Abstract

Smart home technologies on our phones and in our homes are collecting more (quantity) and more (types of) data about us. These tools are intended to simplify everyday tasks, but to do so effectively, they collect significant data about users and their environment. One popular example includes intelligent personal assistants (IPAs) like Apple's Siri, Amazon's Alexa, and Google's Assistant. As these services have transitioned from being embedded in consumers' smartphones to standalone devices in the home, they have evolved to collect and share more data in more potentially invasive ways. In this paper, we consider American adults' attitudes toward IPAs. Through an analysis of focus groups with IPA users and non-users, we describe attitudes and concerns toward IPAs broadly, as well as how these attitudes vary based on the devices' features. We suggest new frameworks for evaluating privacy-based decisions and offer policy suggestions for regulating data flows from smart technologies.

Keywords: privacy, internet of things, intelligent personal assistants, information and communication technologies, smartphones

Feature Creep or Just Plain Creepy?

How Advances in “Smart” Technologies Affect Attitudes Toward Data Privacy

Recent years have seen an explosion in the Internet of Things (IoT) and “smart” technologies designed to simplify our lives. IoT refers to a network of interconnected computing components, digital and mechanical objects, and living organisms; each “thing” is given a unique identifier enabling the data transfer over the network (AlHammadi, 2019). IoT devices share data with the cloud and allow remote access, such as turning lights on/off, monitoring contents in your refrigerator, or adjusting your home’s temperature. These smart technologies are found everywhere—from workplaces to homes and cars—and include smart light switches, appliances, thermostats, digital assistants, door locks, and more. Gartner (2017) estimates that in 2020, there will be more than 20 billion IoT devices operating worldwide, up from 8 billion in 2017.

IoT devices collect a lot of data about the environment around them to function, as well as to learn and improve their functionality. And while IoT devices provide significant utility, they also raise concerns about what data is being collected, how that data is stored, what control users have over managing that data, and how that data might be used in the future. A prime example of the potential risks of IoT devices occurred in October 2016, when hackers harnessed hundreds of thousands of IoT devices to bring down Dyn—a large domain name service (DNS)—through a distributed denial-of-service (DDoS) attack that took Twitter, Netflix, Reddit, CNN, and many more sites offline for several hours (Woolf, 2016). When considering privacy risks to users, these devices contain a variety of sensors to collect audio, location, movement, and other trace data; users risk revealing important information about their likes and dislikes, eating and exercise habits, location data, and more (Boeckl et al., 2018).

In this paper, we focus on one of the most popular IoT interfaces—intelligent personal assistants (IPAs) found in smartphones and smart speakers. The evolution of these devices involves new features that collect a wider range of data (from voice to video) through more channels that reduce the friction between users and devices (from push-to-activate features on the phone to always-listening home devices).

Using data collected from 11 focus groups (65 people) of IPA users and non-users in two metropolitan regions in the U.S., we evaluate how both those who regularly use these devices, as well as those who have chosen to not use them, feel about this evolution, as well as the wider implications of the growth of IoT technology. We interpret our findings through existing privacy frameworks that give insights into the complex ways people negotiate or become resigned to data collection. We also discuss next steps for developing a research agenda to educate and empower end-users to manage their data, and to guide future regulations and policy that protect consumers.

Background

IoT, IPAs, and the Evolving Smart Home Ecosystem

One of the most common applications of IoT is in home automation via mobile apps or standalone devices. According to Zeng and colleagues (2017), standalone smart home devices include thermostats, lights, motion detectors, door/window sensors, air quality sensors, power outlets, and door locks. Many of these technologies are managed through a mobile interface, while people can also use voice commands to control smart speaker “hubs” for a variety of smart devices.

In recent years, these smart speakers—and the IPAs that power them and enable hands-free interactions—have gained in popularity, with a recent survey finding that more than one-quarter of Americans (26.2%) has access to a smart speaker (Voicebot, 2019), up from 8% two years earlier (Pew Research Center, 2017). People use IPAs most frequently to access music, conduct hands-free searches, and control other smart devices that had been connected to the smart speaker (Ammari et al., 2019). IPAs can also be customized to make routines more efficient, such as creating voice-activated routines to lower lights and play soothing music at bedtime.

The ecosystem of IoT technologies promises convenience, safety, and enhanced lifestyles, especially for those with special needs (Pradhan, 2018). For instance, in a smart home system Nath et al. (2018) created for elderly people and their caregivers, Alexa was used to detect and monitor location, analyze and send diagnoses to the caregiver, keep track of the older adults' daily activities and well-being, and detect any abnormalities in their behavior. Beyond those with disabilities, smart homes provide convenience and remote access to one's physical environment and may help reduce energy bills and provide added layers and security to one's home (Wilson, Hargreaves, & Hauxwell-Baldwin, 2015).

Privacy Concerns Regarding IoT and Smart Home Devices

Although useful in many scenarios, IoT devices blur the boundary between public and private spaces, and researchers have begun examining the privacy implications of integrating "always listening" IPAs in home environments. Using survey data from 1160 users and non-users, Liao et al. (2019) found that IPA users reported lower levels of general privacy concerns than non-users, while also reporting higher confidence that companies (Amazon and Google) would ensure the privacy, safety, and security of their data. Through interviews and diary studies with IPA users and non-users, Lau et al. (2018a) found that non-users saw little utility in smart speakers and were less trusting of IPA companies. In contrast, users expressed few privacy concerns, but their rationalizations indicated an incomplete understanding of privacy risks, a complicated trust relationship with speaker companies, and a reliance on the socio-technical context in which smart speakers reside. Studies have also found that privacy controls are rarely used, as they are not well-aligned with users' needs (Lau et al., 2018a; Malkin et al., 2019).

As highlighted by Lau et al. (2018a) and found in studies of other IoT devices (e.g., Vitak et al., 2018; Zeng et al., 2017), IPA users often have limited understanding of how their data is collected, stored, and analyzed through IPAs. People were surprised to learn early in 2019 that Amazon Alexa employees were analyzing IPA audio files to improve the technology and had access to users' sensitive data like their home address (Day, Turner, & Drozdiak, 2019). Other examples of inappropriate data flows, such as a private conversation captured by an Echo and emailed one of the speaker's contacts (Fowler, 2018), have highlighted some of the ways data sharing can go wrong. Ammari et al. (2019) found that most respondents could not articulate specific privacy concerns; when they did, concerns centered on uncertainty about when the device was "listening" and concerns about third parties accessing IPA data. Zeng et al. (2017) found that respondents rationalized this lack of concerns as not feeling personally targeted, trusting potentially adversarial actors (like companies or governments), and believing their existing mitigation strategies to be sufficient.

Taken together, these studies illustrate how privacy concerns can influence the adoption of smart home devices and IPAs. Specifically, non-users might be more sensitive to privacy issues, while users might value the convenience over privacy (e.g., Zheng, Apthorpe, Chetty, & Feamster, 2018), or trust in the company might mitigate any lingering privacy concerns.

Existing Frameworks Related to Privacy

Numerous approaches have been used to examine attitudes and behaviors related to privacy and data sharing. In this section, we highlight those most frequently used to understand consumers' behaviors and attitudes related to using technologies that collect personal data.

Privacy calculus (Culnan 1993; Laufer & Wolfe, 1977) describes a cost-benefit analysis in the individual decision processes before the disclosure of personal information necessary to complete a transaction. Culnan and Bies (2003) argue that people are more likely to accept the loss of privacy that accompanies any disclosure of personal information when risk outweighs the benefits. In the case of IoT users, privacy calculus argues that consumers engage in a rational analysis of the privacy risks and benefits of using a given technology; if the benefits outweigh the risks, they are more likely to adopt that technology.

Privacy calculus is closely connected to another popular framework for considering people's disclosure behaviors, the "privacy paradox" (e.g., Ackerman et al.,1999; Barnes, 2006), in which consumers want to have control of their information but continue to behave in a way that contradicts their preference; they avoid the hassle of actually exploiting the control, which leads to a predominance of over-sharing. For instance, Gross and Acquisti (2005) found that only a small percentage of Facebook users changed the default privacy settings that maximize the visibility of their profile. More recently, Williams, Nurse, and Creese (2018) argued that IoT may further exacerbate the privacy paradox due to the diversity of device features and security protocols, as well as a false belief that end-users have the knowledge and skills to properly connect these devices and take appropriate measures to minimize risks.

Finally, the theory of privacy as "contextual integrity" (Nissenbaum, 2011) provides a useful framework for understanding why certain information flows are acceptable in one context but problematic in another. Contextual integrity begins with the understanding that interactions occur in particular contexts, and that norms govern people's expectations of how personal information should flow within any given context. If a new technology or practice disrupts those norms, it could pose a privacy concern, irrespective of whether the information was public or private. For example, the introduction of a smart appliance that records and shares household data to an internet provider might represent a disruption of existing informational norms. Shklovski and colleagues (2014) applied contextual integrity in an analysis of mobile app data sharing practices, arguing that technology companies should consider data collection practices to be more aligned with users' expectations around information flows.

In this paper, we consider the role these frameworks may play in evaluating the privacy risks posed by IPAs, the role these risks play in (non-)adoption, and how the evolution of features in IPA-embedded devices like smartphones and smart speakers affects people's perceptions of privacy risks. Specifically, we ask the following research questions:

RQ1: How do IPA users and non-users navigate privacy concerns they have related to these devices?

RQ2: How do users' and non-users' attitudes toward IPAs shift as the technology evolves and offers new features to provide greater integration into their daily lives?

Method

This research study was conducted at two universities in the U.S. In January 2018, the authors obtained a random sample of 3000 university staff at each university and invited those employees to complete an online survey about phone and home IPA use. At the end of the survey, participants were invited to enter their email address if they were interested in participating in a follow-up focus group session to discuss their attitudes toward IPAs. We received responses from 1160 people, and 705 expressed interest in the focus groups. We divided this subset of participants into groups based on whether they used home-based IPAs, phone-based IPAs, both, or neither. We then began inviting potential participants to complete a Google

Form to indicate times they would be able to participate in an in-person focus group on campus, with the goal of creating three types of sessions: (1) all users, (2) all non-users, and (3) a mix of users and non-users.

We continued recruiting until we reached saturation; in total, we conducted 11 focus groups with 65 people across the two institutions, with group sizes ranging from 2-8 people. Across the 11 sessions, four were comprised solely of IPA users, two were comprised solely of non-users, and five included a mix of users and non-users. See Table 1 for details on each session.

--TABLE 1 ABOUT HERE--

All sessions ran for 60 minutes. The moderator began with an ice breaker activity so participants could introduce themselves, then moved onto questions about their general attitudes toward and use of new technologies before providing prompts to encourage discussion about their (non)use of IPAs on their phones and in their homes For example, after talking about attitudes toward technology broadly, the moderator prompted: "I want to shift our conversation to focus on the two main types of IPAs. First, let's talk about the ones that are available on your phones. For those of you who use Siri, Cortana, or Google Assistant, I'd like to hear how and why you're using the device. For those who don't, are there reasons why not?"

Near the end of the focus group, the moderator showed the group one of two commercials[1] for the newly released Echo Show from Amazon, which includes a screen, camera, and additional integrations with other smart devices, and asked participants to discuss their reactions to the device. We chose to focus on the Echo Show because it highlighted broader themes of IoT technologies, including the creation of ecosystems of devices and accounts, as

[1] Depending on how much time was left in the session, the moderator either showed a 1-minute or 4.5-minute version of the commercial. Both commercials were created by Amazon.

well and advanced integration of audio and visual features. In some sessions, participants also discussed the Echo Look, a recently released device that included a camera and was marketed as a tool to upload pictures of outfits and get fashion advice from peers. At the conclusion of each session, participants received a US$15 Amazon gift card.

Each focus group session was audio recorded. In addition, at least two researchers attended nearly every session, and those not moderating took detailed notes. Audio files were transcribed and imported into Dedoose for analysis. The research team first developed a codebook based on the interview protocol and researcher notes from the sessions. Therefore, initial codes reflected both explicit questions (e.g., benefits and drawbacks of IPAs) as well as high-level patterns observed in comments across sessions (e.g., comments that reflected a "nothing to hide argument" or "privacy apathy").

Each team member coded a transcript separately, then met to refine and finalize the codebook. During this process, new codes were added and others were collapsed. Next, each transcript went through two rounds of coding using textual microanalysis (Strauss & Corbin, 1998), which involves line-by-line coding to identify emergent themes in the corpus. In cases where a team member was unclear on what code should be applied, they applied the "Unsure" code; these codes were discussed and resolved by the full team.

Excerpts from each code were then exported from Dedoose into Excel to allow for additional analysis (Miles, Huberman, & Saldaña, 2013). Team members reviewed all excerpts for a given code and organized the excerpts into themes (which are presented in the findings), then summarized the emergent narrative from those codes. See Table 2 for a description of codes included in the analysis.

--TABLE 2 ABOUT HERE--

In the findings, we present a selection of quotes that highlight the emergent themes from our analyses. When we reference individual participants, we use a pseudonym to protect their identity.

Findings

Before exploring our two research questions, we want to provide a brief description of our focus group participants. Across the 11 focus groups, 43 people used either a phone IPA, home IPA, or both (phone: 41; Amazon Echo: 22; Google Home: 11). In the survey, we asked two sets of items capturing general privacy concerns (Vitak, 2016) and mobile data concerns (Xu, Gupta, Rosson, & Carroll, 2012).[2] Across the 65 focus group participants, their general privacy concerns were slightly above the midpoint (Somewhat Concerned), *M*=3.13, *SD*=.86, and their mobile data concerns were even higher, *M*=3.97, *SD*=.74; no differences existed between non-users' and users' concerns. We also developed a scale from seven original that evaluated various concerns about IPA devices (Authors, 2019).[3] We found that non-users had significantly higher concerns about IPA devices (*M*=3.32, *SD*=1.22), compared to IPA users (*M*=2.75, *SD*=1.00), *t*(64)=2.00, *p*<.05.

RQ1: Rationalizing privacy concerns in IPA (non-)adoption

Across the focus groups, we found notable differences between the ways IPA users and non-users talked about privacy concerns associated with the technology. Common tropes around data privacy—specifically "nothing to hide" and "privacy is dead" arguments—abounded in participants' discussions as they rationalized the use of IPAs and other smart technologies. Non-users often described their privacy concerns as one of the reasons they avoided using IPAs. We explore these themes in more detail below.

[2] Both scales were measured on a 5-point scale with a higher number indicating elevated concerns.
[3] The scale was measured on a 5-point scale with a higher number indicating elevated concerns.

Few privacy concerns because "I have nothing to hide." When presented with ongoing debates about government surveillance and the tensions between individual privacy and national security, many Americans are likely to respond that data collection is acceptable because they have nothing to hide. Pew Internet research finds that Americans think it's acceptable for the government to monitor non-citizens (Madden & Rainie, 2015), although there is significantly less acceptance of monitoring U.S. citizens. Corporate surveillance and data collection, however, are commonly tied to benefits like facilitating online shopping (Dinev & Hart, 2006). While this fits within the framing of privacy calculus, it also assumes consumers have full information and can make informed decisions. Below, we examine how participants rationalized this stance when talking about IPA use.

Aspects of this trope were reflected in several participants' comments as they discussed their use of IPAs. A common variant on this argument is that "good" people shouldn't have anything to hide, which was reflected in John's comment dismissing privacy concerns about IPAs: "If you're gonna be that concerned about a device listening in, chances are you're probably doing something that you really don't want people overhearing." Others described their lives as "uninteresting" and unworthy of government focus, as when Jackie said, "I live a very boring and average life. I would probably never be tagged by the FBI or anything like that because I don't do anything." Still, others distinguished between the types of things they'd say in front of an IPA and things they might say in more private spaces and described IPA interactions as non-sensitive. For example, James said, "There's nothing that I would share that Alexa would hear that would embarrass me at any point in time."

Another pattern in these responses was that the kind of data being shared through IPAs was less worrisome than other potential threats to privacy or security, or compared to having their IPA connected to more sensitive accounts or devices. For example, Anthony said,

> I live a fairly simple life. I don't work in an industry where I'm protecting trade secrets... To me the bigger security concern is if I use Alexa to purchase something, is that machine any more vulnerable when I put my credit card into a dozen different websites? That level of security is what I'd be most worried about.

Likewise, Emma said she doesn't worry about potential security risks from these devices because she is not doing anything to warrant attention: "I'm boring. I don't have my ballistic missiles sitting in my living room. If somebody wants into my house, they're getting into my house whether I have it guarded through my Google or whether I have it guarded with a key."

Privacy is dead, so I might as well benefit. In rationalizing the use of IPAs and related technologies, many of our respondents noted that they are already tracked through a variety of channels, and the advances of the last decade make them think it's impossible to have true privacy anymore. For example, Charlotte said, "I think there are video cameras on every street. I mean, they are watching us everywhere, they are listening to our every peep and move… I guess I don't know how to prevent that or what to think about it. It just doesn't seem like there is a lot of privacy anymore."

This belief that American citizens are under constant surveillance has become more commonplace since Edward Snowden's revelations about domestic (U.S.) surveillance programs created after the September 11 attacks (Greenwald, 2014). For example, in 2015, Pew Internet reported that Americans have little confidence that the data they share with companies online will remain private over time, and just 9% of Americans feel they have "a lot" of control over the kinds and amount of data collected about them (Madden & Rainie, 2015). These findings are reflected in Brian's comment**:** "I think at the end of the day, no matter what technology you use, I feel like if they want to find something, they can find out...your phone is tracked wherever you go, so they can tell you your whole life story if they wanted to."

Participants also shared specific examples of events that highlight their lack of privacy. Kyle noted that regular data breaches at major corporations means our data is already "out there," while Anne spoke about how she will search for something on Google only to see ads for that product on other sites. Relatedly, Marilyn shared an anecdote about why she thinks Siri is always listening to her conversations: "I was driving with my husband and we were having a conversation about a t-shirt he had seen…The next day on my Facebook, there was an ad for that t-shirt." This assumption that smart technologies—including IPAs—were always listening and collecting data from their surroundings was held by both users and non-users.

The belief that data collection and surveillance was omnipresent led to a sense of apathy and resignation toward data collection among many of the people we spoke with. For example, Jackie said, "I think it's useless to fight. I mean, as much as I agree with most of the cautionary opinions [about how to protect your data], I think in some ways it doesn't matter because the next generation is going to be even more used to technology... People are just going to accept this information." Veronica echoed this sentiment, saying, "I don't think there's running away from technology that we can do efficiently in this age, and I don't mind."

Veronica's comment that she "doesn't mind" technological advances was reflected in several comments in line with the tradeoffs highlighted in the privacy calculus framework. For example, Adam said, "I feel like a lot of these companies are collecting these data anyways. I don't like that they do, but if they're going to collect it, I'd rather get the most utility out of it as possible." In that same session, Jay added, "I realized if I'm gonna have a modern smartphone, I'm always gonna have that technology and I can't guarantee it's turned off, so I might as well use it. I mean, it's built in—there's no escaping it."

Privacy concerns keep me from fully adopting new technologies. While many IPA users we spoke to shared feelings of resignation toward data collection, those who had not adopted IPAs expressed a range of concerns when talking about their decision not to use them. Common responses centered on privacy concerns, trust, and having too many unknowns with these devices.

Non-users often referenced their current use of other Google or Amazon services and the data they already shared with these companies. Unlike IPA users, who may have rationalized their IPA use by saying the company already had their data, non-users talked about wanting to minimize the data these tech giants had about them. Jada said, "I have a Google phone and Google accounts. I feel like Google, at this point, knows everything about my life. But I still have a little bit of worry about setting myself up to use a device that would know more information about me." Another factor that may have influenced this desire to minimize data sharing was trust, which was reflected in Gwen's comment:

> I think there's a bit of a trust factor for me. I don't really trust the corporations, so I'm only willing to let them into parts of my life where I'm like, "Okay, this is really useful." And I also think as we get more smart devices around our home, it's just easier for them to be hacked and I think that that's going to happen more and more. And so if I don't have an overriding need for it, I probably just won't do it.

Likewise, Leah raised concerns about trading personal information for minimal benefits, like using IPAs to play music. "It's one more thing that is used to collect data on you; I assume it's one more thing that can be hacked. I'm old fashioned. I'm happy with the radio and CDs. I can take those extra four steps to the radio or CD player and turn it on."

At the time of data collection, several media reports had identified bugs with the Echo devices, including a heavily-covered story of Alexa laughing without being prompted (see Chokshi, 2018, for details). Many non-users we spoke to mentioned news stories when discussing their reasons for not using IPAs. For example, Cliff said:

> When the review units of the...Google Home Mini went out, the button was constantly pushed to listen by just manufacturing defect. So here's a device that's constantly listening and they get updates continuously from the server. Let's say somebody wanted to change it, how hard would that be to get it to change?

Walter said he stopped using Google Assistant after hearing concerning news stories "of people just mentioning certain words and suddenly, boom, the phone's responding." He also worried about weak security protocols in IoT devices making everything more vulnerable, saying, "I don't want to have the ability to turn on and off a light and someone can come in and steal what's on my hard drive."

Other participants worried about unknowns associated with these devices, including how their data could be used in the future and security risks posed by wider IoT ecosystem. Wade pointed to the newness of these kinds of technologies and the lack of existing legislation to protect consumers: "Probably the biggest drawback for me in terms of not wanting to get one is there's a lot of unknowns, it's all pretty new. Until there's legal precedent, or more history behind it, I don't really want to jump into it." Nina felt the lack of clarity in data collection processes was unnerving, saying, "I don't want a corporation listening to what's going on in my household. I don't know what it's recording. I don't know what's being done with that information. So, it freaks me out." Finally, Leah raised concerns about how data from these devices could be evaluated out of context: "Do you have to worry about being at home with your family and raising your voice to someone and have that come back to haunt you months down the road. 'Oh, we heard you screaming at your children. We're going to arrest you for child abuse.'"

RQ2: Shifts in Privacy Attitudes Across Types of IPA Devices

For our second research question, we considered how IPAs' features have evolved in recent years. Initially only available on smartphones, this technology has expanded to a variety of home devices, including recent versions with cameras and screens. Features in newer versions of smart speakers aim to reduce friction between the user and the task they want to accomplish, which requires the device to have greater access to user data. Throughout our focus groups, participants discussed their (dis-)comfort with these features, and across both users and non-users, participants described newer forms of IPA technology (and "smart technologies" more broadly) as increasingly "creepy," which echoes previous research looking at user perceptions of data collection by mobile apps (Shklovski et al., 2014).

As devices move from phone to home, they raise more concerns about privacy invasion. During each focus group, we began our discussion of IPAs by talking about the phone-based versions, including Apple's Siri, Google's Assistant, and Microsoft's Cortana. Most participants reported using phone-based IPAs at some point, although they described the limited utility of these devices due to technical issues. For example, participants described having a hard time accomplishing tasks with them, like when Jordan said he didn't use Siri much because "she didn't really accomplish [requests I gave her] well." Jordan used both the Amazon Echo and Google Home and was much more favorable toward the home-based IPAs.

Some participants spoke about specific IPA features when describing why they had some concerns. For example, Jin said, "I don't feel like Siri is listening [all the time], because she doesn't turn on unless I press my home button and say 'Hi, Siri.'" Erika echoed this, saying, "I don't have an Alexa or Google Home. But I have Google [Assistant] on my phone...and I really like that I have to trigger it." Renee suggested that explicit triggering features were what kept them from entering "creepy" territory: "If you have to trigger it, it's not creepy. If it's listening to you whispering and you haven't done anything... Like, I don't mind saying 'Okay, Google' or whatever. No problem. But if it's still listening and I don't want it to be listening anymore, that's creepy." Importantly, different IPAs have different activation features, but one of the benefits of home devices is they are typically activated by voice alone ("Hey Alexa," "Hey Google"), whereas the original version of Siri and Google Assistant required users to hold down a button to activate the service. Home IPAs may have a "mute" button that requires a user to unmute the device before using, but this significantly reduces the utility of the device, and prior research suggests the feature is not widely used (Lau, Zimmerman, & Schaub, 2018b).

Many participants expressed concern that their devices were always listening—not just when they spoke the activation phase—because of personal experiences they had with the devices. For example, Marilyn said, "She's definitely always listening because randomly she thinks she hears 'Alexa' but we never said that and she will start talking. In that aspect it's clear that they are always listening and who knows if they are saving [it]." Relatedly, some users expressed concerns that anyone could trigger the device, like when Faith talked about a movie setting off her Echo: "It's kind of creepy because we'd be watching in the living room and you know, the dad would shout the daughter's name [Alexis] and all of a sudden you would hear, 'I'm sorry, I didn't quite catch that.'" These risks require a degree of trust between users and the companies providing these devices. But this also raises questions of whether the companies should be trusted. This sentiment was highlighted by Huong, who said, "We're trusting Google that what they show me…is what they kept. For the most part I trust Google on that, and Amazon. But there's that open concern, it's like, what are you opening yourself up to?"

Building on Huong's comment, participants also expressed concerns about not knowing exactly *when* these devices were listening and *how much* content they captured. For example, Jackie said:

> ...it's always listening for you to say 'Alexa.' Do I really know it's not listening to other things? What if it's listening to a conversation about my religious or political beliefs and it's tagging things? I don't want to sound paranoid, but I really don't trust corporations and I don't trust the government to not do those things just because they say it's wrong.

Because of these concerns, several participants said they refused to put home-based IPAs in especially private places like their bedrooms. James said he won't even put a TV in his room because of privacy concerns. Likewise, Chen described why she removed her Echo device from her bedroom: "I'm really concerned about privacy... I remember at first when I put it in my bedroom, and we talked about my son whose name is Max. I don't know what the similarity was, maybe Alexa and Max. And it starts to work and joined the conversation. So it made me mad."

Cameras and screens and drop-ins, oh my! Newest IPAs seen as creepy and invasive. In all focus group sessions, participants viewed an Amazon-produced Echo Show commercial and then discussed it. In several sessions, a related product (the Echo Look) was also discussed because it shared the camera feature with the Show. While some participants pointed to benefits of these more advanced IPAs (e.g., Huong described the convenience of having a screen so she can see how much time is left after setting a timer), the word "creepy" emerged repeatedly, without prompting, by users and non-users in nearly all focus groups. Below we explore how participants talked about their concerns regarding the most evolved IPA devices.

The main feature that provoked strong responses from participants after watching an Echo Show commercial was the "Drop-In" feature, which Amazon describes as "two-way intercom." For this feature to work, users create a list of approved contacts they can connect with. Once the contact approves this privilege, they can instantly connect via audio (on the original Echo and Echo Dot devices) or video (on the Echo Show). One participant, Sun-Joo, shared her experiences trying out Drop-In on her Echo Dot, and she spoke of tensions between feeling connected to her family and being *too* connected: "I don't need them to call me at every minute of the day. If it tells them I'm active, they know I'm at home, so if I don't answer, I get a text message, 'Hey, where are you? I just tried to call you.' ...I'm trying to find the balance between that." Otherwise, no other participants had direct experience with the feature.

Immediate reactions after watching the commercial reflected a sense of wariness toward features like Drop-In that seemed creepy and invasive. For example, Liz said, "I'm the kind of person that has a piece of tape over my computer camera just 'cause I don't trust that either. So the Drop-In thing, that's creepy." Likewise, Walter described the stress of having to be more aware of what you do in private spaces. Speaking about the Echo Look—described as a "Hands-Free Camera and Style Assistant with Alexa"—he asked, "What happens when you come out of the shower and it takes a picture of your body and tells you you need to diet, you need to exercise more?"

Multiple participants expressed concerns about versions of the Echo equipped with cameras, especially since the Look is framed for use in the bedroom (to let you take pictures of yourself and get feedback on your outfit), although female participants expressed greater concerns than male participants about the potential for nude photos being captured. Talking about the Echo Show, Olivia said,

> I also feel a little uncomfortable with the idea of a camera that could always be on because they always say cover your laptop camera. ...But if you had something that had a camera that was looking into your bedroom or an intimate space, I feel like that's really

> creepy. If somebody were to hack that or hack a Drop-In and just like, actively watch you... I don’t like that.

While the initial reaction to the Echo Show was frequently speaking to its general “creepiness,” participants’ comments also reflected a sense of weariness toward more invasive technologies that required them to think about more things that could go wrong (e.g., camera positioning, being careful about what you say near the device). For example, Huong said, “I don’t have a problem with pointing cameras outside, but I’m not too comfortable with all the cameras inside always on.” This was echoed by Jada in a separate session, when she said:

> I’m guessing the device is always gonna be on or else it’s not very convenient to have it there, which means that anyone could make a request to do a video call. Maybe your hair’s not done, maybe you just woke up, maybe you were taking a nap or enjoying your peace and quiet or solitude, then all of a sudden there’s a Drop-In call.... So, just that worry that unless I say the right word, it’s going to pick up and someone’s going to be able to see what’s going on behind me.

Moving beyond IPAs to consider the wider ecosystem of smart devices in homes, as well as improvements in machine learning that enable devices to make better predictions—these themes of wariness and weariness were exacerbated further. Marilyn shared how she and her husband still haven’t bought a smart lock: “The only concern I have [with] smart locks, if you hook it up, a hacker could get into your Alexa and unlock your home that way.” Participants shared their discomfort with how widespread data sharing was between companies, which was particularly visible when they saw customized advertising and considered how those inferences were made. Olivia talked about “canceling all her social media” after seeing how data from various sources were shared to generate tailored ads; while others hadn’t taken direct action, they said seeing ads based on prior searches or conversations was disconcerting.

When thinking about how technology is continually getting smarter and able to learn from individual users’ patterns of behavior, some participants expressed significant concerns.

Rebecca raised the following question: “I like the idea [of devices learning and customizing responses], but where do we draw the line? To the point where we’re 100% dependent upon devices doing certain things for us?” Zack also pushed back against extreme customization, sharing how he tries to sabotage the underlying algorithm in his IPA: “I’ve been trying to feed it specific information and it fails in so many ways to get any type of personalized response.”

Discussion

In this study, we shared findings from focus groups with IPA users and non-users to explore the role that privacy considerations play in use of these technologies, as well as how privacy concerns are evolving as smart technologies add new features, collect more data, and become better equipped to make inferences and recommendations to users. IPAs provide an important case study in thinking about the privacy risks of IoT ecosystems because of their popularity, where they are used (private spaces), the types of data they collect (audio/video), and their function as a hub for a range of smart home devices.

Privacy calculus (Culnan 1993; Laufer and Wolfe 1977) is a commonly applied framework that posits consumers engage in a cost-benefit analysis to make decisions about whether to share personal information. For example, when deciding whether to make a purchase from an online site, a person may compare potential risks (e.g., Will the transaction be encrypted? Is the site trustworthy?) with potential benefits (e.g., scarcity of desired product, speed of delivery). Applying this framework to IoT—where more data sharing is often required for a device or service to operate—Kim, Park, Park, and Ahn (2019) found that perceived benefits of IoT and organizational trust positively influenced one’s willingness to share personal information, but perceived risks and information sensitivity had no effect on one’s use. Unfortunately, Kim et al. (2019) do not conduct a deep exploration of why the privacy calculus model fell apart when looking at IoT technologies; they instead suggest consumers place higher value on benefits of these technologies and “do not pay much attention” to privacy risks associated with IoT (p. 278).

But this finding highlights some of the biggest problems with privacy calculus as a framework for understanding the complex decision making associated with new technologies. One of the most powerful arguments against framing these decisions as tradeoffs comes from Joseph Turow and colleagues (2015) in their work on the “tradeoff fallacy.” They argue that Americans are increasingly willing to share personal information in exchange for benefits, not because they engage in a rational assessment and see such tradeoffs as fair; rather, Americans have become deeply resigned to sharing their data, believing they have no control or agency to manage it: “Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them” (Turow et al., 2015, p. 3).

This sense of resignation was highlighted in many of our participants’ comments about their IPA use. Turow et al. (2015) note that people experiencing this sense of resignation share their data in unpredictable ways, which may explain why many people in our sample expressed concerns but still used IPAs—and why many used “privacy is dead” tropes to describe their attitudes toward data sharing. These arguments are similar to Hargittai and Marwick’s (2016) work on privacy apathy, where they note that young adults believe “privacy violations are inevitable and opting out is not an option” (p. 3752). They point to the networked nature of privacy that distributes privacy management and information sharing across multiple parties, including the individual, the company or service being used, and (potentially) other users; this shared ownership can make one feel like they lack control over their data.

One of the biggest threats to privacy and technology from smart technologies is in how they are increasingly blurring public and private spaces. A prominent example of this occurrence was seen with the release of Google Glass, which was released in 2012 and raised concerns about the data it could surreptitiously collect in public and private spaces. Wagner (2013) argues that the device infringed on individuals " right to not be recognized by strangers while in public" (p. 486). Smart speakers create a new worry by bringing recording devices into the home and normalizing data collection in traditionally private spaces like one's bedroom. Furthermore, in order to work effectively, users are encouraged to enable the devices to always be turned on, reducing the friction between an information need or task request and the device's ability to complete that task. Shoshanna Zuboff (2019), in her work on surveillance capitalism, argues that friction is the flipside of convenience, with companies wanting to minimize any friction between consumers and technology; it may be that we need to reintroduce some friction into these devices to regain a sense of the boundaries between public and private spaces and information.

Relatedly, we observed increasing concerns associated with feature creep of IPA devices. Overall, participants in our focus groups expressed greater concerns about IPAs that were "always listening" and didn't require an explicit action (like pushing a button) to activate them. These concerns increased when cameras were added to more recent versions (Echo Look and Show) and many expressed concerns related to the uncertainty around *when* the devices collected data and *what* happened to collected data. Amazon recently responded to these concerns by adding new features to allow users to repeat their last command and to explain why it made a recommendation (Conner, 2019), but it is not yet clear if consumers will use these features or decide they provide sufficient levels of transparency.

Overall, our findings show that many IPA users feel a risk of unexpected recordings and uncertainty about how their information might be used or shared beyond the context of their home. Our data also revealed that many users felt unable to conduct a proper threat analysis when making decisions about what information to share with an IPA, due to a lack of technical literacy regarding how the devices collect and process information, as well as due to general vagueness in how the manufacturers communicate these risks. Furthermore, both users and non-users of IPAs expressed concern that they lacked the ability to properly manage their privacy with respect to IPAs.

Limitations

We note several limitations in our study. Participants in the study were employees at two public universities in the United States and have a higher overall education than the general population. We attempted to alleviate participant bias in recruitment in a number of ways: we used random sampling of university employees for the survey study and used criterion sampling (Patton, 2002) to ensure diversity in our focus group participants. We also felt it was important to include perspectives from non-users and to introduce diversity in focus groups, which is why some sessions included only users or only non-users, while others included a mix of users and non-users.

Our data collection occurred at a time when IPAs were receiving news coverage due to a system bug that led Amazon devices to randomly laugh; this may have heightened concerns among participants at the time of data collection. However, the goal of our research was not to generalize to a wider population but to surface themes in how people think about and respond to privacy risks from IPAs and IoT technologies, and we believe our findings provide important directions for future research.

Conclusion

Research suggests IoT technologies will continue to expand in future years, as will the push toward creating smart home ecosystems that can provide instant access to and control over one's home environment with the push of a button on a mobile app or a spoken voice command. As these devices create new privacy risks to users' data, we must continue to evaluate how users' assess and respond to these risks, as this can inform future design and policy. Such evaluations can also provide important insights into how to increase user knowledge and skills related to technology use, as any policy changes to increase consumer data protections will likely take years to implement.

One framework that may be useful in evaluating these risks going forward is Protection Motivation Theory (Maddux & Rogers, 1983; Rogers & Prentice-Dunn, 1997), which highlights the connections between risk appraisal and self-efficacy when considering how motivated users are to protect their privacy when faced with a technology that also provides perceived benefits. This theory provides an important extension to earlier models of privacy management (e.g., privacy calculus) by focusing on subjective appraisals of threats rather than assuming users will make a rational assessment (Dienlin & Metzger, 2016). Early research in this space suggests that while people are more likely to take protective measures when they perceive a threat as severe, they also lack the self-efficacy to confidently and effectively protect their data from threats (Boerman et al., in press).

Future research should apply this theory to people's use of IoT technologies, as it can provide recommendations for the types of information companies should communicate to consumers about the devices, as well as recommendations for updates to existing consumer privacy policies. Looking at findings from the current study, it could be that people who reflected the “nothing to hide” trope in their comments perceive IPAs as having risks, but believe their threat susceptibility is low. However, the risks of these devices are often vague and abstract, so people may be unable to conduct a proper threat analysis when making decisions about sharing their data. Because of this, we believe this study highlights a critical need to shift the burden of protecting privacy from consumers—who often lack the knowledge and skills to properly use existing privacy controls—to companies, who should provide more transparency regarding their data collection practices and enable consumers to make truly informed decisions.

References

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proceedings of the 1st ACM Conference on Electronic Commerce* (pp. 1-80. New York: ACM.

AlHammadi, A., AlZaabi, A., AlMarzooqi, B., AlNeyadi, S., AlHashmi, Z., & Shatnawi, M. (2019). Survey of IoT-Based Smart Home Approaches. *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, 1–6. https://doi.org/10.1109/ICASET.2019.8714572

Authors. (2019).

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), n.p..

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., ... & Scarfone, K. (2018). Considerations for managing internet of things (IoT) cybersecurity and privacy risks. *National Institute of Standards and Technology,* NISTIR 8228.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (in press). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research.* https://doi.org/10.1177/0093650218800915

Chokshi, N. (2018, March 8). Amazon knows why Alexa was laughing at its customers. *New York Times.* Available: https://www.nytimes.com/2018/03/08/business/alexa-laugh-amazon-echo.html

Conner, K. (2019, October 24). Have Amazon Echo privacy fears? Here’s what you can do. *CNET.* Available: https://www.cnet.com/how-to/have-amazon-echo-privacy-fears-heres-what-you-can-do/

Culnan, M. J. (1993). “How did they get my name?”: An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, *17,* 341-363.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*, 323-342.

Day, M., & Turner, G., & Drozdiak, N. (2019, April 24). Amazon’s Alexa team can access users’ home addresses. *Bloomberg Technology.* Available: https://www.bloomberg.com/news/articles/2019-04-24/amazon-s-alexa-reviewers-can-access-customers-home-addresses

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21,* 368-383. doi:10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*, 61-80.

Fowler, G.A. (2018, May 24). Hey Alexa, come clean about how much you’re really recording us. *Washington Post*. Available: https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/

Gartner. (2017, February 7). *Gartner says 8.4 billion connected “things” will be in use in 2017, up 31 percent from 2016.* Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Green-Pedersen, C., Kersbergen, K. V., & Hemerijck, A. (2001). Neo-liberalism, the “third way” or what? Recent social democratic welfare policies in Denmark and the Netherlands.

Journal of European Public Policy, *8*(2), 307–325. https://doi.org/10.1080/13501760110041604

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state.* New York: Metropolitan Books.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80. https://doi.org/10.1145/1102199.1102214

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281.

Lau, J., Zimmerman, B., & Schaub, F. (2018a). Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102, 31 pages. doi: https://doi.org/10.1145/3274371

Josephine Lau, Benjamin Zimmerman, and Florian Schaub. (2018b)."Alexa, stop recording": Mismatches between smart speaker privacy controls and user needs. *Poster presented at the 14th Symposium on Usable Privacy and Security (SOUPS 2018).*

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, *33*, 22-42.

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). Understanding the role of privacy and trust in intelligent personal assistant adoption. In N. G. Taylor, C. Christian-Lamb, M. H. Martin, & B. Nardi (Eds.), *Information in Contemporary Society* (pp. 102–

113). https://doi.org/10.1007/978-3-030-15742-5_9

Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. *Pew Internet Project.* Available: https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19,* 469-479.

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* (pp. 250-271). https://content.sciendo.com/view/journals/popets/2019/4/article-p250.xml

Miles, M., Huberman, M., & Saldana, J. (2013). SAGE: Qualitative Data Analysis: A Methods Sourcebook.

Moorthy, A.E., & Vu, K.P.L. (2015). Privacy concerns for use of voice activated personal assistant in the public space. *International Journal of Human-Computer Interaction*, *31*(4), 307-335.

Nath, R. K., Bajpai, R., & Thapliyal, H. (2018). IoT based indoor location detection system for smart home environment. *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 1–3. https://doi.org/10.1109/ICCE.2018.8326225

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.

Patton, M.Q. (2002). *Qualitative research & evaluation methods.* Sage Publications: Thousand Oaks, CA.

Pew Research Center. (2017, December 12). *Nearly half of Americans use digital voice* *assistants, mostly on their smartphones.* Available: https://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/

Pew Research Center. (2019, July 22). *Americans' trust in government, each other, leaders.* Available: https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/

Pradhan, A., Mehta, K., & Findlater, L. (2018). "Accessibility came by accident": Use of voice-controlled intelligent personal assistants by people with disabilities. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Paper No. 453). New York: ACM. https://doi.org/10.1145/3173574.3174033

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113-132). New York, NY, US: Plenum Press.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2347-2356). New York: ACM. https://doi.org/10.1145/2556288.2557421

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory, 2nd edn.* Thousand Oaks, CA: SAGE.

Missing Turow citation

Vitak, J. (2016). A digital path to happiness? Applying Communication Privacy Management theory to mediated interactions. In L. Reinecke & M.B. Oliver (Eds.), *Handbook of media use and well-being: International perspectives on theory and research on positive media effects* (pp. 274-288). New York: Routledge.

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018, March). Privacy attitudes and data valuation among fitness tracker users. In *International Conference on Information* (iConference) (pp. 229-239). Springer, Cham.

Voicebot AI. (2019, March). Smart speaker consumer adoption report. Available: https://voicebot.ai/wp-content/uploads/2019/03/smart_speaker_consumer_adoption_report_2019.pdf

Wagner, M. S. (2013). Google Glass: A preemptive look at privacy concerns. *Journal on Telecommunications and High Technology Law, 11*, 477-490.

Williams, M., Nurse, J. R., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-Things. In *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 644-652). IEEE.

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2015). Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing*, *19*(2), 463-476.

Woolf, N. (2016, October 26). DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian.* Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *In Proceedings of the Thirty Third International Conference on Information Systems* (pp. 1-16). Association for Information Systems.

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS)* (pp. 65-80). USENIX.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction archive Volume 2 Issue CSCW* (Article 200). doi:10.1145/3274469

Zuboff, S. (2019). *The age of surveillance capitalism.* New York: Public Affairs.

Appendix

Table 1: Descriptive Data for Focus Group Sessions

Focus Group #	Group Type	Number of Participants	Sex (%=male)	User Type (%=IPA user)	Age Mean (SD)
Group 1	User Only	4	25%	100%	41.75 (11.84)
Group 2	User Only	7	14%	100%	39.14(11.28)
Group 3	Mix	6	50%	50%	39.67(14.15)
Group 4	Mix	6	50%	33%	36.00(12.08)
Group 5	Mix	8	63%	38%	38.13 (14.23)
Group 6	User Only	6	50%	100%	39.50(15.15)
Group 7	Non-User Only	4	25%	0%	35.25 (16.68)
Group 8	User Only	8	25%	100%	35.13(11.49)
Group 9	Mix	8	63%	75%	31.38(9.16)
Group 10	Mix	6	17%	67%	37.33(8.94)
Group 11	Non-User Only	2	50%	0%	50(12.76)
Totals	4 User, 5 Mixed, 2 Non-User	65	40%	66%	37.45(11.23)

Table 2: Codes and Code Definitions for Qualitative Analysis

Code Name in Dedoose	**Code Description**
Compare IPAs	Explicit statements comparing features of or attitudes toward two or more versions of IPAs (e.g., Siri, Home, Echo Show).
Privacy-Security	Participant talks broadly about how technology affects privacy, security, surveillance, and related topics. Strategies they employ to attain desired level of privacy/security. Comments about corporations using/accessing their data.
IPA Listening	Explicit responses to question, "Do you have a sense of when these devices are listening for your voice or if they're always listening?" Also, general comments about IPA microphones and their capabilities, as well as concerns about when IPAs are capturing audio data and what happens to that data.
Nothing to Hide	Comments that there are minimal risks to using IPAs, the participant's "life is boring," etc.
Privacy Apathy	Comments reflecting the belief that privacy is dead, we are already tracked in many ways, etc.
Reaction to Echo Show	Comments and discussion captured after watching the Echo Show commercial