines.

An AI/S must maintain *Confidentiality*. We have divided this category into the traits of Privacy and Secure/Safe. Privacy was recognized as a basic human right in the International Bill of Rights in 1948 (United Nations, 1948). In the context of this paper, privacy refers to data and information privacy and it deals with what AI/S data in an AI/S can be shared with third parties. We have associated the two traits safety/security and privacy with this category. Whereas privacy concerns the safeguarding of user identity, security concerns the protection against unauthorized access to data. While the Partnership on AI document and the OECD documents do not specifically address privacy issues, all organization’s guidelines address security in the documents.

The fifth category we have defined based on the organization’s policy guidelines is *Reliability*. In its simplest form, it describes something that you can depend on. While AI/S’s cannot be accountable or take responsibility for its own actions or responses, their designers must. To do so, we have defined the following seven traits that designers/manufacturers of AI/S’s must possess: They must be accountable – i.e. someone in the organization must have ultimate responsibility for their performance; they must be ethical; they must educate the users of their devices; they must have effective teamwork during the R&D phase of the AI/S development via thoughtful collaborations and open dialogue; they must assign clear responsibility for their system; they must be transparent; and they must be trustworthy. All organizations include multiple Reliability traits in the policy guideline except for the Privacy coalition, which includes none.

Table 2 summarizes the above discussion by indicating which categories and traits are included in the policy guidelines of each of the six organizations examined.

FROM TRAIT TO TOOL

So far in this paper, we have presented evidence that the advent of the COVID-19 pandemic has accelerated the development and use of AI/S's, including VAPAs, in private homes, banks, health care and educational institutions. Millions of people across the globe will be interacting with these devices in the most private matters. Yet, as we have shown, privacy could not be guaranteed before COVID. And it cannot be guaranteed after COVID. Privacy is not the only concern. With the flood of new skills and applications being launched by both public and private organization, the question remains as to how the user population can be informed about the strengths, weaknesses, opportunities and threats associated with the use of a particular AI/S and or VAPA?

High profile incidents of cybersecurity data breaches motivated a study of preparing millennials to be more socially responsible digital citizens (Burgess-Wilkerson, Hamilton, Garrison, & Robbins, 2019). Similar advocacy and pressure need to continue to be placed on AI/S developers by policy and law makers. With the rise of data breaches, consumers are increasingly at risk. "If the US were to draft a federal statute similar to the GDPR, the regulation needs to be able to address innovative business models [of personal data collection and sales] that are on the rise" (Garrison, 2019).

As described herein, several prestigious organizations have addressed this issue through the development of a set of policy guidelines which we have analyzed and categorized. They collectively indicate that an AI/S must have mastery of their domain(s), it must make provisions be just so that a variety of populations have equal access to it, it's artificial intelligence should understand and take into account human rights when supporting human endeavors, it should keep its information in a confidential environment and protect its content from unauthorized use, and it should be reliable in terms of the information it provides and actions it prescribes. Having said what an AI/S should do begs the question of how the consumer can know that it does?

Whether an AI/S application conforms to the five categories and their corresponding traits that we have extracted from the policy guidelines of the six organizations we studied is unlikely to be a categorical yes or no. Instead, it is likely to be an indication of the degree to which it meets these policy guidelines. For example, one may be exceptionally competent compared to others, while not exceptionally trustworthy. Thus, the question arises as to how we can "measure" the extent to which and AI/S conforms to the guidelines and who should do the measuring.

TABLE 2
COMPARISON OF CATEGORIES AND TRAITS BY ORGANIZATION POLICY GUIDELINES

CATEGORY	TRAIT	DESCRIPTION	POLICY SOURCES					
			Partnership on AI	OECD	BS 8611	FLI	IEEE	Privacy Coalition
Confidentiality	C ₁	Privacy			✓	✓	✓	✓
	C ₂	Safe/secure	✓	✓	✓	✓	✓	✓
Human Rights	H ₁	Aligned with human values				✓		
	H ₂	Reflects clear understanding & confidence about situations and human control	✓			✓	✓	
	H ₃	Respects democratic values		✓				
	H ₄	Respects human rights		✓		✓	✓	

	H ₅	Well-being		✓	✓	✓	✓	
Justice	J ₁	Detects & Corrects Biases	✓	✓				
	J ₂	Equitable		✓		✓	✓	
	J ₃	Fair	✓	✓		✓	✓	✓
	J ₄	Nondiscrimatory		✓	✓			
	J ₅	Provisions for pluralism, inclusiveness & cultural diversity		✓	✓			✓
Mastery	M ₁	Competent					✓	
	M ₂	Effective					✓	
	M ₃	Minimum Potential to disrupt jobs & nature of work	✓		✓		✓	
	M ₄	Record keeping System					✓	
	M ₅	Registration System					✓	
Reliability	R ₁	Accountable	✓	✓			✓	
	R ₂	Ethical	✓	✓	✓		✓	
	R ₃	Public awareness/ educational outreach					✓	
	R ₅	Responsible		✓	✓	✓	✓	
	R ₆	Transparent	✓	✓		✓	✓	
	R ⁷	Trustworthy	✓		✓	✓	✓	

How to Measure – Developing a Tool

To measure the extent to which an AI/S conforms to the policy guidelines, we use the theoretical framework laid out by Churchman and Ackoff (1954) and applied by Gearing, Swart, and Var (1974). We first will develop a set of relative importance weights for each of the traits defined in Table 2. Collectively, the weights will sum to 1 (or 100%). An AI/S will be “measured” as to the extent it conforms to guidelines by having a yet to be defined group of experts assess the extent to which the subject AI/S conforms to the letter and intent of each of the traits, as defined by its originating organization. The experts will assign a score between zero and 100 to each trait. Zero meaning that the trait is not addressed by the AI/S and 100 if it is fully addressed. The result will be a composite score between zero and 100 that can be assigned to the AI/S by this yet to be defined group of experts and, if appropriate, divulged to consumers.

To illustrate the approach, we note that the six organizations have identified a total of 24 traits that define the five categories encompassing their policy guidelines. We define the importance of a trait as the ratio of the number of check marks it received in Table 2 to the total number of check marks in that table. Thus, the more organizations include a particular trait in the guidelines, the more important the trait. In total, the combined policy guidelines in Table 2 make 66 references to traits, some more than once. The trait C₁ in the Confidentiality category is referenced by four organizations. Thus, we give it an importance weight of 4/66, or 0.060606. Similarly, trait H₁ in the Human Rights category is referenced only once (by FLI). Thus, we give it an importance weight of 1/66, or 0.015152. Table 3 list weights, as computed per the above convention, for each trait. We have also defined the relative importance of each category as the sum of the relative importance of their constituent traits. Thus, by our convention, *Reliability* is the most important category, followed by *Justice*, *Human Rights*, *Confidentiality*, and *Mastery*, in that order.

Table 3 is, in effect, the measuring stick that will be used to assess a candidate AI/S’s adherence to the combined policy guidelines. Table 4 illustrates how through a fictitious example. The yet to be determine rating body has been asked to rate a new AI/S, represented by the Android Icon in the chart. After doing due diligence, they compare their notes and score the Android device based on the extent it adheres to each trait. A score of zero indicated that that trait has been ignored and a score of 100 means that it has been fully implemented. After noting the trait scores, these are multiplied by the trait weights and summed. In the example, this candidate receives a “Design Rating” 44.47. This rating reflects the degree to which it

satisfies the mastery in which it performs its tasks, its reliability in performance, and the prevalent justice and human right norms of the place(s) it will be used. A perfect “Design Rating” would require that it receive a score of 100 on every trait.

DISCUSSION

Nearly half of US adults say they use VAPAs; 14% use them on computers and 8% use them on stand-alone devices (Pew Research Center, 2017). To gain an understanding of VAPA user perceptions of privacy, we examined literature related to privacy issues with their current use in: (1) private homes, (2) healthcare facilities, (3) banks, (4) K-12 classrooms and (5) higher education. First, there is an exploration of what the expressions of concerns are in current affairs. This section is followed by a discussion of what policy guidelines are calling for. Six (6) sets of artificial intelligent systems (AI/S) policy guidelines were reviewed. This is followed by an analysis of the current concerns and policy guidelines.

With the exploding consumption of AI/S devices which was accelerated by the COVID pandemic, but which is certain to continue to increase, there appears to be a growing need for an institution or agency that should be responsible for the administration and provision of protective measures regarding AI/S consumer rights. In addition to protecting the public against unfair and unsafe practices in the marketplace, they should also safeguard the consumer against unethical and/or unauthorized use of the data that such devices engender. However, it should not absolve the consumer from taking personal responsibility and the environmental costs and consequence of what they purchase and how they use it.

We believe that a first step in that direction is the establishment of an impartial group or agency to develop what we have dubbed as “Design Ratings.” These ratings must be arrived at by a consensus of experts who understand both the categories and the traits contained in the policy guidelines of the six policy organizations studied herein. One possibility is that each of the six organizations “donate” one of their experts to serve in such a group and oversee the development of these ratings. It is not necessary for this “Design Ratings” system to become a legal mandate to alleviate the concerns noted in our review of current affairs. Its voluntary use by AI/S, IAC, and VAPA product developers will likely have the positive impact of alleviating end user concerns as did the “Good Housekeeping Seal of Approval”. Since 1909, the Good Housekeeping Institute of product testing has helped consumers rest assured that products bearing their seal has been extensively vetted by expert engineers, scientists, and analysts (Good Housekeeping Institute, 2020). Here, the “Design Ratings” refers to adherence to AI/S policy guidelines which are much more extensive than the product safety, quality and value concerns addresses by the Good Housekeeping Institute.

TABLE 3
TRAIT AND CATEGORY RELATIVE IMPORTANCE WEIGHTS

CATEGORY	TRAIT	DESCRIPTION	TRAIT WEIGHT	CATEGORY WEIGHT
Confidentiality	C ₁	Privacy	0.06060606	0.151515152
	C ₂	Safe/secure	0.09090909	
Mastery	M ₁	Competent	0.01515152	0.106060606
	M ²	Effective	0.01515152	
	M ³	Minimum Potential to disrupt jobs & nature of work	0.04545455	
	M ⁴	Record keeping System	0.01515152	
	M ⁵	Registration System	0.01515152	
Justice	J ₁	Detects & Corrects Biases	0.03030303	0.227272727
	J ₂	Equitable	0.04545455	
	J ₃	Fair	0.07575758	
	J ₄	Nondiscriminatory	0.03030303	

	J ₅	Provisions for pluralism, inclusiveness & cultural diversity	0.04545455	
Human Rights	H ₁	Aligned with human values	0.01515152	0.181818182
	H ₂	Reflects clear understanding & confidence about situations and human control	0.04545455	
	H ₃	Respects democratic values	0.01515152	
	H ₄	Respects human rights	0.04545455	
	H ₅	Well-being	0.06060606	
Reliability	R ₁	Accountable	0.04545455	0.33333333
	R ₂	Ethical	0.04545455	
	R ₃	Public awareness/ educational outreach	0.01515152	
	R ₄	Reflects Thoughtful collaborations/ open dialogue in R&D	0.04545455	
	R ₅	Responsible	0.06060606	
	R ₆	Transparent	0.06060606	
	R ₇	Trustworthy	0.06060606	

CONCLUSIONS

The explosive growth in the use of VAPA's together with their rapidly increasing sophistication is placing personal privacy and confidentiality at risk. Consumers are caught in a dilemma. They either forego the convenience of a VAPA or risk their privacy and confidentiality, even in their own homes. We have shown that despite assertions to the contrary, personal information can and will be used. To date, there is no user-friendly way to assess the social, ethical, and legal ramifications associated with the acquisition of a VAPA.

In this research we have laid out what we believe is a first of kind outline of how consumers may be better informed about what they are getting in a VAPA, not just from a functionality and quality point of view, but also about the social, ethical and legal risks associated with bringing it into their home, school, bank, or medical office. We have proposed a model that requires that an importance weight be determined for each of the traits that has been defined by one or more of six organizations that have studied policy issues associate with VAPAs. We have adopted the view that the more organizations adopted the same or similar trait in their policy guidelines, the more important that trait must be. However, there are several other approaches that can be invoked to weight criteria (Gearing et al., 1974; Armacost et al., 1994). These all require the participation of panels of experts, which opens Pandora's box regarding who should be chosen and why as an expert. Regardless of how the weights are determined, they should be kept in place until a good and valid reason arises to change them.

TABLE 4
EXAMPLE OF DETERMINING THE “DESIGN RATING” OF A NEW DEVICE

AI/S
 DEVICE



CATEGORY	TRAIT	DESCRIPTION	TRAIT WEIGHT	TRAIT SCORE	WEIGHT*SCORE
Confidentiality	C ₁	Privacy	0.060606061	60	3.636363636
	C ₂	Safe/secure	0.090909091	50	4.545454545
Mastery	M ₁	Competent	0.015151515	20	0.303030303
	M ₂	Effective	0.015151515	30	0.454545454
	M ₃	Minimum potential to disrupt jobs & nature of work	0.045454545	70	3.181818182
	M ₄	Record keeping System	0.015151515	10	0.151515152
	M ₅	Registration System	0.015151515	50	0.757575758
Justice	J ₁	Detects & Corrects Biases	0.03030303	40	1.212121212
	J ₂	Equitable	0.045454545	10	0.454545455
	J ₃	Fair	0.075757576	10	0.757575757
	J ₄	Nondiscriminatory	0.03030303	100	3.03030303
	J ₅	Provisions for pluralism, inclusiveness & cultural diversity	0.045454545	0	0
Human Rights	H ₁	Aligned with human values	0.015151515	0	0
	H ₂	Reflects clear understanding & confidence about situations and human control	0.045454545	60	2.727272727
	H ₃	Respects democratic values	0.015151515	0	0
	H ₄	Respects human rights	0.045454545	0	0
	H ₅	Well-being	0.060606061	80	4.848484848
Reliability	R ₁	Accountable	0.045454545	75	3.409090909
	R ₂	Ethical	0.045454545	80	3.636363636
	R ₃	Public awareness/ educational outreach	0.015151515	60	0.909090909
	R ₄	Reflects Thoughtful collaborations/ open dialogue in R&D	0.045454545	30	1.363636364
	R ₅	Responsible	0.060606061	80	4.848484848
	R ₆	Transparent	0.060606061	0	0
	R ₇	Trustworthy	0.060606061	70	4.242424242
				SUM=	44.46969697

We suggested the creation of an agency modelled after the Good House Keeping Institute, that can test VAPAs and determine their “Design Rating.” This institute (or whatever) should be staffed by experts who understand both the categories and the traits contained in the policy guidelines of the six policy organizations studied herein. One possibility is that each of the six organizations “donate” one of their experts to serve in such a group and oversee the development of these ratings. However, maintaining such an organization free from conflicts of interest may be more feasible if it were staffed by independent professional funded along similar lines as the professionals in the Good House Keeping Institute.

While the devil is in the details, we believe that this research has shown a direction for making strategic innovations in the developments of VAPAs sustainable by protecting the social, ethical and legal rights of all consumers.

REFERENCES

- Abdolrahmani, A., Kuber, R., & Branham, S.M. (2018). “Siri Talks at You”: An Empirical Investigation of Voice-Activated Personal Assistant (VAPA) Usage by Individuals Who are Blind. *ASSETS*, pp. 249–258. Galway, Ireland: Association for Computing Machinery (ACM).
- Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., & Kapadia, A. (2015). Privacy concerns and behaviors of people with visual impairments. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 3523–3532. Seoul, Republic of Korea: Association for Computing Machinery (ACM).
- Allen, S. (2018). Privacy in the Twenty-First Century Smart Home. *The Journal of High Technology Law*, 19(1), 162–191.
- Anderson, T. (2018). N.H. judge orders Amazon to provide Echo recordings in double murder case. *Boston Globe*.
- Armocost, R., Compton, P., Mullens, M., & Swart, W. (1994). An AHP Framework for Prioritizing Customer Requirements in QFD: An Industrialized Housing Application. *IIE Transactions*, 26(4), 72–79.
- Asimov, I. (1950). Runaround. In *I, Robot (The Isaac Asimov Collection)*. New York, NY: Doubleday.
- Augusto, J.C. (2009). Ambient intelligence: Opportunities and consequences of its use in smart classrooms. *Innovation in Teaching and Learning in Information and Computer Sciences*, 8(2), 53–63.
- Bank of America. (2020). *Meet Erica, Your Financial Digital Assistant From Bank of America*. Retrieved July 6, 2021, from <https://promo.bankofamerica.com/erica/>
- Beach, S., Schulz, R., Downs, J., Matthews, J., Barron, B., & Seelman, K. (2009). Disability, age, and informational privacy attitudes in quality of life technology applications: Results from a national web survey. *ACM Transactions on Accessible Computing (TACCESS)*, 2(1), 1–21.
- Bedi, M. (2013). Facebook and interpersonal privacy: Why the third party doctrine should not apply. *Boston College Law Review*, 54, 1–71.
- BESA. (2018a). *Adopting a forward-thinking approach to E-safety. Insights*. London, UK: British Educational Suppliers Association (BESA).
- BESA. (2018b). *Are you GDPR ready? Insights*. London, UK: British Educational Suppliers Association (BESA).
- Boccella, K. (2019). Voice of Authority: Systems like Alexa are helping teachers in the classroom, and kids are listening. *The Philadelphia Inquirer*, p.B1
- Botelho, S. (2018). *Adapting computer policies to cover new risks*. University Business.
- British Standards Institute. (2016). *Robots and robotic devices: Guide to the ethical design and application of robots and robotic systems* (Vol. BS 8611). British Standards Publication.
- Brown, D. (2019). Alexa accused of secret recordings. *USA Today*.
- Brown, E.A. (2018). *The privacy risks of AI*. District Administration: Professional Media Group, LLC.
- Bubar, J. (2018). Does Facebook Know Too Much? *New York Times Upfront*, 151(1).

- Burgess-Wilkerson, B., Hamilton, C., Garrison, C., & Robbins, K. (2019). Preparing Millennials as Digital Citizens and Socially and Environmentally Responsible Business Professionals in a Socially Irresponsible Climate. *Proceedings of the 83rd Annual Conference of the Association for Business Communication*. Miami, FL: Association for Business Communication.
- Burkett, C. (2017). I call Alexa to the stand: The privacy implications of Anthropomorphizing virtual Assistants accompanying smart-home technology. *Vanderbilt Journal of Entertainment and Technology Law*, 20(4), 1181–1217.
- Carpenter v. United States, 585 U.S. __ (U.S. Supreme Court June 22, 2018). Retrieved May 18, 2021, from <https://supreme.justia.com/cases/federal/us/585/16-4021/>
- Carroll, R. (2015). Goodbye privacy, hello ‘Alexa’: Amazon Echo, the home robot who hears it all. *The Guardian*.
- Children's Internet Protection Act (CIPA), P.L. 106-554, Title XVII § 1701-1741, 114 STA. 2763A-336 to 353 (2000).
- Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501-6505; 16 C.F.R. 312. (1998).
- Churchman, C.W., & Ackoff, R.L. (1954). An approximate measure of value. *Journal of the Operations Research Society of America*, 2(2), 172–187.
- Cohen, J.E. (1999). Examined lives: Informational privacy and the subject as object. *Stan. L. Rev.*, 52, 1373–1438.
- Consent Act, S. 2639, 115th Congress. (2018).
- Cowan, B.R., Pantidi, N., Coyle, D., Morrissey, K., Clarke, P., Al-Shehri, S., . . . Bandeira, N. (2017). “What can I help you with?”: Infrequent users' experiences of Intelligent Personal Assistants. *Mobile HCI Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 1–12).
- Cozens, C. (2001). Microsoft cuts ‘Mr Clippy’. *The Guardian*.
- Crist, C. (2019). Voice activated. *District Administration*, pp. 43–45.
- Crosman, P. (2017a). Alexa, Let's Talk Money USAA wants its members to feel free to chat up the bot. *American Banker*, 127(9).
- Crosman, P. (2017b). B of A gives its bot time to become a banker. *American Banker*, 182(94).
- Crosman, P. (2017c). USAA lets members bare their financial souls to Alexa. *American Banker*, 182(148).
- Crosman, P. (2018). Mad about erica: Why a million people use Bank of America's chatbot. *American Banker*, 183(114).
- Davie, N., & Hilber, T. (2018, April 14–16). Opportunities and Challenges of Using Amazon Echo in Education. *Proceedings of the 14th International Association for Development of the Information Society (IADIS) International Conference on Mobile Learning*. Lisbon, Portugal: IADIS.
- Davis, A. (2018). Amazon Alexa in the classroom ‘will help shy children put up their hands’: Artificial intelligence in the classroom will be a good thing says chairman of the HMC group of private schools. *London Evening Standard*.
- Day, M. (2019a). Alexa in the classroom? Amazon's voice assistant leads kids’ story time. *National Post's Financial Post & FP Investing (Canada)*, p.FP8.
- Day, M., Turner, G., & Drozdiak, N. (2019b). Amazon workers are listening to what you tell Alexa. *Daily Herald*.
- Desai, K., & Choudhari, A. (2019). ‘Alexa’ turns teacher for kids in rural areas. *The Times of India*.
- Duijst, D. (2017). *Can we improve the User Experience of Chatbots with Personalisation?* Master’s Thesis. University of Amsterdam.
- Economist. (2017). For my next trick Looking Ahead. *The Economist*, 422, 12.
- EFF. (2017). *EFF Applauds Amazon for pushing back on request for Echo data* (Vol. 2020). Electronic Frontier Foundation (EFF).
- EFF. (2019). *Smart Home Tech, Police and Your Privacy: Year in Review 2019* (Vol. 2020). Electronic Frontier Foundation (EFF).
- EFF. (2020). *EFF Turns 30 this year!* (Vol. 2020). Electronic Frontier Foundation (EFF).

- EPIC. (2020). *EPIC - About EPIC* (Vol. 2020). Electronic Privacy Information Center (EPIC).
- EU GDPR. (2018). *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 1191 (European Union 2016)*.
- Executive Order No.13859. (2019). *Artificial Intelligence for the American People*. Retrieved May 18, 2021, from <https://fas.org/irp/offdocs/eo/eo-13859.pdf>
- Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 C.F.R. § 99. (1974).
- Fedders, B. (2019). The constant and expanding classroom: Surveillance in K-12 public schools. *North Carolina Law Review*, 97(6), 1673–1726.
- Firth-Butterfield, K. (2017). Artificial Intelligence and the Law: More Questions than Answers? *The Scitech Lawyer*, 14(1), 28–31.
- Fiske, A., Henningsen, P., & Buyx, A. (2019). Your robot therapist will see you now: Ethical implications of embodied artificial intelligence in psychiatry, psychology, and psychotherapy. *J. Med. Internet Res.*, 21(5), e13216.
- Flynn, M. (2018). Police think Alexa may have witnessed a New Hampshire double homicide. Now they want Amazon to turn her over. *The Washington Post*.
- Fohner, K. (2019). Technology altering the classroom. *News Topic*.
- Fourie, L., & Bennett, T. (2019). Super intelligent financial services. *Journal of Payments Strategy & Systems*, 13(2), 151–164.
- Fowler, G.A. (2019). Alexa has been eavesdropping on you this whole time. *Washington Post*.
- Fredericks, K. (2019). Discussion of Technology's Role in the Classroom. *UWIRE*.
- FTC. (2002). *Protecting Children's Privacy Under COPPA: A Survey on Compliance*. Washington, DC: US Federal Trade Commission (FTC).
- FTC. (2012). *Protecting Consumer Privacy in an Era of Rapid Change*.
- Future of Life Institute. (2020). *AI Policy Challenges and Recommendations* (Vol. 2020).
- Future of Life Institute. (n.d.). Asilomar principles. In *Future of Life Institute* (Ed.).
- Gajendar, U. (2019). Humanizing the Experience in the Era of Automation. *Interactions*, pp. 22–24.
- Garcia, J. (2019a). FTC urged by child advocates to investigate Amazon's Alexa. *UWIRE*.
- Garcia, J. (2019b). Lawsuit claims Amazon's Alexa devices record without consent. *UWIRE*.
- Garrison, C., & Hamilton, C. (2019). A Comparative Analysis of the EU GDPR to the USA's data breach notifications. *Information and Communication Technology Law Journal*, pp. 1–16. DOI: 10.1080/13600834.2019.1571473
- Gearing, C.E., Swart, W.W., & Var, T. (1974). Establishing a Measure of Touristic Attractiveness. *Journal of Travel Research*. <https://doi.org/10.1177/004728757401200401>
- Good Housekeeping Institute. (2020). *Good Housekeeping Institute Product Reviews* (Vol. 2020). New York, NY: Hearst Magazine Media, Inc.
- Hale, C. (2019). Microsoft rolls out healthcare-focused chat features and AI assistants. *FierceBiotech*.
- Hansson, O. (2018). *Exploring users' perception of chatbots in a bank environment*. Bachelor's Thesis. Malmo University.
- Haslag, C. (2018). Technology or Privacy: Should you really have to choose only one? *Missouri Law Review*, 83(4), 1027–1052.
- Hawley-Hague, H., Boulton, E., Hall, A., Pfeiffer, K., & Todd, C. (2014). Older adults' perceptions of technologies aimed at falls prevention, detection or monitoring: A systematic review. *International Journal of Medical Information*, 83(6), 416–426.
- Hensel, B.K., Demiris, G., & Courtney, K.L. (2006). Defining obtrusiveness in home telehealth technologies: A concept framework. *Journal of the American Medical Informatics Association*, 13, 428–431.
- Herold, B. (2018, July 17). Classroom digital assistants: Teachers' aides or privacy threats? *Education Week*, 37, 1.

- Herold, B. (2019, February 26). Could Artificial Intelligence Automate Student Note-Taking? *Education Week*, 38, 1.
- Hong, J.I., & Landy, J.A. (2004, June 6–9). An Architecture for Privacy-sensitive Ubiquitous Computing. *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services (MobiSys)*, pp. 177–189. Boston, MA: MobiSys.
- Horn, M.B. (2018). “Hey Alexa, Can You Help Kids Learn More?” *Education Next*, pp. 82–83. Retrieved from educationnext.org
- Hoy, M.B. (2018). Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. *Medical Reference Services Quarterly*, 37, 81–88.
- IEEE. (2020). *IEEE SA - The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems* (Vol. 2020). Institute of Electrical and Electronics Engineers (IEEE).
- Katz v. United States, 389 U.S. 347 (U.S. Supreme Court December 18, 1967). Retrieved May 17, 2021, from <https://supreme.justia.com/cases/federal/us/389/347/>
- Kaye, J., Hong, J., Hiniker, A., Fischer, J. Bentley, F.R. , Tsai, J.Y., . . . Ammari, T. (2018). [Panel Discussion] *Panel: Voice Assistants, UX Design and Research*. CHI. Montreal, QC, Canada: ACM.
- Kirton, J. (2018). A G7 Summit of Significant Success at Charlevoix 2018. *Proceedings of the Charlevoix Canada*. Charlevoix, C: University of Toronto Trinity College Munk School of Global Affairs & Public Policy, G7 Information Centre.
- Knutson, J. (2018). What is COPPA? Learn what teachers need to know about this important law. *THE Journal (Technological Horizons in Education)*, 45(2).
- Lau, J., Zimmerman, B., & Schaub, F. (2018a). Alexa, Are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with Smart Speakers. *ACM Human Computational Interactions*, 2, 1–31.
- Lau, J., Zimmerman, B., & Schaub, F. (2018m, August 12–14). “Alexa, Stop Recording”: Mismatches between Smart Speaker Privacy Controls and User Needs. 14th Symposium on Usable Privacy and Security (SOUPS). Baltimore, MD: SOUPS.
- Luger, E., Urquhart, L., Rodden, T., & Golembewski, M. (2015). *Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process*. CHI. Seoul, Republic of Korea: ACM.
- Luger, E., & Rodden, T. (2013). An Informed View on Consent for UbiCorp. *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*. Zurich Switzerland: ACM.
- Lynskey, D. (2019). ‘Alexa, are you invading my privacy?’ *The Guardian*.
- Mallat, N., Tuunainen, V., & Wittkowski, K. (2017). *Voice activated personal assistants - Consumer use contexts and usage behavior*. Twenty-third Americas Conference on Information Systems. Boston, MA: AMCIS.
- Manheim, K., & Lyric, K. (2019). Artificial Intelligence: Risks to Privacy and Democracy. *Yale Journal of Law & Technology*, 21, 106–188.
- Mannes, J. (2016). Facebook, Amazon, Google, IBM and Microsoft come together to create the Partnership on AI. *Tech Crunch*.
- Marder, H. (2019). Blackboard to Launch New Blackboard Learn Skill for Amazon Alexa. *PR Newswire*.
- McCollum, T. (2017). Audit in an age of intelligent machines: Already in use at many organization, artificial intelligence is poised to transform the way business operates. *Internal Auditor*, 74(6), 24–29.
- McLaughlin, E.C. (2017). *Suspect OKs Amazon to Hand over Echo Recordings in Murder Case*. CNN.
- Melancon, T. (2018). Alexa, Pick an Amendment: A comparison of Fourth and First Amendment protections of ECHO device data. *Southern University Law Review*, 45, 302–310.
- Moltzau, A. (2020). The Global Partnership for Artificial Intelligence. *Medium*.

- Morris, R.R., Kouddous, K., Kshirsagar, R., & Schueller, S.M. (2018). Towards an artificially empathic conversational agent for mental health applications: System design and user perceptions. *Journal of Medical Internet Research*, 20(6), e10148. doi: 10.2196/10148
- Nadarzynski, T., Miles, O., Cowie, A., & Ridge, D. (2019). Acceptability of artificial intelligence (AI)-led chatbot services in healthcare: A mixed-methods study. *Digital Health*.
<https://doi.org/10.1177/2055207619871808>
- National Public Media. (2020). *The Smart Audio Report: Edison Research and NPR*.
- Nazerian, T. (2018). Do Voice Assistant Devices Have a Place in the Classroom? *EdSurge*.
- Nielsen. (2018). *Nielsen Launches new MediaTech Trender survey to uncover consumer sentiment on emerging technologies*.
- Oakley, J. (2018). *Intelligent Cognitive Assistants (ICA) Workshop Summary and Research Needs Collaborative Machines to Enhance Human Capabilities. Intelligent Cognitive Assistants (ICA) Workshop*. IBM Almaden Research Center, San Jose, CA: Semiconductor Research Corporation and NSF.
- OECD. (2013). *The OECD Privacy Framework*. Organisation for Economic Cooperation and Development (OECD).
- OECD. (2019). *Artificial Intelligence in Society*. Paris: OECD.
- Ogan, A. (2019). Reframing Classroom Sensing: Promise and Peril. *IX Interactions*, (XXVI.6), 26.
- Pan, S.B. (2016). Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetrating Gaze. *Harvard Journal of Law & Technology*, 30(1), 239–261.
- Partnership on AI. (2019). *Collaborations Between People and AI Systems (CPAIS) Human - AI Collaboration Framework and Case Studies*.
- Partnership on AI. (2020). *About - The Partnership on AI Our Goals* (Vol. 2020).
- Penn State University. (2017). *Beaver Professor Debuts Voice-Enabled Classroom Assistant*. Penn State News Service.
- Pew Research Center. (2017). *Nearly half of Americans use digital voice assistants, mostly on their smartphones*.
- Pfannenstiel, K. (2019). Is Alexa the newest teaching assistant? *UWIRE*.
- Pfeifle, A. (2018). Alexa, what should we do about privacy? Protecting Privacy for Users of Voice Activated Devices. *Washington Law Review*, 93(1), 421.
- Pierce, D. (2017). One for All. *Wired*.
- Pierce, D., & Hathaway, A. (2018). The promise (and pitfalls) of AI for Education: Artificial intelligence could have a profound impact on learning, but it also raises key questions. *T H E Journal (Technological Horizons in Education)*, 45(3).
- Privacy Coalition. (2020). *Privacy Pledge - The Privacy Coalition* (Vol. 2020).
- Rabkin Peachman, R. (2017). Mattel pulls Aristotle children's device after privacy concerns. *New York Times*.
- Rakheja, J. (2018). AI Has the potential to fundamentally change the framework of industries. *PC Quest*.
- Rauthmann, J.F. (2017). Situational Factors. In V.S. Zeigler-Hill & K. Todd (Eds.), *Encyclopedia of Personality and Individual Differences*. SpringerLink.
- Romano, B. (2019). Suits allege Amazon's Alexa violates laws by recording children's voices without consent. *Seattle Times*.
- Rowh, M. (2019). Your voice is my command. *University Business*, pp. 31–33.
- Rozenshtein, A.Z. (2018). Surveillance Intermediaries. *Stanford Law Review*, 70, 99–189.
- Sabharwal, C.L., & Anjum, B. (2018). Robo-Revolution in the Financial Sector, Social Network Analysis, Social Media, & Mining. *International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1279–1283. Las Vegas, NV: IEEE Explorer CSCI.
- Saint Louis University. (2018). *Saint Louis University Installing Amazon Alexa-Enabled Device in Every Student Living Space on Campus*. Saint Louis University News.
- Savva, A. (2020). Scientists develop Amazon Alexa blocker to stop it listening to conversations. *Daily Star*.

- Schwartz, E.H. (2020). *Coronavirus Lockdown is Upping Voice Assistant Interaction in the UK*. Voicebot.ai.
- Sciuto, A., Saini, A., Forlizzi, J., & Hong, J.I. (2018). "Hey Alexa, What's Up?": Studies of In-Home Conversational Agent Usage. *Proceedings of the 2018 Designing Interactive Systems Conference (DIS '18)*, pp. 857–868. Hong Kong: ACM. <https://doi.org/10.1145/3196709.3196772>
- Shaban, H. (2018a). Amazon Alexa user receives 1,700 audio recordings of a stranger through 'human error'. *Washington Post*.
- Shaban, H. (2018b). An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says. *Washington Post*.
- Shaban, H. (2018c). Two senators want Amazon's Jeff Bezos to answer to Alexa's eavesdropping. *Washington Post*.
- Shackleton, J.R. (2019). Comment: Alexa, Amazon Assistant or Government Informant? *University of Miami Law Review*, 27, 301–327.
- Silverman v. United States, 365 U.S. 505 (U.S. Supreme Court March 6, 1961). Retrieved May 17, 2021, from <https://supreme.justia.com/cases/federal/us/365/505/>
- Simpson, J. (2017). Amazon Echo in Education? *EduGeek*.
- Singer, N. (2019). Critics Assail Amazon Over Children's Privacy. *The New York Times*.
- Skiba, D.J. (2016). On the horizon: Trends, challenges, and educational technologies in higher education. *Nursing Education Perspectives*, 37(3), 183–185.
- Smith v. Maryland, 442 U.S. 735 (U.S. Supreme Court June 20, 1979). Retrieved May 17, 2021, from <https://supreme.justia.com/cases/federal/us/442/735/>
- Smith, P. (2017). Will Alexa Take the Witness Stand? *New York Times Upfront*, 150.
- Soper, T. (2020). Amazon Alexa leader: COVID-19 has sparked 'a huge increase in the use of voice in the home'. *Geekwire*.
- Springer, P. (1999). Get Over It. *Wired*.
- SRC. (2016). *Intelligent Cognitive Assistants (ICA) Workshop and Recommendations*. Intelligent Cognitive Assistants (ICA) Workshop. Semiconductor Research Corporation and NSF.
- Sterling, B. (2018). The Asilomar AI Principles. *Wired*.
- Stokes, G. (2020). Autonomy. *Korean Business Maeil Economic Daily*.
- Stoneman, A. (2018). *ASU and Amazon inspire new student ventures with Alexa*. ASU Now: Access, Excellence, Impact.
- Tate, E. (2019). Alexa goes to ISTE: Edtech Companies - and Teachers - Debut New Skills for Learning. *EdSurge*.
- TechCrunch. (2018). Amazon expands its Alexa Fund Fellowship to a total of 18 universities, up from 4 last year. *Tech Crunch*.
- The Advocates for Human Rights. (n.d.). *Human Rights Basics* (Vol. 2020). Minneapolis, MN: The Advocates for Human Rights.
- Thomas, L. (2018). Hey, Alexa, stop listening to everything I say. *UWIRE*.
- Thompson, C. (2018). May A.I. help you? *The New York Times Magazine*, 46.
- U.S. CONST. amend. IV. (1791).
- United Nations, General Assembly. (2008b). *Mandate of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises: Report of the Human Rights Council, HRC/Resolution 8/7*.
- United Nations. (1948). THE INTERNATIONAL BILL OF HUMAN RIGHTS. In U. Nations (Ed.), *General Assembly resolution 217 A (III)*. Geneva: United Nations.
- United Nations. (1989). Convention on the Rights of the Child. In G. Assembly (Ed.), *1577 U.N.T.S. 3.*, (Vol. 20).
- United Nations. (2008a). *Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*. United Nations General Assembly Human Rights Council.

- United States v. Jones, 565 U.S. 400 (U.S. Supreme Court January 23, 2012). Retrieved May 18, 2021, from <https://supreme.justia.com/cases/federal/us/565/400/>
- United States v. Miller, 425 U.S. 435 (U.S. Supreme Court April 21, 1976). Retrieved May 17, 2021, from <https://supreme.justia.com/cases/federal/us/425/435/>
- Vaidyam, A., & Torous, J. (2019). Chatbots: What are they and why care? *Psychiatric Times*, 36(6), 21.
- Vajradhar, V. (2020). Rise of AI-Powered Chatbots in the Banking Industry. *Medium*.
- Villasenor, J. (2013). What you need to know about the Third-Party Doctrine. *The Atlantic*.
- Wakefield, J. (2016). Microsoft chatbot is taught to swear on Twitter. *BBC News*.
- Wall, L.D. (2018). Some financial regulatory implications of artificial intelligence. *Journal of Economics and Business*, 100, 55–63.
- Wueest, C. (2017). Everything You Need to Know About the Security of Voice-Activated Smart Speakers. *Symantec*.
- Yousufani, M., Courbe, J., & Babczenko, K. (2020). How retail banks can keep the lights on during the COVID-19 crisis — and recalibrate for the future. *PWC*.
- Zeide, E. (2016). Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS. *Drexel Law Review*, 8, 339–394.
- Zwijnsen, S.A., Niemeijer, A.R., & Hertogh, C. (2010). Ethics of using assistive technology in the care for community-dwelling elderly people: An overview of the literature. *Aging & Mental Health*, 15(4), 419–427.