5-15-2019

PROPOSING AN EXTENSION OF THE PRIVACY CALCULUS TO REFLECT THE IMPLICATIONS OF SPEECH-DISCLOSURE

Jakob Wirth
University of Bamberg, jakob.wirth@uni-bamberg.de

Christian Maier
University of Bamberg, christian.maier@uni-bamberg.de

PRIVACY AND SPEECH-DISCLOSURE: AN EXTENSION OF THE PRIVACY CALCULUS

Short paper

Wirth, Jakob, University of Bamberg, Germany, jakob.wirth@uni-bamberg.de

Maier, Christian, University of Bamberg, Germany, christian.maier@uni-bamberg.de

Abstract

Besides disclosing information via keyboard, disclosing information via speech is on the rise, for example, when speaking with digital assistants such as Amazon Echo. However, when disclosing information via speech, additional information is disclosed such as volume, pitch, tone or accent. With this additional information, further information of the individual can be derived such as age, gender or race. Also, other individuals around can overhear the spoken information. Both may lead to additional privacy risks. However, previous research has mainly considered the privacy risks through disclosure via keyboard, neglecting the mentioned additional privacy risks through disclosure via speech. Therefore, to better understand disclosure via speech, we rely on the basic privacy calculus, yet extend it with further privacy risks through additional information and through other individuals around. We propose a quantitative survey, to shed light on the effect of the additional privacy risks on speech-disclosure and aim to contribute to theory by recommending scholars to include the additional privacy risks when researching on speech-disclosure.

Keywords: Voice, Speech-disclosure, Chatbot, Digital assistant.

1 Introduction

When individuals disclose their personal information, their privacy is at risk (Solove 2006, 2011). This results in disadvantages for the individual including identity theft, price discrimination or chilling effects (Dinev 2014). Typically, individuals disclose information online when using their keyboard and typing text, e.g. while searching on Google or buying products on Amazon. Alternatively, disclosure can also happen through speaking with an information system (IS). For example, individuals speak to digital assistants, such as the Google Assistant (Google 2018) or Amazon Echo (Amazon 2018) or send voice messages over messaging services such as WhatsApp. Since speaking is more natural than typing (Akila and Ganesh 2012), speech-disclosure is on the rise (Forbes 2018). Estimates are made that, in 2020, 50 percent of all searches will be conducted via speech which is twice as much as 2016 (campaign 2016).

However, compared to disclosing information via keyboard, speech-disclosure differs in two main aspects. One, an individual discloses additional information, such as accent, pitch or volume of the spoken words (Akila and Ganesh 2012). That means that receivers of the information can infer further information about the individual, such as mood (Mencattini et al. 2014), age, gender, race or weight of the individual (Krauss et al. 2002; Pisanski et al. 2014a; Pisanski et al. 2014b). Two, others standing next to the individual might potentially overhear the spoken words (Easwara and Vu 2015). For example, an individual is speaking to a digital assistant on a smartphone in a crowded train. Through this, not only the intended receiver of the spoken words but also other, unintended receivers, will overhear the spoken words (Petronio and Altman 2002).

Both differences can lead to additional privacy risks (Moorthy and Vu 2015; Singh et al. 2016). Privacy risks in general are one of the major determinants inhibiting disclosure of information (Dinev and Hart 2006). Therefore, to better understand speech-disclosure one needs to research on in how far potential additional privacy risks through speech-disclosure influence speech-disclosure. With this study, we aim to research on that issue, by posing the following research question:

In how far do additional privacy risks determine an individuals' disclosure via speech?

We rely on the privacy calculus (Smith et al. 2011), stating that individuals weigh benefits of disclosure with privacy risks of disclosure. While the privacy calculus has rather been used when individuals disclose information via keyboard and not via speech, additional privacy risks relevant for speech-disclosure are neglected. So, we extend the privacy calculus with information from previous research regarding speech-disclosure.

2 Theoretical Background

In the following, we provide information on the privacy calculus and on speech-disclosure. We then carve out the research gap, and theorize on additional privacy risks through speech-disclosure.

2.1 The Privacy Calculus

Privacy is defined as having the control over ones' personal information (Bélanger and Crossler 2011). Disclosing information leads to potentially losing control whereas disclosure is defined as revealing actual personal information to the receiver (Wakefield 2013) which can be an organization or an individual. Thereby, the *intention to disclose* covers the motivation of an individual to reveal actual personal information (Dinev and Hart 2006). To explain the intention to disclose, the privacy calculus is one of the most used theories (Dinev and Hart 2006; Smith et al. 2011). Although it has been shown that the privacy calculus does not always hold true (Dinev et al. 2015; Kehr et al. 2013), it is still an applicable theory in the privacy context to explain the disclosure of information (Smith et al. 2011).

The privacy calculus includes on the one hand *benefits of disclosure*. They represent all positive outcomes of disclosure (Dinev and Hart 2006), including perceived usefulness or perceived enjoyment (Krasnova et al. 2012; Lin and Lu 2011; Wakefield 2013). On the other hand, disclosure of information refers to risks to ones' privacy which is defined as "*Perceived risk of opportunistic behavior related to the disclosure of personal information*" (Dinev and Hart 2006, p. 64). Such a definition might already include additional risks that are inferred through speech-disclosure. However, the privacy calculus has only been used, when information is disclosed via keyboard. Also, other studies define privacy risks as the degree to which an individual believes that releasing *actual* personal information to the intended receiver is associated with a high potential for loss (Smith et al. 2011). We therefore assume that previous privacy research has mainly focused on privacy risks of actual information against the receiver and has not focused on additional privacy risks through speech-disclosure. Therefore, we call this concept *privacy risks of actual information against the receiver*.

If benefits outweigh privacy risks of actual information against the receiver, then maximization of positive outcomes is fulfilled, and individuals are more likely to disclose information (van Eerde and Thierry 1996). So far, the privacy calculus has only been used to study disclosure via keyboard, while information can also be disclosed via speech, e.g. when using digital assistants.

2.2 Speech-Disclosure

Speaking is a process that can be divided up into five steps (Indefrey and Levelt 2004): Step 1) *Preparation*: The individual is conceptually preparing what to say. Step 2) *Selection*: The individual relies on her own lexicon in her mind to select appropriate words. Step 3) *Grammatical encoding*: The individual grammatically encodes the words using a particular syntax. For example, the individual puts the words into a particular order. Step 4) *Phonetic encoding*: The individual sets up how to speak the word out loud, by accessing her own phonological code. Step 5) *Articulating*: The process is finalized by actually articulating the word using vocal cords such that the spoken word is said out loud. This all comes so naturally, that we do not even realize, how complex speaking actually is (Akila and Ganesh 2012).

In comparison, keyboard-disclosure is identical in preparation (step 1), selection (step 2) and grammatical encoding (step 3). However, in steps 4 and 5, speech-disclosure is different to keyboard-disclosure. As shown in the subsequent sections, these differences can lead to additional privacy risks, altering the privacy calculus. In particular, through the phonetic encoding (step 4) and especially through articulating (step 5), speech-disclosure is different than disclosing information via keyboard. Thereby, the human

vocal tract and articulators are biological organs with nonlinear properties. These are not under conscious control and therefore, additional information is transmitted through speech, other than through keyboard. To find out, in how far previous research has already considered this, we conducted a literature review on speech-disclosure in the domain of privacy.

2.3 Previous Research on Speech-Disclosure in the Domain of Privacy

We conducted a literature review on disclosure via speech in the domain of privacy[1]. Five articles were identified. A summary is given in Table 1. In particular, the literature review reveals two insights.

One, research on speech-disclosure is rather scarce and several empirical studies have yet to be conducted (see Table 1). Besides, the article of Han and Yang (2018) have already presented empirical results, but do not go deeper into determinants of speech-disclosure. The study by Moorthy and Vu (2015) is more about usage, which is conceptually different to disclosure (Brakemeier et al. 2016). While usage is more about the functionalities of the technology and how to employ them, disclosure is more about the actual act of revealing information, so that we do not know determinants of speech-disclosure.

Two, although research on that topic is rather scarce, one concept has been suggested that is important in the context of speech-disclosure: the environment of individuals determines, whether other individuals around can potentially overhear information that is spoken or not (Moorthy and Vu 2015). In case individuals disclose information via speech, other individuals around can potentially overhear that information, e.g., when being on a crowded train or standing in line in a supermarket. In case individuals are alone at home, then there is no other individual who is potentially overhearing the information.

Major findings	**Major drawbacks**	**Reference**
Influence of risk, trust and privacy by home assistants.	No conduction of the research, yet.	Crossler et al. 2018
Social relationships with intelligent personal assistants via voice and subsequent satisfaction of individuals.	No presentation of determinants of speech-disclosure.	Han and Yang 2018
Consumer insights on voice-activated personal assistants.	No conduction of the research, yet.	Mallat et al. 2017
Usage of voice-based devices.	Mainly about usage and not about disclosure which is conceptually different.	Moorthy and Vu 2015
Reciprocal self-disclosure, trust and privacy risks when using voice-based devices.	No conduction of the research, yet.	Saffarizadeh et al. 2017

Table 1. Literature review[1] on speech-disclosure in the domain of privacy

To put it in a nutshell, two main issues arise in the context of speech-disclosure: First, we know that additional information is disclosed when information is spoken out loud because of the phonetic encoding and articulating. Second, the environment, i.e. if other individuals are around who can potentially overhear information, is important when disclosing information via speech.

2.4 Additional Privacy Risks Through Speech-Disclosure

Respecting research on speaking in general (Singh et al. 2016) and on speaking in the domain of privacy (Moorthy and Vu 2015), two main issues have been identified: On the one hand, additional information that is disclosed through speaking. On the other hand, the environment, when other individuals are around who potentially overhear the spoken information. So, next to the *privacy risks of actual information against the receiver*, when disclosing information via keyboard, three further privacy risks arise:

One, *privacy risks of additional information against the receiver*. Individuals disclose information to a particular receiver (Petronio and Altman 2002). For example, an individual is speaking to a digital assistant which is the actual receiver. Considering the process of speaking, the phonetic encoding as well as articulating the spoken words lead to disclosing additional information. That additional information

[1] We searched in the entire AIS eLibrary as well as the entire EBSCO Business Host by using privacy and voice or privacy and speech as our keywords. Articles, which did not deal with privacy risks in relation to voice were excluded.

relates to accent, pronunciation, articulation, roughness, nasality, pitch, volume, and speed (Akila and Ganesh 2012). Through such additional information, an IS as the receiver, can infer different characteristics of the individual and its surroundings. For example, bio descriptive characteristics such as age, gender, race or weight (Krauss et al. 2002; Lee et al. 2013; Pisanski et al. 2014a; Pisanski et al. 2014b); the current mood of the individual (Mencattini et al. 2014) or information about the environment one is, e.g. what size the room has one is in, or if one is not even inside but outside of a building (Singh et al. 2016). With all such additional information, one could among others even identify or verify a speaker where the average correct identification rate is at about 80 percent (Mendes and Ferreira 2012). This can then lead to additional privacy risks. For example, one might not be anonymous anymore although she thinks she is actually. Or, although not being perfectly accurate yet (Souza and Santos 2018), insurance companies could use the voice to find out if one is overweight and raise prices for insurance.

Two, *privacy risks of actual information against others around*. When disclosing information via speech, others standing around, might potentially overhear the spoken words (Moorthy and Vu 2015). Thereby, these other individuals standing around, can evaluate the actual information that is disclosed. Through this, privacy risks can occur. For example, an individual is conducting payment transactions via speech on a crowded train. A potential thief standing by, overhearing that information, might conclude that the individual is rich, and select him as a potential target for robbery.

Three, *privacy risks of additional information against others around*. When disclosing information via speech, others around might not only overhear the actual information but also additional information. This additional information relates among others to accent, pronunciation, articulation, roughness, nasality, pitch, volume, and speed (Akila and Ganesh 2012). Others around can overhear that information and come to different conclusions which might in turn lead to privacy risks. For example, an individual is speaking to an IS. Others might overhear that this individual has a foreign accent. They could then mistakenly conclude that this individual is more criminal because she is a foreigner.

3 Research Model

We use the privacy calculus (grey shaded, see Figure 1) as our basis. In addition, we include the three identified additional privacy risks when disclosing information via speech (black shaded, see Figure 1). In the following, the hypotheses are crafted.

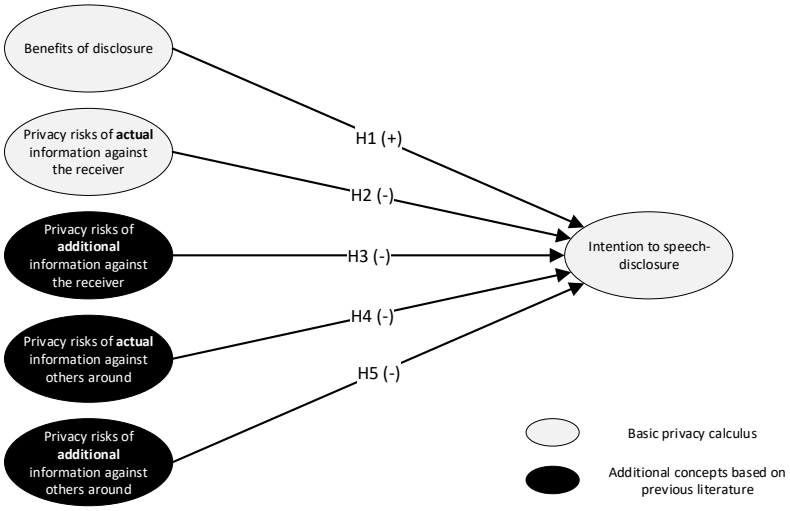

Figure 1. Research model

Benefits of disclosure: This concept is based on the privacy calculus and depicts all benefits that individuals receive when they disclose actual information (Dinev and Hart 2006). Examples refer to fun or perceived usefulness (Krasnova et al. 2012; Lin and Lu 2011; Wakefield 2013). Individuals try to maximize their benefits and try to minimize their disadvantages (van Eerde and Thierry 1996). Disclosing

information via speech can bring several benefits such as personalized services or fun. In line with previous research (Sun et al. 2015), we therefore hypothesize:

H1: The higher the benefits of disclosure, the higher the intention to speech-disclosure.

Privacy risk of actual information against the receiver: The privacy calculus states that individuals face certain risks when disclosing actual information. Thereby, the basic privacy calculus concentrates on the risks of the *actual* information disclosed (Brakemeier et al. 2016; Smith et al. 2011), i.e. the actual content of the spoken words. This content can lead to actual privacy risks. For example, an individual disclosing its birthday and credit card number via speech to an organization who is the receiver, might suffer from opportunistic behavior of that receiver. As individuals try to minimize negative outcomes (van Eerde and Thierry 1996) we hypothesize:

H2: The higher the privacy risks of actual information against the receiver, the lower the intention to speech-disclosure.

Privacy risks of additional information against the receiver: Besides the actual information that is disclosed via speech, also additional information is disclosed. This relates to accent, pronunciation, articulation, roughness, nasality, pitch, volume, and speed (Akila and Ganesh 2012). Through that additional information, one can infer even further information about the individual. such as age, gender, race or weight (Krauss et al. 2002; Pisanski et al. 2014a; Pisanski et al. 2014b). Such further information depicts a privacy risk to the individual who is disclosing the information. For example, an organization could create a voiceprint of the individual to verify and identify the individual (Mendes and Ferreira 2012). Individuals, disclosing information to a digital assistant, could then not be anonymous anymore. Since individuals want to avoid any negative outcomes (van Eerde and Thierry 1996), we hypothesize:

H3: The higher the privacy risks of additional information against the receiver, the lower the intention to speech-disclosure.

Privacy risks of actual information against others around: When disclosing the information to the actual receiver, also other individuals standing around might overhear the spoken words (John et al. 2011; Petronio and Altman 2002). Previous research has researched on that setting and suggested that individuals consider sharing information to social groups differently (Dey et al. 2005). Thus, they also consider sharing with the actual receiver and other individuals standing around differently. Therefore, individuals also consider the privacy risks, resulting from individuals standing by who overhear the actual information, differently. For example, individuals standing around, overhear that an individual is disclosing its e-mail address and telephone number via speech. That information could be used inappropriately by these individuals, e.g. by misusing when registering for particular services. Here, privacy risks against the actual receiver might be low, but privacy risks against others around might be high. Since individuals want to avoid these negative outcomes (van Eerde and Thierry 1996), we hypothesize the following:

H4: The higher the privacy risks of actual information against others around, the lower the intention to speech-disclosure.

Privacy risks of additional information against others around: The same should apply for additional information. Individuals can evaluate other individuals' speech, e.g. by their accent, speed or pitch (Akila and Ganesh 2012). This makes it possible for individuals – similar to IS – to derive further information about these other individuals. For example, if one is speaking to an IS very quietly, others might infer that the disclosed information could be very sensitive and might even put more energy into overhearing the information (Moorthy and Vu 2015). Again, since individuals want to avoid any negative consequences that could result out of such overheard disclosure, we hypothesize:

H5: The higher the privacy risks of additional information against others around, the lower the intention to speech-disclosure.

To evaluate the hypotheses, we aim to conduct a quantitative study, which is described in the following.

4 Methodology

Since this is a short paper, no data has been collected, yet, to examine the research model. However, we aim to gather data, using standardized items from previous research, by conducting a positivist study. The items will be slightly adapted to the context of speech-disclosure as follows: 1) At the beginning of the survey, participants will be told that this survey is about speech-disclosure to a service-provider. Such a service provider could e.g. be a digital assistant such as Google Home or Amazon Echo. This service provider will serve as the actual receiver. 2) To evaluate all four privacy risks constructs, we will use well-established items (Xu et al. 2009), which will be adapted to the particular privacy risk construct. An exemplary item of privacy risks of actual information against the receiver would be *It would be risky to disclose my personal information via speech to the service provider*. 3) To also include privacy risks of additional information, that term will be explained by stating that when disclosing information via speech, additional information such as accent, pitch and volume is disclosed which can then lead to further privacy risks. An exemplary item of privacy risks of additional information against the receiver is *It would be risky if such additional information about my voice was disclosed to the service provider*. 4) To also account for privacy risks of actual and additional information against others around, we will also adapt the items accordingly. An exemplary item of privacy risks of actual information against others around would be *It would be risky that others around could overhear me providing personal information via speech to the service provider*. To make sure that the items will depict the correct concept, we will conduct a small pilot-test before conducting the actual survey.

Further items include perceived usefulness as well as perceived enjoyment to operationalize benefits of disclosure (Sun et al. 2015). Intention to speech-disclosure will be based on items from Xu et al. (2009). Furthermore, we will control for the environment the individual is in. We will do so, by asking, in how far the individual is more likely to disclose information via speech in a more private environment where he is alone without any other individuals. Or, in a more public environment where many unknown others around can potentially overhear the information. Based on this control variable, we aim to better understand the effect of both privacy risks concepts against others around.

Besides, we will also control for the sensitivity of information (Mothersbaugh et al. 2011; Wirth et al. forthcoming) to exclude effects that are solely based on this concept. Furthermore, we will also control for individuals' fear that a microphone in their device such as smartphone or digital assistant will always be switched on (Johnston and Warkentin 2010). In addition, we will ask for age, gender and country of residence. Furthermore, we will control for the western privacy index, which groups individuals into five different groups based on their general information seeking behavior (Morton and Sasse 2014).

The order of the survey will be set up as follows: we first ask demographic questions as well as control variables. We then continue with asking for benefits of disclosure as well as privacy risks of actual information against the receiver and privacy risks of additional information against the receiver. We then ask the three remaining concepts which are privacy risks of actual information against others around, privacy risks of additional information against others around, and intention to speech-disclosure.

To conduct the survey, we will rely on participants from two different sources. On the one hand, participants of earlier scientific surveys were asked at the point of time of that earlier studies if they were interested to participate in any future surveys. All individuals who did so, represent the first part of individuals. On the other hand, every year we conduct a survey in association with a project partner about working conditions. Based on that survey, we will ask all participants if they want to participate in any future studies. Participants who affirm this question, represent the second part of individuals. Based on these surveys, we expect the gender of the participants to be equally distributed and the majority of the participants will be between 18 and 35 years old. All in all, this pool represents about 1,500 participants which has already brought up valid results in previous studies (Maier et al. 2014). We will then put up the survey online on our own server, using Limesurvey and then send the link to the survey via e-mail to the participants. To incentivize participation, we will also raffle prices among the participants. If our hypotheses will be supported, we aim to contribute to theory and practice.

5 Anticipated Contributions and Next Steps

Disclosure can lead to reduced privacy of individuals which in turn might result in disadvantages for the individuals (Dinev 2014). Finding out, what leads to disclosure, is therefore one of the main concerns of privacy research (Smith et al. 2011). Besides disclosing information via keyboard, speech-disclosure is on the rise (Forbes 2018). Through speech-disclosure, three additional privacy risks emerge. In this study, based on the privacy calculus, we aim to research how these influence the intention to speech-disclosure, to contribute to theory and practice.

Based on Whetten (1989), a good theoretical contribution should include three essential elements: 1) What factors should be included, 2) how these factors are related and 3) why they are related. In case our hypotheses are supported, we include these three elements: 1) We show that five concepts, namely benefits of disclosure as well as four different privacy risks concepts should be included when trying to understand speech-disclosure. 2) We show the relationship which is direct positive for benefits of disclosure and direct negative for all four privacy risks concepts. 3) Rationales are that individuals try to minimize negative outcomes and to maximize positive outcomes (van Eerde and Thierry 1996). Particular implications of this study are given in the following:

The general tenets proposed by the privacy calculus is relevant for speech-disclosure*:* The privacy calculus has mainly researched in the context of keyboard-disclosure. This depicts an issue since theories also need to be investigated in different contexts (Hong et al. 2014). With our research study, we contribute by using the basic concepts of the privacy calculus – benefits and privacy risks – to study speech-disclosure. With this, we contribute to current research such that scholars who want to research on speech-disclosure, can also rely on the basic premises of the privacy calculus.

To fully understand speech-disclosure, the privacy calculus needs to be adapted: The basic premises of the privacy calculus also hold true in the context of speech-disclosure. However, there are several determinants that do not play a role in the context of keyboard-disclosure but become important in the context of speech-disclosure. In particular, we ask scholars to consider the following two issues:

a) *Considering additional information*: Previous research on speech-recognition has emphasized that besides the actual content of speech also additional information can be derived. Such additional information relates e.g. to accent, pitch or volume of the spoken words (Akila and Ganesh 2012). It can then be used to derive further information about the individual such as bio descriptive parameters (Krauss et al. 2002; Pisanski et al. 2014a; Pisanski et al. 2014b), leading to further privacy risks. These privacy risks inhibit the disclosure of information via speech. Therefore, in contexts, where individuals might have the perception that additional information is evaluated by disclosing information via speech, scholars might want to include that concept into their research studies. Furthermore, scholars should not exclude that concept just because additional information is not evaluated. The perceptions might still be different. Then, privacy risks of additional information might still be an important factor determining speech-disclosure.

b) *Considering other individuals around*: Compared to keyboard-disclosure, other individuals around potentially overhear information that is disclosed via speech (Moorthy and Vu 2015). This can either be the actual information or can also be additional information. Independent of that, it has a negative effect on speech-disclosure because individuals try to avoid negative outcomes (van Eerde and Thierry 1996). Scholars who research on speech-disclosure should therefore also display in how far they have considered such individuals around in their research setting. In case other individuals are around, they should not neglect privacy risks against other individuals around (Moorthy and Vu 2015).

Practice might emphasize to not evaluate additional information: To avoid decreased disclosure, organizations who provide disclosure via speech, might want to advertise with not collecting and evaluating additional information from speech. Then the perception of risks related to the evaluation of additional information might be decreased, leading to more information disclosed via speech.

Digital assistants should also be useable when disclosing information via keyboard: Organizations, which provide disclosure via speech, especially when individuals are not at home, might want to make

sure that disclosure is also possible via keyboard. Then, individuals can also disclose their information when they are on the road, without having to fear any additional privacy risks from other individuals around, which could limit their speech-disclosure.

As this is a research in progress, the next steps are well planned but not finished yet. First, we will set up the survey. Second, we will conduct the actual empirical study. The acquisition of the participants and the conduction of the survey is described in the methodology section. Third, we will then evaluate the research model, by conducting a structural equation modeling approach. With this we will also be able to show the effect sizes of each concept on the outcome variable to then also better show in how far the additional concepts are useful to explain speech-disclosure. Here, we will also conduct standard procedures for validating the measurement model, e.g. by accounting for validity and reliability of the measurements.

In sum, disclosure via speech is on the rise (campaign 2016), yet, additional privacy risks then emerge. We therefore have created a research model that investigates the effect of these additional privacy risks on speech-disclosure. We aim to reveal, that among others, privacy risks through additional information that can be extracted from speech-disclosure, is an important factor explaining speech-disclosure.

References

Akila, A., and Ganesh, A. 2012. "An Overview of Speech Recognition and Speech Synthesis Algorithms," *Int.J.Computer Technology & Applications* (3:4), pp. 1426–1430.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.

Brakemeier, H., Widjaja, T., and Peter Buxmann 2016. "Distinguishing usage and disclosure intentions in privacy research: How our two selves bring about differences in the effects of benefits and risks," *Research Papers* .

campaign 2016. *Just say it: The future of search is voice and personal digital assistants*. https://www.campaignlive.co.uk/article/just-say-it-future-search-voice-personal-digital-assistants/1392459. Accessed 20 November 2018.

Crossler, R. E., Belanger, F., and Choo, K.-K. R. 2018. "Intelligent Home Assistant Use in the Home Environment," *AMCIS 2018 Proceedings* .

Dey, A., Kokinov, B., Leake, D., Turner, R., Khalil, A., and Connelly, K. (eds.) 2005. *Context-Aware Configuration: A Study on Improving Cell Phone Awareness*: *Modeling and Using Context*, Berlin, Heidelberg, Springer Berlin Heidelberg.

Dinev, T. 2014. "Why would we care about privacy?" *European Journal of Information Systems* (23:2), pp. 97–102.

Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61–80.

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* , pp. 636–655.

Forbes 2018. *The Continued Rise Of Voice Search And How Your Business Can Leverage It*. https://www.forbes.com/sites/forbesagencycouncil/2018/01/29/the-continued-rise-of-voice-search-and-how-your-business-can-leverage-it/#6b3d15f4301c. Accessed 19 November 2018.

Han, S., and Yang, H. 2018. "Understanding adoption of intelligent personal assistants," *Industrial Management & Data Systems* (118:3), pp. 618–636.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2014. "A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research," *Information Systems Research* (25:1), pp. 111–136.

Indefrey, P., and Levelt, W. J. M. 2004. "The spatial and temporal signatures of word production components," *Cognition* (92:1-2), pp. 101–144.

John, L. K., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* (37:5), pp. 858–873.

Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* (34:3), 549-A4.

Kehr, F., Wentzel, D., and Mayer, P. 2013. "Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect," in *Proceedings of the 34th International Conference on Information Systems*, R. Baskerville and M. Chau (eds.), Milan, Italy, Milan, Italy, pp. 1–10.

Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127–135.

Krauss, R. M., Freyberg, R., and Morsella, E. 2002. "Inferring speakers' physical attributes from their voices," *Journal of Experimental Social Psychology* (38:6), pp. 618–625.

Lee, B. J., Kim, K. H., Ku, B., Jang, J.-S., and Kim, J. Y. 2013. "Prediction of body mass index status from voice signals based on machine learning for automated medical applications," *Artificial intelligence in medicine* (58:1), pp. 51–61.

Lin, K.-Y., and Lu, H.-P. 2011. "Why people use social networking sites: An empirical study integrating network externalities and motivation theory: Group Awareness in CSCL Environments," *Computers in Human Behavior* (27:3), pp. 1152–1161.

Maier, C., Laumer, S., Eckhardt, A., and Weitzel, T. 2014. "Giving too much social support: social overload on social networking sites," *European Journal of Information Systems* (24:5), pp. 447–464.

Mallat, N., Tuunainen, V., and Wittkowski, K. 2017. "Voice Activated Personal Assistants – Consumer Use Contexts and Usage Behavior," *AMCIS 2017 Proceedings* .

Mencattini, A., Martinelli, E., Costantini, G., Todisco, M., Basile, B., Bozzali, M., and Di Natale, C. 2014. "Speech emotion recognition using amplitude modulation parameters and a combined feature selection procedure," *Knowledge-Based Systems* (63), pp. 68–81.

Mendes, D., and Ferreira, A. 2012. "Speaker identification using phonetic segmentation and normalized relative delays of source harmonics," .

Moorthy, A. E., and 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), pp. 307–335.

Morton, A., and Sasse, M. A. 2014. "Desperately seeking assurances: Segmenting users by their information-seeking preferences," in *2014 Twelfth Annual Conference on Privacy, Security and Trust (PST)*: *23 - 24 July 2014, Toronto, Canada*, A. Miri (ed.), Toronto, ON, Canada. 7/23/2014 - 7/24/2014, Piscataway, NJ: IEEE, pp. 102–111.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2011. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76–98.

Petronio, S. S., and Altman, I. 2002. *Boundaries of privacy*: *Dialectics of disclosure*, Albany, NY: State University of New York Press.

Pisanski, K., Fraccaro, P. J., Tigue, C. C., O'Connor, J. J. M., and Feinberg, D. R. 2014a. "Return to Oz: voice pitch facilitates assessments of men's body size," *Journal of experimental psychology. Human perception and performance* (40:4), pp. 1316–1331.

Pisanski, K., Fraccaro, P. J., Tigue, C. C., O'Connor, J. J.M., Röder, S., Andrews, P. W., Fink, B., DeBruine, L. M., Jones, B. C., and Feinberg, D. R. 2014b. "Vocal indicators of body size in men and women: a meta-analysis," *Animal Behaviour* (95), pp. 89–99.

Saffarizadeh, K., Boodraj, M., and Alashoor, T. 2017. "Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-Disclosure," *ICIS 2017 Proceedings* .

Singh, R., Keshet, J., Gencaga, D., and Raj, B. 2016. "The relationship of voice onset time and Voice Offset Time to physical age," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, IEEE, pp. 5390–5394.

Smith, J. H., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 980–1015.

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477–564.

Solove, D. J. 2011. "Why privacy matters even if you have 'nothing to hide'," *Chronicle of Higher Education* (15).

Souza, L. B. R. d., and Santos, M. M. D. 2018. "Body mass index and acoustic voice parameters: is there a relationship?" *Brazilian journal of otorhinolaryngology* (84:4), pp. 410–415.

Sun, Y., Wang, N., Shen, X.-L., and Zhang, J. X. 2015. "Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences," *Computers in Human Behavior* (52), pp. 278–292.

van Eerde, W., and Thierry, H. 1996. "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* (81:5), pp. 575–586.

Wakefield, R. 2013. "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157–174.

Whetten, D. A. 1989. "What Constitutes a Theoretical Contribution?" *Academy of Management Review* (14:4), pp. 490–495.

Wirth, J., Maier, C., Laumer, S., and Weitzel, T. forthcoming. "Perceived information sensitivity and interdependent privacy protection: a quantitative study," *electronic markets* .

Xu, H., Teo, H.-H., Tan, Bernard C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135–173.