Research Article

CONVERGENCE

Convergence: The International
Journal of Research into
New Media Technologies
2021, Vol. 0(0) 1–20
© The Author(s) 2021
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/13548565211042234
journals.sagepub.com/home/con
SAGE

Household intelligent personal assistants in the Netherlands: Exploring privacy concerns around surveillance, security, and platforms

Anouk Mols, Yijing Wang and Jason Pridmore
Erasmus University Rotterdam, Rotterdam, The Netherlands

Abstract

Intelligent personal assistants (IPAs), also known as smart speakers, are becoming part of everyday life in more and more households around the world. Phone and household IPAs are integrated in intimate home contexts and require connections to (social) media profiles, user accounts, and domestic appliances. Users can control their household with voice-activated commands in order to make life more convenient and efficient. Yet, IPAs also bring privacy and surveillance concerns about devices "listening in," the "platformization" of home life, and data security. Our exploratory mixed-methods study provides an in-depth and multidimensional account of users' privacy concerns around the emergence of IPAs in Dutch households. We differentiate between surveillance, security, and platform concerns, and our survey results indicate by which factors these are influenced. The focus group analysis highlights the role of conversation, recordability, locatability, control-ability, and assistance affordances. Our findings present a multidimensional and nuanced understanding of privacy concerns around household IPAs. We indicate how smart home technologies raise concerns about privacy, surveillance, device security, everyday behavior, and platform transparency, topics that demand urgent attention before the integration of IPAs will be fully normalized.

Keywords

Affordances, intelligent personal assistants, privacy, smart speakers, voice assistants

Introduction

> A man in sweatpants and socks enters the kitchen and says: "OK Google. Play the morning playlist." A Google Home device on kitchen counter lights up and replies: "OK, playing morning playlist." Soft music starts to play. Man: "OK Google, play music in all rooms."

Corresponding author:
Anouk Mols, Media and Communication, Erasmus Universiteit Rotterdam, Campus Woudestein, Burgemeester Oudlaan 50, Rotterdam 3000 DR, The Netherlands.
Email: mols@eshcc.eur.nl

This is a fragment from a Google Home commercial about a family (Peek of the Net, 2017). Google Home devices are integrated into this family's morning routine and are consulted by all family members for travel updates, homework queries, calendar items, and traffic information. This commercial illustrates how household Intelligent Personal Assistants (IPAs), also referred to as smart speakers, are becoming part of everyday life. Household IPAs were directly preceded by IPAs on smartphones. Such voice-activated virtual assistants include Apple's Siri, Google Now/Google Assistant, Microsoft's Cortana, and Samsung's Bixby (Kinsella and Mutchler, 2019). While phone IPAs function via an app and are not bound to a location, household IPAs work with the same technology but take the form of standalone devices which need an internet connection and power to function. Household and phone IPAs can be activated with a trigger word in order to get answers to questions, set alarms or timers, listen to music, control smart appliances (such as lamps, smart TVs, and doorbells), listen to news or hear the weather, call someone, access calendars, send text messages, or make purchases (Kinsella and Mutchler, 2019). The US is forerunner in adoption with nearly 90 million US adults using household IPAs in January 2020—34.4% of all US adults (Kinsella, 2020). In 2018, household IPA ownership in Western Europe amounted to 22.4% of internet users in the UK, compared to 17.2% in Germany and 14% in France (McNair, 2019). The most popular household IPAs are Amazon's Echo devices, Google's Home devices, and Apple's HomePod (Perez, 2019). The integration and normalization of household IPAs has led to concerns in relation to the devices "listening in" (Lau et al., 2018), the "platformization" of the home (Pridmore et al., 2019, based on Helmond, 2015), and security (Lei et al., 2017). Researchers emphasize that more awareness about the privacy implications of household IPA use is required (Chandrasekaran et al., 2018; Lutz and Newlands, 2021; Manikonda et al., 2017).

Our mixed-methods study is based on a survey and focus groups and explores privacy concerns of potential users in the the Netherlands. We provide insights about a continental European population that is culturally distinctive from previous studies which mainly research US and UK populations (Huang et al., 2020; Liao et al., 2019; Manikonda et al., 2017). This study also focuses on a population just at the cusp of normalizing these devices within the home—our research took place in Spring 2018, whereas after the introduction of the Google Home in November 2018, household IPA ownership grew from 5% of all Dutch households in 2019 to 19% in April 2020 (Multiscope, 2019, 2020).

A growing body of research about household IPA use discusses privacy concerns whereby only a few researchers differentiate between different types of concerns (Lutz and Newlands, 2021; Manikonda et al., 2017). Because privacy concerns are not uniform, we distinguish between surveillance, security, and platform-related issues which are presented in the literature section. Subsequently, our results section contributes to a multidimensional understanding of household IPA privacy concerns whereby we highlight the role of affordances. Our survey examines to what extent multidimensional privacy concerns are influenced by their familiarity to the internet, digital literacy, general privacy concerns, and phone IPA use. The analysis is guided by RQ1: *Which factors influence household IPA privacy concerns in the context of surveillance, security, and platforms?* Subsequently, the results from our focus groups are used to explore the role of affordances in order to answer RQ2: *What role do affordances play in household IPA privacy concerns in the context of surveillance, security, and platforms?* We draw out a nuanced understanding of privacy perceptions around household IPAs, indicating how these smart home technologies raise concerns about privacy, surveillance, device security, everyday behavior, and platform transparency.

Literature: Household IPAs, privacy concerns, and affordances

Household IPA use goes hand in hand with everyday negotiations around user privacy. Researchers suggest that more awareness of privacy threats of household IPAs and knowledge about protective practices is needed (Malkin et al., 2019; Manikonda et al., 2017). However, others indicate that awareness not always leads to privacy protecting practices (Huang et al., 2020; Lutz and Newlands, 2021). It might be the case that some users of household IPAs accepted these privacy risks or became fatalistic or apathetic toward privacy concerns (Lau et al., 2018; Lutz and Newlands, 2021; Pridmore et al., 2019). Nevertheless, privacy concerns have had a demonstrably weakening effect on motivations for household IPA use (McLean and Osei-Frimpong, 2019). Recent studies including non-users suggest that privacy concerns can also lead to a lack of trust in household IPA platforms, and consequently, form a reason not to use a household IPA (Lau et al., 2018; Liao et al., 2019). Therefore, it is important to provide a better understanding of the foundations of privacy concerns and insights into diversity within these. Following Lutz and Newlands (2021) and Manikonda et al. (2017), we use a multidimensional conceptualization of household IPA privacy concerns. We differentiate between surveillance, security, and platform concerns: Surveillance concerns revolve around household IPA devices being perceived as surveilling agents listening in on users; security concerns focus on device security threats; and platform concerns regard issues around data collection, processing, and sharing by IPA platforms.

Privacy as a multidimensional concept

Surveillance, security, and platform-related privacy concerns each focus on different aspects of household IPA use. Privacy is a fluid and abstract concept, loaded with moral considerations. There are many definitions of privacy connected to different aspects of human life and the concept is seen as essentially contested due to its openness and internal complexity (Mulligan et al., 2016). In order to deal with the complex nature of privacy, we follow Koops et al.'s typology of privacy (2016) and approach privacy as a multifaceted concept. Koops et al. (2016) present nine types of privacy, whereby information privacy can be seen as an integral to as well as overarching the other eight types. Information privacy is paramount to household IPA privacy concerns because these revolve around the collection of and access to user data and personal information. In the context of household IPA use, information privacy is intertwined with three other types—namely, communicational, spatial, and intellectual privacy (Koops et al., 2016). Communicational privacy of mediated and unmediated communication can be infringed when users interact with and around household IPA devices. Moreover, intellectual privacy can be at stake when IPAs influence how users develop opinions and beliefs. Finally, household IPA use can infringe spatial privacy of the private sphere and intimate activities. In order to take physical and virtual spaces into account, territorial privacy forms a relevant addition for this research. Territorial privacy addresses privacy around what can be observed (i.e., recorded/collected) about a person in their personal space and what can be observed by entities having virtual access to the personal space (Könings et al., 2010). This applies to household IPA use whereby devices are able to record audio (and some devices also video) in the physical personal space whereby platform actors, third-party service providers, and in some cases malicious actors, can access these recordings virtually. The following sections zoom in on how information, spatial, territorial, intellectual, and communicational privacy concerns are linked to particular surveillance, security, and platform issues.

Surveillance concerns

The increase of household IPA adoption is accompanied by growing concerns about communicational privacy of unmediated communication (Koops et al., 2016). In the past years, several issues prompted public debate about household IPAs "listening in" and acting without user requests.

People were concerned about the story of a Google Home Mini recording and sending to Google servers 24/7 which was caused by a malfunctioning touch-button—now disabled on all Google Mini devices (Russakovskii, 2017). An Amazon Echo device not only recorded a private conversation, but also sent this to a random contact (Horcher, 2018). People were also made uncomfortable by reports of Amazon Echo devices laughing randomly without being prompted (Chang and Mogg, 2018). While these issues seemingly focus on isolated technical incidents, researchers found that users are often concerned about devices acting as surveillance machines. Household IPA users in the UK voiced concerns about the device listening to them constantly and were afraid that it would record intimate conversations (Manikonda et al., 2017). Moreover, American non-users expressed that they felt uncomfortable with putting a device with a microphone in their private home because this would harm its sanctity (Lau et al., 2018).

Security concerns

The security of household IPAs is tested and challenged by researchers who found that there are different security vulnerabilities which can be exploited by hackers to access houses with smart doorbells and to make purchases via household IPAs (Lei et al., 2017). Because this concerns the private space in physical and virtual form, these practices infringe users' spatial (Koops et al., 2016) as well as territorial privacy (Könings et al., 2010). Remarkably, users might increase security risks when they fail to protect their routers and connect their device to appliances with weak security (Furey and Blue, 2018). According to Manikonda et al.'s (2017) US-based survey results, many household IPA users are concerned that their device will be hacked, they fear that this makes them vulnerable to malware or cybersecurity breaches. When users in the US were presented with three different household IPA security technologies to explore privacy and security concerns, they proved to be aware of different types of threats (such as software bugs causing erroneously behavior and platforms/third parties listening in). Yet, they were not concerned about these threats having personal privacy implications (Chandrasekaran et al., 2018). Notably, non-users in the US displayed more concerns about household IPAs being hacked than active users (Lau et al., 2018). In general, many users are unaware of security risks and how to secure their devices (Furey and Blue, 2018).

Platform concerns

Household IPAs collect, process, and share personal data to function. Connected media accounts, smart appliances, and credit cards enable users to control entertainment services, manage smart appliances, and make purchases via their household IPAs. These practices are embedded in smart home ecosystems connected to third-party providers of services, skills, and smart appliances, something that many household IPA users are not aware of (Abdi et al., 2019). The fact that these third parties also have access to the (meta)data of IPA users complicates privacy protection and awareness, and infringes information privacy (Koops et al., 2016). Moreover, cases have been reported where governments requested household IPA recordings for law enforcing purposes (Fussel, 2020). Malkin et al. (2019) found that many American household IPA users seem to be unaware of the fact that their requests toward the device are stored. Once made aware of this, most users wanted to be able to delete recordings in order to avoid private conversations ending up in the hands of the platform owners, prevent platforms from building detailed profiles, and protect children and guests from being monitored. Moreover, Huang et al. (2020) suggest that some American users are concerned about data collection by IPA platforms and about a lack of clarity and transparency around how data are used and shared.

Data collection via platforms seems to instigate the most pressing privacy concerns. For UK users, concerns about third-party developers of software/skills/apps and contractors, and to a lesser extent household IPA platforms and law enforcement are more pressing than concerns about social privacy issues (Lutz and Newlands, 2021). Interestingly, German users expressed fear that governments can request access to their household IPA data while they were less concerned about data use by IPA platforms (Pridmore and Mols, 2020). Moreover, contextual differences also become visible in how users regard different types of data. Namely, financial transactions and credit card account information are deemed more sensitive than other types of information (Huang et al., 2020; Manikonda et al., 2017; Pridmore et al., 2019).

This inventory of research findings about household IPA privacy concerns in three different contexts indicates the need for more research into what drives these concerns and on which perceptions they are based. In order to provide insight into the drivers of these concerns, our survey data follows the exploratory research question: Which factors influence household IPA privacy concerns in the context of surveillance, security, and platforms? (RQ1)

IPA affordances

A recurring theme in discourses about household IPAs, something that also came up in our focus groups, is the notion that household IPAs enable users to "do" everyday practices differently. To makes sense of how potential users regard these activities and experiences offered by household IPAs we turn to the concept of affordances. Gibson coined the term "affordances" in 1979 to describe how environments and objects have basic properties which "afford" humans to engage in particular actions or behavior. For instance, some objects "afford" to be lifted and carried (e.g., due to their shape or because they have a handle), while others do not (Gibson, 2014). Affordances can broadly be defined as "possibilities for action" which take place in relations between humans, technologies and their material features, and the situated nature of use (Evans et al., 2017: 36).

Affordances are enacted social, physical, and technological contexts, and therefore the situational context must be considered in order to understand an object's affordances (Humphreys et al., 2018). The concept of affordances has been widely used yet there is no consistent application. Bucher and Helmond (2017) and Evans et al. (2017) present helpful analyses of different (mis)uses of the term and offer tools to analyze affordances in social media contexts. In our analysis, we build on Nagy and Neff's (2015) concept of "imagined affordances." The concept imagined affordances includes material, mediated, and emotional aspects of human-technology interaction and takes relations between designers, users, and algorithms, as well as user perceptions, emotions, and experiences into account. Imagined affordances "emerge between users' perceptions, attitudes, and expectations; between the materiality and functionality of technologies; and between the intentions and perceptions of designers." (Nagy and Neff, 2015: 5) The authors provide an example of an imagined affordance by describing how the Facebook News Feed is perceived by users as offering objective reporting of posts of their Facebook friends, "rather than an algorithmically encoded parsing of them." (Nagy and Neff, 2015: 5) This conceptualization of socio-technical imagined affordances provides useful tools to analyze mediated uses of technologies embedded in intangible platforms and operated via hidden algorithms—such as household IPAs.

Previous studies indicate that the particular affordances of household IPAs enable users to engage in specific practices. Building on affordances from a relational perspective (Evans et al., 2017), Lutz and Newlands (2021) mention how the relation between household IPAs and users brings possibilities for action in enabling interactivity, searchability, and recordability. There are no details provided about these affordances; however, the authors indicate that they can enable interpersonal surveillance practices between family members (Lutz and Newlands, 2021). Furthermore, Brause and Blank (2020) identify three spatial affordances in household IPA use. The first is potential ubiquity, users can connect household IPAs to other devices and their phones to create seamless experiences in their IPA use. Second, household IPAs can connect spatially separated people via their link-ability. The third spatial affordance concerns control-ability which allows users to control a plethora of connected devices via one device. Finally, Cho (2019) presents voice interaction as a key affordance of IPAs. Communication via voice interaction can afford the experience of engaging in a social conversation, in contrast to less "social" experiences of text interactions. However, this effect only occurred for users with low privacy concerns and for interactions about non-sensitive health topics (compared to more sensitive health topics) (Cho, 2019).

In the analysis of our focus groups, we aim to provide an in-depth understanding of how specific socio-technical affordances are paramount to multidimensional privacy concerns around surveillance, security, and platforms. This analysis is guided by the question: What role do affordances play in household IPA privacy concerns in the context of surveillance, security, and platforms? (RQ2)

Methods: Survey and focus groups

Our research design combines an exploratory survey with semi-structured focus groups in order to provide an in-depth and multidimensional understanding of household IPA privacy concerns. The research was conducted among Dutch university personnel (research as well as support staff), a sample that enabled us to explore a variety of attitudes toward household IPAs as a novel technology (rather than focusing on a more uniform group such as early adopters). This mixed-method study includes qualitative focus group data to explain the initial results of the quantitative survey data, following an explanatory sequential design (Creswell and Plano Clark, 2017). In the focus groups, we engaged participants in conversations about household IPA use with the aim of exploring their perceptions (Stewart et al., 2007).

Survey sampling, measurements, and variables

In April 2018, we distributed our survey via email to 3000 employees of a university in the the Netherlands, including university staff and research personnel. A total of 325 respondents participated in the survey, among which, 291 completed the questionnaire, resulting in a response rate of 10%. The following control variables are included. Gender; approximately 36.2% of the final sample identified as male *(N = 114*) and 58.4% identified as female *(N = 170)* (5.4% of the respondents preferred not to answer this question). Education level; the majority of the participants *(55%, N = 160)* obtained a master's degree. The age of the respondents varied from 22 to 64 *(M = 37, SD = 11*). Annual household income; 22.7% *(N = 66)* respondents indicated an income between €25k–40k, 11.3% *(N = 33)* indicated €40k–50k, 17.2% *(N = 50)* indicated €50k–65k, 14.4% *(N = 42)* indicated €65k–85k, 14.4% *(N = 42)* indicated €85k–130k, and 4.1% *(N = 12)* above €130k (11.3% of the respondents preferred not to answer this question).

The majority of the respondents use either an iPhone *(N = 140, 48.1%)* or an Android device *(N = 136, 46.7%),* the remaining 5.2% of the respondents use a different operating system. Further, 17.9% *(N = 52)* respondents indicated that they are currently using a phone IPA, whereas only 4.5% *(N = 13)* respondents are using a household IPA. Mobile and household IPA use takes place in broader repertoires of everyday technology use, and IPAs are by nature interconnected with mobile phones, entertainment services, and other technologies. Therefore, our survey explores privacy perceptions around household IPAs in the broader context of everyday technology use. More specifically, we aimed to identify how IPA-focused privacy concerns relate to more general technology perceptions such as internet familiarity, digital literacy, general privacy concerns, mobile privacy concerns, mobile privacy confidence, and smartphone reliance. Below follow descriptions of the dependent and independent variables, through which we indicate how some variables are constructed for this study, whereas others are based on existing scales. The full survey is included in Supplementary Appendix 1 and an overview of the reliability tests is presented in Table 1.

Dependent variables (all developed for this survey). Household IPA surveillance concerns. This variable measures how concerned respondents are about IPA devices functioning as a surveilling agent. Two items are combined into one variable through a weighted averaged method. The first item is "I am concerned that the device is always listening," and the second item is "I am concerned that the device is always recording any sounds in the room." Both statements were followed by a 5-point scale from "Not at all concerned" to "Extremely concerned." The reliability test shows a modest internal consistence of the items *(α = 0.681, M = 2.739, SD = 1.043)*.

Household IPA security concerns: This variable measures how concerned respondents are about security vulnerabilities of household IPAs being exploited. Two items are combined into one variable through a weighted averaged method, which are "I am concerned that other people might activate/access the device and trigger unauthorized purchases," and "I am concerned that other people might activate/access the device and disrupt my internet accounts or personal information." The reliability test shows a good internal consistence of the items *(α = 0.720, M = 3.371, SD = 1.111)*.

Household IPA platform concerns. This variable measures how concerned respondents are about household IPA data being stored and used by law enforcement, third parties, and by IPA platforms. Three items are combined into one variable through a weighted averaged method. An example item is "I am concerned that my questions directed at the device are stored and sold to third parties (e.g., advertisers)." The reliability test shows a high internal consistence of the items *(α = 0.849, M = 3.538, SD = 1.088)*.

Table 2 shows the correlation matrix of the constructed variables. Among the three dependent variables, we observe a positive correlation between *household IPA surveillance concern* and *household IPA security concern (r = 0.695, p < 0.01)*, and between *household IPA surveillance concern* and *household IPA platform concern (r = 0.596, p < 0.01)*. The strongest correlation is found between *household IPA security concern* and *household IPA platform concern (r = 0.810, p < 0.01)*.

Table 1. Descriptive statistics and internal consistency of variables.

	Mean	Std. Dev	Cronbach's α
Internet familiarity (IF) (10 items, 5-point scale)	4.023	0.76	0.883
Digital literacy (DL) (10 items, 5-point scale)	4.105	0.804	0.902
General privacy concerns (GPC) (12 items, 5-point scale)	3.183	0.901	0.918
Mobile privacy concerns (MC) (9 items, 5-point scale)	3.965	0.737	0.920
Mobile privacy confidence (MCF) (4 items, 5-point scale)	2.169	0.736	0.644
Household IPA *surveillance* concerns (HSU) (2 items, 5-point scale)	2.739	1.043	0.681*
Household IPA *security* concerns (HSE) (2 items, 5-point scale)	3.371	1.111	0.720*
Household IPA *platform* concerns (HPA) (3 items, 5-point scale)	3.538	1.088	0.849
Smartphone reliance (SR) (2 items, 0–100)	61.085	21.569	0.644*

Notes: (1) *N* = 291. (2) *Spearman–Brown coefficients are reported for variables measured through 2-item scales.

Independent variables. Internet familiarity. This variable uses Hargittai and Hsieh's (2012) 10-item Abbreviated Web-Use Skills Index for the General Population. This scale is often used as a variable in surveys regarding privacy decisions (Fiesler et al., 2017; Zimmer et al., 2020). The reliability test shows a high internal consistence of the items *($\alpha = 0.883$, $M = 4.023$, $SD = 0.76$).*

Digital literacy (related to smartphone use). Specifically developed for this survey, this 20-item variable measures respondents' level of confidence with regard to conducting particular tasks on their smartphones. The reliability test shows a high internal consistence of the items *($\alpha = 0.902$, $M = 4.105$, $SD = 0.804$).*

General privacy concerns. We used Vitak's 12-item general privacy concerns scale (2015), this scale is also used by Vitak and others in different contexts, such as fitness trackers and social media use (Vitak, 2016; Vitak et al., 2018) and Facebook use among colleagues (Van Prooijen et al., 2018). This variable maps how concerned respondents are about risks related to digital communication technologies via a 5-point scale from "Not at all concerned" to "Extremely concerned." The reliability test shows a high internal consistence of the items *($\alpha = 0.918$, $M = 3.183$, $SD = 0.901$).*

Mobile privacy concerns. This variable uses Xu et al.'s 9-item mobile users' information privacy concerns scale (2012) including questions about perceived surveillance, perceived intrusion, and secondary use of personal information. This scale is also used in research about health apps (Bol et al., 2018). A high internal consistency of the items is observed *($\alpha = 0.920$, $M = 3.965$, $SD = 0.737$).*

Mobile privacy confidence. Mobile privacy confidence is measured by four items, designed for this study, which measure how confident respondents feel about their mobile privacy. The internal consistency of the constructed variable is modest but acceptable *($\alpha = 0.644$, $M = 2.169$, $SD = 0.736$).* While the alpha is close to the 0.7 threshold, it still indicates a good reliability of the measurement as is the case for other variables noted below.

Household IPA familiarity. Household IPA familiarity (constructed for this study) is measured as a 0/1 variable based on respondents' familiarity with either "Google Home / Home Mini," "Amazon Echo / Echo Dot" or "Apple HomePod" (value = 1), or none of those (value = 0).

Table 2. Correlation matrix.

	If	Dl	GPC	MC	MCF	HSU	HSE	HPA	SR
IF	1								
DL	0.450**	1							
GPC	0.033	0.028	1						
MC	0.028	−0.060	0.454**	1					
MCF	0.149*	0.294**	−0.155*	−0.365**	1				
HSU	0.007	−0.066	0.456**	0.430**	−0.195**	1			
HSE	0.073	−0.030	0.443**	0.511**	−0.246**	0.695**	1		
HPA	0.098	−0.071	0.409**	0.598**	−0.269**	0.596**	0.810**	1	
SR	0.155*	0.223**	0.084	−0.055	−0.004	0.048	0.063	−0.008	1

Notes: (1) ** $p < 0.01$. * $p < 0.05$.2) $N = 291$.

Phone IPA use. This variable is designed for this study and constructed from the question “Do you have Siri, Google Assistant, or another intelligent personal assistant (IPA) activities on your smartphone?” Respondents who answered “Yes, I currently use it” are assigned to one group (value = 1), whereas the rest who chose another answer (“My phone has this feature but I’ve never used it”; “No, and I have disabled this feature”; or “No, there isn’t a service like that available on my phone”) are assigned to the other group (value = 0). Hence, a 0/1 dummy variable is created.

Smartphone reliance. This variable (constructed for this study) is measured by two items on a 100-point slider scale. Respondents indicate how often they access their smartphone and how anxious they feel after leaving the house without their smartphone. Both items reflect a respondent’s smartphone reliance, and thus are combined to construct the variable. The internal consistency of the constructed variable is modest but acceptable ($\alpha = 0.635$, $M = 61.085$, $SD = 21.569$).

Focus group design and analysis

We used an experimental focus group design aimed at collecting rich, in-depth data. The six focus groups (*N* = *35*) were semi-structured, one was conducted in English, and the other five in Dutch. Details about the focus group respondents are included in Supplementary Appendix 2. The focus groups were conducted in May 2018. Notably, at that time only two participants (Hannah and Mark) owned a household IPA and because smart speakers were not officially available on the Dutch Market they could only operate these in English and could not connect them to many services. Moreover, four respondents (Bjorn, Julia, Anna, and Linda) first-handedly experienced the use of smart speakers when they visited friends in the UK and US. All focus group discussions followed a two-phase set-up, the focus group conversation guide is included in Supplementary Appendix 3. Phase 1 included a discussion of technology use in general, and the experiences with phone IPAs in particular. Phase 2 focused on household IPAs. The respondents first watched a commercial of Google Home (described in introduction) wherein multiple Google Homes are integrated in the life of a busy family. The respondents were then invited to interact with a Google Home device that was installed in the focus group space and was connected to a lamp and a smart TV (with YouTube, Netflix, and Spotify). We provided example prompts, such as “OK Google, what is the weather forecast”; “OK Google, switch on the lamp”; and “OK Google, play Bruno Mars on Spotify.” In all focus group conversations, engaging with the device naturally led to a conversation about the device which was guided by specific follow-up questions from the moderator. The group discussions were recorded, transcribed, and analyzed in an inductive manner (inspired by a constructivist grounded theory approach as described by Charmaz, 2014). First, a round of open coding took place whereby we labeled the transcripts with verbatim codes (such as “sneaky goals platforms”). In an iterative manner, the open codes were then clustered into conceptual categories (such as “platforms and distrust”). After this axial coding, we connected the conceptual categories in the selective coding phase to three distinct concerns—around household IPA surveillance, security, and platforms. The codebook is included in Supplementary Appendix 4. In the results section we present translated quotes and connect these to existing research and the concept of affordances to provide an in-depth account of the three different household IPA privacy concerns.

Results

Survey results: Factors influencing surveillance, security, and platform concerns

To assess the factors influencing different household IPA privacy concerns around surveillance, security, and platforms (RQ1), we conducted three ordinary least squares regression analyses. Their results are summarized in Table 3.

Model 1 shows the impact of constructed independent variables on household IPA *surveillance* concerns. The results reveal that if general privacy concerns are perceived higher, it will lead to a higher household IPA *surveillance* concern *(β = 0.405, SE = 0.077, p < 0.001)*. Also, higher mobile privacy concerns correspond to higher household IPA *surveillance* concerns *(β = 0.403, SE = 0.099, p <0.001)*. Interestingly, a significant difference is detected between people who currently use a phone IPA versus others who do not. Phone IPA users are found to be concerned less about household IPA *surveillance* than non-users *(β = −0.348, SE = 0.175, p < 0.05)*. One potential explanation is that the experience of using a phone IPA helps people lower their concerns about household IPAs "listening" in or recording conversations because they have overcome or have never experienced such concerns toward their phone IPA. Another potential explanation could be an

Table 3. Assessing household IPA *surveillance*, *security,* and *platform* concerns.

	Model 1	Model 2	Model 3
	DV = household IPA *surveillance* concerns	DV = household IPA *security* concerns	DV = household IPA *platform* concerns
Parameter estimates: Beta (SE.)			
Internet familiarity	−0.026 (0.100)	0.018 (0.101)	0.156 (0.096)
Smartphone reliance	−0.001 (0.003)	0.001 (0.003)	−0.001 (0.003)
Digital literacy	−0.029 (0.091)	−0.034 (0.092)	−0.136 (0.087)
General privacy concerns	0.405 (0.077)***	0.262 (0.078)***	0.157 (0.074)*
Mobile privacy concerns	0.403 (0.099)***	0.589 (0.100)***	0.695 (0.095)***
Mobile privacy confidence	−0.082 (0.091)	−0.110 (0.092)	−0.060 (0.087)
Phone IPA use (yes)	−0.348 (0.175)*	−0.460 (0.177)**	−0.442 (0.168)**
Household IPA familiarity	0.094 (0.058)	0.198 (0.059)***	0.159 (0.056)**
Gender	0.134 (0.092)	0.138 (0.093)	0.165 (0.088)
Age	0.002 (0.006)	−0.002 (0.006)	0.001 (0.006)
Education	−0.033 (0.056)	−0.039 (0.057)	0.037 (0.054)
Household	0.008 (0.060)	−0.033 (0.061)	0.019 (0.057)
Income	0.031 (0.037)	0.039 (0.037)	−0.021 (0.035)
Constant	0.001 (0.769)	0.264 (0.778)	−0.187 (0.738)
F-value	*7.552* *p < 0.001*	*8.672* *p < 0.001*	*10.327* *p < 0.001*
R-square	*0.321*	*0.351*	*0.393*

Notes: (a) *** $p < 0.001$. ** $p < 0.01$. * $p < 0.05$. B) $N = 291$.

unidentified common factor, which drives peoples' intention to use IPAs, both on phones and at home.

Model 2 in Table 3 shows the impact of constructed independent variables on household IPA *security* concerns. The results reveal a positive relationship between general privacy concerns and household IPA *security* concern *(β = 0.262, SE = 0.078, p < 0.001)*, as well as a positive relationship between mobile privacy concerns and household IPA *security* concern *(β = 0.589, SE = 0.100, p < 0.001)*. Phone IPA users are found to be concerned less about household IPA *security* issues than non-users *(β = −0.460, SE = 0.177, p < 0.01)*. In addition, different from the results of Model 1, we found a positive impact of household IPA familiarity on household IPA *security* concern *(β = 0.198, SE = 0.059, p < 0.001).* It implies that people with knowledge of household IPAs are more concerned about its security risks, compared to those who know less about such devices. It might be the case that these people have heard about household IPAs via newspaper articles about the devices laughing unexpectedly which were covered in Dutch news media a couple of weeks before our survey was conducted (*RTL Nieuws*, 2018).

Model 3 in Table 3 shows the impact of constructed independent variables on household IPA *platform* concerns. The results reveal a positive relationship between general privacy concerns and household IPA *platform* concerns *(β = 0.157, SE = 0.074, p < 0.05)*, and a positive relationship between mobile privacy concern and household IPA *security* concern *(β = 0.695, SE = 0.095, p < 0.001)*. Phone IPA users are found to be less concerned about household IPA *platforms* than non-users *(β = −0.442, SE = 0.168, p < 0.01)*. Also, similar to Model 2, we found a positive impact of household IPA familiarity on household IPA *platform* concerns *(β = 0.159, SE = 0.056, p < 0.01).* In addition, a comparison of the R-square (see Table 3) shows the difference in explained variance between the three models: The independent variables were most predictive and accounted for most variance in Model 3 (platform concerns), followed by Model 2 (security concerns) and Model 1 (surveillance concerns).

The most striking finding is the fact that respondents who are familiar with household IPAs are found to be more concerned when it comes to household IPA *security* and *platform* concerns than they are about *surveillance* aspects. This might suggest that being exposed to information about household IPAs (via commercials, through experiences of peers, or by having interacted with a device) lowers "creepy" associations of devices functioning as *surveillance* agents. In contrast, this familiarity sparks concerns about platform data collection, processing and sharing, and household IPA security. This finding emphasizes the need for more diversified approaches toward household IPA concerns (Lutz and Newlands, 2021; Manikonda et al., 2017), as it confirms that these are not uniform.

Focus group results: Affordances and surveillance, security, and platform concerns

The focus group conversations highlight how household IPA concerns are embedded in broader repertoires of everyday technology use:

> "I have a smartphone, and I'm very keen on protecting my privacy. My location tracking is always disabled, I switched off WIFI completely, so that I cannot be followed, I'm very keen on that, and that's why I like to think about things like this…I tried to use Siri on the iPad, but it didn't feel comfortable to me…And no, I don't see myself using this [household IPA], I'm not very enthusiastic." (Jay, communication)

Jay’s quote shows how he wants to control the collection and access to his personal information, protecting his information privacy underpins his technology use. Supporting the survey results, Jay’s general privacy concerns and concerns around mobile privacy led to higher privacy concerns about household IPA use. His quote indicates that he does not want to be followed or tracked, yet the data collection and recording features of household IPAs afford platforms searchability and recordability (Lutz and Newlands, 2021). These affordances motivate Jay to refrain from using IPAs. In answer to RQ2, the focus groups indicate that other affordances also play a role in particular household IPA privacy concerns in the context of surveillance, security, and platforms.

Surveillance concerns around conversation and recordability affordances. Household IPAs can be controlled via voice-activation. This feature affords conversations with the devices. During the focus groups, the respondents tried out a Google Home and interacted with the device. Many of our respondents find this conversation affordance uncomfortable. Leah (organization support) states: “If it can respond and you can have a conversation, I would find that scary…I see myself alone in my apartment talking to a device, yeah, I don’t know, I find that weird.” Mona reflects on her family context: “I would not like to have this interaction in my family…I just don’t feel comfortable with saying a command and ask it to do something, it is just a thing.” While these experiences from potential household IPA users might be influenced by the novelty of this experience, these findings resonate with American non-users who also feel uncomfortable about this conversation affordance (Lau et al., 2018).

These uncomfortable feelings are interconnected with another affordance, namely, recordability (also described by Lutz and Newlands, 2021). For a household IPA to afford conversation, the device needs to record user requests which activate IPA responses or actions. It became clear that our respondents vary in their attitudes toward recordability, many do not trust the device to only listen when the trigger word is used. They are concerned that the devices are constantly “listening in” and recording conversations and environmental sounds, a finding that resonates with earlier research (Manikonda et al., 2017). These concerns were discussed in focus group 1:

> Jessica “Companies like Google and Apple will definitely save everything you (marketing): say to Siri or whoever, and not particularly to listen to each specific
>
> word, but to use all your commands to create a whole, a sort of, image of who you are and what your interests are. I find that very scary, and with something like this [household IPA], this only gets worse.”
>
> Interviewer: “Mm-hm, and are there particular things you deliberately don’t want to share with such a device?”
>
> Kim “Well, it is more that you suddenly have to pay attention to what you (PhD say. Because, yeah, you never know who’s listening…And then that candidate): raises the question: ‘Okay, I’m now having a private conversation, or whatever, and eh, do I want others to hear that?’ No, of course not!”

Whereas Kim feels that private conversations should not be listened to or recorded by household IPAs, Marcus (IT) does not deem living room conversations sensitive: “What would be hackable for these devices? Only that someone can listen in from a distance in your living room. Then I dare to state that most living room conversations are not interesting at all.” It becomes clear that respondents have different perceptions of the sensitivity of personal conversations in the intimate sphere of the home.

Respondents also have different perceptions of the consequences of the recordability affordance. Some respondents share pragmatic attitudes toward technology. For instance, Charlie (professor) believes that it is impossible to listen in on “all these Siri devices” because this would require too much data processing and manpower. Charlie perceives recordability as an affordance in a less concerned manner than most respondents because he deems it impossible that household IPAs are continuously recording. His perceptions resonate with previous research wherein American users stated that it would be impossible for companies to store and process all the data of continuously recording devices (Lau et al., 2018).

Household IPA use and its conversation and recordability affordances produces different concerns around communication privacy. Some regard the content of mediated interactions with the device and unmediated interactions around the device sensitive, while others are more pragmatic and do not perceive these as sensitive or deem it unlikely that all conversations and interactions can be recorded and processed. This shows that the situatedness of technology use determines how particular affordances are perceived (Evans et al., 2017; Humphreys et al., 2018).

Household IPA security concerns around locatability affordance. When it comes to concerns around household IPA security, prior research indicates that users and non-users are mainly concerned about the devices being hacked which leads to malware or cybersecurity breaches (Manikonda et al., 2017). In contrast, our respondents are more concerned about break-ins into their house. Unexpectedly, these concerns about break-ins came up in three out of six focus group discussions. For example, Peggy (education support) brought this up when the conversation addressed drawbacks of household IPA use: “If someone would hack this, they could easily see when you’re not at home, when there are no activities, and when you look at break-ins, I’m curious how people can deal with that.” In another focus group discussion, Bjorn (PhD candidate) shared similar concerns: “There will be a moment when these devices will be hacked. Without a doubt. And when that information comes out, you have, well then you can easily map when someone’s home and away. So that is very interesting information for burglars.” Furthermore, Linda (professor) shares that she does not feel comfortable with booking a hotel via a household IPA. She is afraid to share information with the device about when she plans to be away, and that this in turn allows others to ask the device “Hey Google, when will she return?” Linda is not concerned about her data being stolen; she is afraid that burglars will consult the device to find out when she is away. While existing research approaches security in the context of information privacy (Chandrasekaran et al., 2018; Furey and Blue, 2018; Lei et al., 2017; Manikonda et al., 2017), our respondents share concerns about their spatial and territorial privacy of their private space and intimate activities (Könings et al., 2010; Koops et al., 2016).

This is caused by how they perceive their devices to be connected to their homes and their personal space. The locatability affordance could enable hackers to locate users (and use patterns) within their intimate sphere. Moreover, respondents fear that hackers can infringe their spatial and territorial privacy by taking over their devices. Mark (education support) shares his fears: “They [hackers] can listen to your voice, but can also hear what happens in your home,” to which Hannah (education support) adds: “And switch on your microphone.” These concerns further highlight how our respondents’ privacy concerns in the context of security boil down to tangible threats that directly impact their intimate home contexts.

Platform concerns around control-ability and assistance affordances. The final type of household IPA privacy concern is characterized as more intangible because it regards data collection by platforms. As Babette (researcher/lecturer) describes: “I am concerned about privacy and everything that is stored of the things you do." Robert (IT department) voices similar concerns "I am critical towards new technologies when it comes to privacy, I am pretty concerned about what they all collect." More specifically, respondents are critical toward the use of the data that is stored about their activities and their conversations. Household IPAs collect data to afford control-ability (coined by Brause and Blank, 2020), they allow users to control other appliances, devices, and accounts via their household IPA. This technical affordance is embedded in platform ecosystems wherein user data is shared with third-party providers of smart appliances, services, and skills (Abdi et al., 2019). Echoing prior research (Huang et al., 2020; Malkin et al., 2019), our respondents indicate that their concerns are fueled by platforms' lack of transparency around data collection, processing, and sharing. For instance, Dennis states:

> "I'm really a privacy-watcher. And, before I investigated it, I will not activate a functionality…Maybe when I've looked into it, I'll know what type of data or information is being stored. But for me it's: If I've not looked into it, I will not use it. And for functionalities like these [household IPAs], it is hard to find out what exactly they do with [personal data]. Or how much you give away and how much control you have." (Dennis, IT department)

The affordance control-ability complicates data collection, processing, and sharing in an opaque manner. For many (potential) users, it remains unclear what data are shared with what other parties and what these parties in turn do with their data. This makes it difficult for users to protect their information privacy (Koops et al., 2016), and for some respondents like Dennis, a lack of transparency forms the reason for not using IPAs. Ironically, the affordance control-ability allows users to control their smart homes, yet it prevents them from controlling their information privacy.

A key concern that emerged from multiple focus groups is related to the affordance of assistance. Household IPA platform ecosystems afford users to activate a plethora of services to assist them. For example, they can provide data about their daily commute so that the device can suggest taking another route when there is a traffic jam. Or they can provide access to their email accounts and streaming services to receive notifications of new entertainment releases and flight changes for purchased tickets. Some respondents were afraid that their own actions and decisions will be affected by a household IPA that constantly assists them. Karen (professor) fears that she will become too dependent on the device: "You become dependent, I think, that concerns me, yes, that when you put this [household IPA] in your house, that you will not think about what is in agenda for tomorrow, but that you'll ask that thing." Similarly, Monica (communication) fears that she will rely too much on the device: "You know how your grammar might be degrading more because text prediction? I thought the same, with all these services that I would not want to become so reliant on it that I wouldn't know what to do if it disappeared from my life."

For these respondents, the assistance affordance can harm their intellectual privacy by influencing their decisions and routines (Koops et al., 2016). The fact that the risks that they foresee are related to their own behavior adds insights to privacy decisions specific for the use of household IPAs. Bjorn (PhD candidate) is particularly concerned that selections in notifications and information might be used to influence behavior: "I believe that you're unknowingly, or maybe even knowingly, part of a huge Google A/B test." Bjorn fears that data collection for assistance leads to the device not only influencing his behavior but also testing how he reacts to the suggestions and adapt these accordingly. This mirrors general concerns about how the embeddedness of voice-activated assistants in everyday life have the potential to change behavior and actions. In combination with the earlier mentioned recordability affordance, assistance can have a chilling effect by affecting how users behave in their private space. Karen, Monica, and Bjorn display awareness of data collection and about potential influences on their behavior. When such awareness makes them adopt particular behavior to avoid undesired actions being recorded by the device a chilling effect occurs (a practice also described by Büchi et al., 2020 in relation to algorithmic profiling). Moreover, existing research emphasizes the expectation that household IPA use can ultimately affect how our memory works (Atkinson and Barker, 2020).

Discussion

This mixed-method study presents an in-depth and differentiated account of privacy concerns around household IPAs. We provide insights about a continental European population on the cusp of normalizing such devices in the home. This sample is culturally distinctive from most other studies, and in this discussion, we provide insights in how Dutch respondents differ from populations studied in existing research (mainly US- and UK-oriented). Moreover, we reflect on the implications of our findings, in particular on how affordances amplify privacy concerns.

Our survey results show overlap in the factors influencing surveillance, security, and platform concerns, yet they also show where these concerns differentiate. First, the finding that general privacy and mobile privacy concerns lead to higher household IPA surveillance concerns across the board indicates that existing privacy concerns extend to novel technologies and potentially amplify them. In contrast, phone IPA use lowered all three types of concerns, which indicates that negotiations around privacy already resulted in phone IPA use and that using similar technologies might lower the threshold to household IPA adoption. However, surprisingly the survey results indicate that whereas IPA familiarity correlates with more concerns around security and platforms, this is not the case for concerns about surveillance itself. This suggests that familiarization lowers the more concerning or creepy associations of devices listening in as surveillance agents, but simultaneously sparks concerns about platforms and household IPA security. While the first two findings simply illustrate a trajectory—of already existing concerns (privacy) and acceptance of already existing devices (phone IPA use) increasing in relation to these devices—the last finding shows a more nuanced view. Platforms themselves are seen as a more important factor than the surveillance they may afford as is the security of the device more concerning than the surveillance it may afford.

The focus groups provide insights into the perceptions and experiences behind diversified privacy concerns and indicate how these are tied to particular affordances. Interestingly, most respondents focus more on immediate and physical risks and have a pragmatic perspective toward hypothetical and long-lasting risks. With regards to the latter, the focus group results show overlap between our Dutch respondents and existing research. Namely, US-based research indicates that concerns about recordability and listening in are dissuaded by pragmatic attitudes based on how impossible it is for platforms to store and process recordings of all devices all the time (Lau et al., 2018). This pragmatic perception was also shared by some of our respondents. Moreover, many respondents felt uncomfortable in interacting with the device (conversation affordance), resonating with research about non-users (Lau et al., 2018). This indicates that uncomfortable feelings can also motivate consumers to refrain from using household IPAs. For our respondents, some of these uncomfortable experiences might have to do with the novelty of household IPAs but also with the fact that it is not very common to be talking to devices in the the Netherlands. Mirroring the authors' personal assumptions, focus group respondents described that talking out loud to smartphones (without holding the phone to the ear) is mainly restricted to younger smartphone users and not (yet) a widespread practice.

The most striking finding of the focus groups substantiates the survey's security concerns as these prove to be connected to a locatability affordance. Whereas existing research indicates how UK and US (non-) users are concerned about security and fear for their information privacy (Lau et al., 2018; Manikonda et al., 2017), our respondents perceive insufficient or failing device security as a risk potentially leading to house break-ins. This is caused by household IPAs' interconnectedness with the personal home context, affording locatability as it might enable hackers to determine the physical location of users and their devices. Our respondents' concerns around device security are closely connected with spatial and territorial privacy (Könings et al., 2010; Koops et al., 2016) because these risks are perceived as threatening intimate home contexts. The physical and tangible nature of these threats seems unique for our respondents in light of existing research. This might be influenced by a more familial connection to local space in terms of expectations of openness (such as illustrated in social norms around open curtains in the the Netherlands, see Horst and Messing, 2006). This openness goes hand in hand with social control and the active safeguarding of neighborhoods (such as via popular WhatsApp neighborhood crime prevention groups—see Mols and Pridmore, 2019). Being more aware of physical safety concerns might cause people in the the Netherlands to perceive more tangible risks around household IPA devices.

Moreover, affordances in relation to platform concerns also reveal similarities and differences with existing research. The affordance control-ability (Brause and Blank, 2020) instigates concerns about a lack of transparency around data collection, processing and sharing, and resonating research among US and UK household IPA users (Huang et al., 2020; Malkin et al., 2019). Concerns that we have not seen to be reflected in existing research, revolve around household IPAs assistance affordance. This affordance initiates concerns around intellectual privacy (Koops et al., 2016) because respondents fear that the algorithmically driven suggestions and assistance of the device will influence their behavior and their decisions.

Limitations and directions for future research

While our study highlights important aspects of user privacy decisions and potential uses of household IPAs, it is based on a one-time survey and focus groups. Moreover, our research sample is limited to university employees and its results may not be generalizable to a wider Dutch population. University employees might have higher privacy concerns and awareness compared to a representative sample of Dutch citizens. While we aimed to increase the diversity in our sample by including both support staff and academic employees, future research should focus on a more representative sample. Moreover, our sample of potential users (and a few early adopters) did not allow for an exploration of privacy concerns around shared use and other household members, an aspect of household IPA use that can lead to power imbalance (e.g., see Geeng and Roesner, 2019; Huang et al., 2020; Lutz and Newlands, 2021).

Following Lutz and Newlands (2021) and Manikonda et al. (2017), our findings emphasize the need for more diversified approaches toward household IPA privacy concerns. They confirm that privacy concerns are not uniform but concern information, communicational, intellectual, spatial, and territorial privacy (Könings et al., 2010; Koops et al., 2016). Future explorations of the multidimensionality of privacy concerns around household IPAs or other smart home devices and services will bring insights into which aspects matter most to (potential) users. These insights can not only inform privacy awareness raising initiatives but can also indicate where gaps in privacy literacy reside (e.g., fears about physical threats to spatial privacy may indicate limited knowledge or awareness about identity theft and data breaches). Our focus groups also show how a qualitative approach to multidimensional privacy concerns allows for unexpected findings, such as the tangible nature of IPA security concerns we found. Therefore, more qualitative approaches to privacy concerns around IPAs and other technologies will provide more context and insights into motivations behind privacy attitudes.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: the Netherlands Organisation for Scientific Research (NWO) under the Privacy Research in Cyber Environment (PRICE) [Grant number 628.001.024].

ORCID iD

Anouk Mols https://orcid.org/0000-0003-0355-9849

Supplementary Material

Supplementary Material for this article is available online.

References

Abdi N, Ramokapane KM, and Such JM (2019) More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Fifteenth symposium on usable privacy and security {SOUPS} 2019. Available at: https://www.usenix.org/conference/soups2019/presentation/abdi (accessed 26 January 2021)

Atkinson P and Barker R (2020) ’Hey Alexa, what did I forget?’: networked devices, internet search and the delegation of human memory. *Convergence: The International Journal of Research into New Media Technologies* 27: 52–65. DOI: 10.1177/1354856520925740. Convergence Epub ahead of print 26 May 2020: 1–14

Bol N, Helberger N, and Weert JCM Van (2018) Differences in mobile health app use: a source of new digital inequalities?. *The Information Society* 34(3): 12. DOI: 10.1080/01972243.2018.1438550

Brause SR and Blank G (2020) Externalized domestication: smart speaker assistants, networks and domestication theory. *Information, Communication & Society* 23(5): 751–763. DOI: 10.1080/1369118X.2020.1713845

Bucher T and Helmond A (2017) The affordances of social media platforms. In: Burgess J, Poell T, and Marwick A (eds), *The SAGE Handbook of Social Media*. Los Angeles: SAGE, pp. 233–253.

Büchi M, Fosch-Villaronga E, Lutz C, et al. (2020) The chilling effects of algorithmic profiling: mapping the issues. *Computer Law & Security Review* 36: 105367. DOI: 10.1016/j.clsr.2019.105367

Chandrasekaran V, Fawaz K, Mutlu B, et al. (2018) *Characterizing Privacy Perceptions of Voice Assistants: A Technology Probe Study*. arXiv preprint:1812.00263 Preprint. Available at: https://deepai.org/publication/characterizing-privacy-perceptions-of-voice-assistants-a-technology-probe-study

Chang L and Mogg T (2018) Amazon offers a reason for Alexa’s ‘random,’ creepy laugh. *Digital Trends*, 8 March. Available at: https://www.digitaltrends.com/home/amazon-alexa-laugh/ (accessed 20 June 2019).

Charmaz K (2014) *Constructing Grounded Theory*. 2nd ed. Los Angeles: SAGE.

Cho E (2019) Hey Google, Can I Ask You Something in Private?. In: Proceedings of the 2019 CHI conference on human factors in computing systems, New York, NY, USA, 2 May 2019. Association for Computing Machinery, p. 1. DOI: 10.1145/3290605.3300488

Creswell JW and Plano Clark VL (2017) *Designing and Conducting Mixed Methods Research*. 3rd ed.. SAGE. Available at: http://us.sagepub.com/en-us/nam/designing-and-conducting-mixed-methods-research/book241842 (accessed 18 January 2021).

Evans SK, Pearce KE, Vitak J, et al. (2017) Explicating affordances: a conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication* 22(1): 35–52. DOI: 10.1111/jcc4.12180.

Fiesler C, Dye M, Feuston JL, et al (2017) What (or who) is public?. In: Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing, Portland Oregon USA, 25 February 2017. ACM, pp. 567–580. DOI: 10.1145/2998181.2998223

Furey E and Blue J (June 2018) She knows too much - voice command devices and privacy. In: 2018 29th Irish signals and systems conference (ISSC). Belfast, UK, 21–22 June 2018. IEEE, pp. 1–6. DOI: 10.1109/ISSC.2018.8585380

Fussel S (2020) Meet the star witness: your smart speaker. *Wired*, 23 August. Available at: https://www.wired.com/story/star-witness-your-smart-speaker/ (accessed 4 February 2021).

Geeng C and Roesner F (2019) Who's In control? Interactions In multi-user smart homes. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. doi: 10.1145/3290605.3300498.

Gibson J (2014) Junkspace (2002). In: Gieseking JJ, Mangold W, Katz C, et al. (eds), *The People, Place, and Space Reader*. New York: Routledge, pp. 56–60.

Hargittai E and Hsieh YP (2012) Succinct survey measures of web-use skills. *Social Science Computer Review* 30(1): 95–107. DOI: 10.1177/0894439310397146

Helmond A (2015) The platformization of the web: making web data platform ready. *Social Media + Society* 1: 205630511560308. DOI: 10.1177/2056305115603080. Social Media + Society Epub ahead of print: 1–11.

Horcher G (2018) Woman says her amazon device recorded private conversation, sent it out to random contact. *KIRO7*, 25 May. Available at: https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974 (accessed 20 June 2019).

Van Der Horst H and Messing J (2006) "It's not dutch to close the curtains": visual struggles on the threshold between public and private in a multi-ethnic Dutch neighborhood. *Home Cultures* 3(1): 21–37. DOI: 10.2752/174063106778053264

Huang Y, Obada-Obieh B, Beznosov K, et al. (2020) Amazon vs. My brother: How users of shared smart speakers perceive and cope with privacy risks. In: Proceedings of the 2020 CHI conference on human factors in computing systems, New York, NY, USA, 21 April 2020. Association for Computing Machinery, pp. 1–13. DOI: 10.1145/3313831.3376529. (accessed 26 January 2021).

Humphreys L, Karnowski V, and Pape T von (2018) Smartphones as metamedia: A framework for identifying the niches structuring smartphone use. *International Journal of Communication* 12: 2793–2809.

Kinsella B (2020) Amazon smart speaker market share falls to 53% in 2019 with google the biggest beneficiary rising to 31%, sonos also moves up. *Voicebot.ai*, 28 April. Available at: https://voicebot.ai/2020/04/28/amazon-smart-speaker-market-share-falls-to-53-in-2019-with-google-the-biggest-beneficiary-rising-to-31-sonos-also-moves-up/ (accessed 14 July 2020).

Kinsella B and Mutchler A (2019) *Smart Speaker Consumer Adoption Report March 2019*. U.S. March. Voiebot.ai. Available at: https://voicebot.ai/wp-content/uploads/2019/03/smart_speaker_consumer_adoption_report_2019.pdf.

Könings B, Schaub F, Weber M, et al. (2010) Towards territorial privacy in smart environments. In: AAAI 2010 spring symposium, Stanford, CA, USA, 2 June 2010. Universität Ulm. DOI: 10.18725/OPARU-1727

Koops B-J, Newell BC, Timan T, et al. (2016) A typology of privacy. *University of Pennsylvania Journal of International Law* 38(2): 483–576.

Lau J, Zimmerman B, and Schaub F (2018) Alexa, are you listening?. *Proceedings of the ACM on Human-Computer Interaction* 2(CSCW): 1–31. DOI: 10.1145/3274371.

Lei X, Tu G-H, Liu AX, et al. (2017) *The Insecurity of Home Digital Voice Assistants - Amazon Alexa as a Case Study. arXiv:1712.03327 [cs]* Preprint. Available at: http://arxiv.org/abs/1712.03327 (accessed 31 May 2019).

Liao Y, Vitak J, Kumar P, et al. (2019) Understanding the role of privacy and trust in intelligent personal assistant adoption. In: Information in contemporary society. iConference 2019. Lecture notes in computer science, Washington, DC, USA, 31 March–3 April, 2019. Cham: Springer, pp. 102–113. Available at: https://link.springer.com/chapter/10.1007/978-3-030-15742-5_9

Lutz C and Newlands G (2021) Privacy and smart speakers: a multi-dimensional approach. *The Information Society* 37(2): 147–162. DOI: 10.1080/01972243.2021.1897914.

Malkin N, Deatrick J, Tong A, et al. (2019) Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019(4): 250–271. DOI: 10.2478/popets-2019-0068

Manikonda L, Deotale A, and Kambhampati S (2017) *What's up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants*. arXiv:1711.07543 [cs] Preprint. Available at: http://arxiv.org/abs/1711.07543 (accessed 29 January 2021).

McLean G and Osei-Frimpong K (2019) Hey Alexa … examine the variables influencing the use of artificial intelligent in-home voice assistants examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior* 99: 28–37. DOI: 10.1016/j.chb.2019.05.009

McNair C (2019) Global smart speaker users 2019. *eMarketer*. Available at: https://www.emarketer.com/content/global-smart-speaker-users-2019 (accessed 31 May 2019).

Mols A and Pridmore J (2019) When citizens are "actually doing police work": The blurring of boundaries in Whatsapp neighbourhood crime prevention groups in the the Netherlands. *Surveillance & Society* 17(3/4): 272–287. DOI: 10.24908/ss.v17i3/4.8664

Mulligan DK, Koopman C, and Doty N (2016) Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374(2083): 20160118. DOI: 10.1098/rsta.2016.0118.

Multiscope (2019) Slimme speakers in half miljoen huishoudens. Available at: http://www.multiscope.nl/persberichten/slimme-speakers-in-half-miljoen-huishoudens.html (accessed 31 May 2019).

Multiscope (2020) Slimme speaker verovert huiskamer consument. Available at: http://www.multiscope.nl/persberichten/slimme-speaker-verovert-huiskamer-consument/ (accessed 9 July 2020).

Nagy P and Neff G (2015) Imagined affordance: reconstructing a keyword for communication theory. *Social Media + Society* 1(2): 205630511560338. DOI: 10.1177/2056305115603385. SAGE Publications Ltd.

Peek of the Net (2017) Google home official Ad. Available at: https://www.youtube.com/watch?v=OsXedJq1aWE&t=2s (accessed 31 May 2019).

Perez S (2019) Report: smart speaker adoption in US reaches 66M units, with Amazon leading. *TechCrunch*. Available at: http://social.techcrunch.com/2019/02/05/report-smart-speaker-adoption-in-u-s-reaches-66m-units-with-amazon-leading/ (accessed 31 May 2019).

Pridmore J and Mols A (2020) Personal choices and situated data: privacy negotiations and the acceptance of household intelligent personal assistants. *Big Data & Society* 7: 205395171989174. Big Data & Society Epub available ahead of print: 1–12. DOI: 10.1177/2053951719891748

Pridmore J, Zimmer M, Vitak J, et al. (2019) Intelligent personal assistants and the intercultural negotiations of dataveillance in platformed households. *Surveillance & Society* 17(1/2): 125–131. DOI: 10.24908/ss.v17i1/2.12936

Nieuws RTL (2018). Creepy: Amazon-speakers lachen je onverwacht uit. 8 March. Available at: https://www.rtlnieuws.nl/tech/artikel/3914526/creepy-amazon-speakers-lachen-je-onverwacht-uit (accessed 8 February 2021).

Russakovskii A (2017) Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7Android Police. Available at: https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/ (accessed 20 June 2019).

Stewart D, Shamdasani P, and Rook D (2007) *Focus Groups*. Los Angeles: SAGE. DOI: 10.4135/9781412991841

van Prooijen A-M, Ranzini G, and Bartels J (2018) Exposing one's identity: Social judgments of colleagues' traits can influence employees' Facebook boundary management. *Computers in Human Behavior* 78: 215–222. DOI: 10.1016/j.chb.2017.10.002

Vitak J (2015) Balancing privacy concerns and impression management strategies on Facebook. In: Symposium on usable privacy and security (SOUPS), College Park, MD, 2015. Ottawa: Canada. Available at: https://cups.cs.cmu.edu/soups/2015/papers/ppsVitak.pdf

Vitak J (2016) A digital path to happiness? Applying communication privacy management theory to mediated interactions. In: Reinecke L and Oliver MB (eds), *The Routledge Handbook of Media Use and Well-Being*. New York: Routledge, pp. 247–287.

Vitak J, Liao Y, Kumar P, et al. (2018) Privacy attitudes and data valuation among fitness tracker users. In: Chowdhury G, McLeod J, Gillet V, et al. (eds), *Transforming Digital Worlds: iConference 2018*. Cham: Springer International Publishing, pp. 229–239. DOI: 10.1007/978-3-319-78105-1_27

Xu H, Gupta S, Rosson M, et al. (2012) Measuring mobile users' concerns for information privacy. In: Proceedings of the international conference on information systems 2012 on digital innovation in the service economy, Orlando, FL, USA, 16–19 December 2012, pp. 1–16. Available at: http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10

Zimmer M, Kumar P, Vitak J, et al. (2020) 'There's nothing really they can do with this information': unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society* 23(7): 1020–1037. DOI: 10.1080/1369118X.2018.1543442

Author biographies

Anouk Mols is a PhD candidate at the Department of Media & Communication of the Erasmus University Rotterdam. She is currently involved in the 'Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems' project and her research revolves around everyday privacy and surveillance practices in the context of local communities, workplaces, messaging apps, and families. She is particularly interested in public safety, participatory policing, parental monitoring, digital interactions, artificial intelligence, and smart technologies.

Yijing Wang is an organizational communication scholar specialized in the study of corporate social responsibility, crisis communication and reputation management. She is particularly interested in the dynamic interplay of organizations, media, and publics in urgent sustainability transitions. She is Assistant Professor and Chair of the Professional Advisory Committee in the Department of Media and Communication at Erasmus University Rotterdam. Yijing serves as Associate Editor of the Corporate Reputation Review, Editorial Board Member of the Business Horizons, Guest Editor of the Public Relations Review and the International Journal of Communication. She has published in leading field journals such as Journal of Business Ethics, Journal of International Management, Business Horizons, among others.

Jason Pridmore is the Vice Dean of Education at the Erasmus School of History, Culture and Communication and an Associate Professor in the Department of Media and Communication at Erasmus University Rotterdam. His research interests focus on practices of digital identification, the use of new/social media and consumer data as surveillance practices, and digital (cyber) security issues. He coordinates and participates in a number of international research projects focused on privacy, data ethics, surveillance, AI, IoT, and (cyber) security in differing socio-technical contexts.