



## UvA-DARE (Digital Academic Repository)

### “My phone must be listening!”

*Peoples’ surveillance beliefs around devices “listening” to offline conversations in the US, the Netherlands, and Poland*

Segijn, C.M.; Strycharz, J.; Turner, A.; Oprea, S.J.

**DOI**

[10.1177/20539517251337102](https://doi.org/10.1177/20539517251337102)

**Publication date**

2025

**Document Version**

Final published version

**Published in**

Big Data and Society

**License**

CC BY-NC

[Link to publication](#)

**Citation for published version (APA):**

Segijn, C. M., Strycharz, J., Turner, A., & Oprea, S. J. (2025). “My phone must be listening!”: Peoples’ surveillance beliefs around devices “listening” to offline conversations in the US, the Netherlands, and Poland. *Big Data and Society*, 12(2).  
<https://doi.org/10.1177/20539517251337102>

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

*UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)*

# “My phone must be listening!”: Peoples’ surveillance beliefs around devices “listening” to offline conversations in the US, the Netherlands, and Poland

Big Data & Society  
April–June: 1–15  
© The Author(s) 2025  
Article reuse guidelines:  
sagepub.com/journals-permissions  
DOI: 10.1177/20539517251337102  
journals.sagepub.com/home/bds



Claire M Segijn<sup>1</sup> , Joanna Strycharz<sup>2</sup> , Anna Turner<sup>3</sup>  and Suzanna J Oprea<sup>4</sup> 

## Abstract

Previous research has shown that internet users believe that electronic devices are listening to their offline conversations (i.e., e-eavesdropping) for commercial purposes. Such beliefs are important to study because they could shape media effects and human behavior (e.g., limiting free speech around devices). We conducted a preregistered cross-sectional survey in the United States, Netherlands, and Poland ( $N=886$ ) to examine internet users’ surveillance beliefs and evaluate the factors related to such beliefs. The results showed that respondents had different surveillance beliefs, including e-eavesdropping, priming, coincidence, and digital traces. US respondents were most likely to believe in e-eavesdropping. A higher frequency of conversation-related advertising and shorter time perception were associated with e-eavesdropping beliefs. Moreover, in all three countries, we found a positive relation between conspiracy mentality and e-eavesdropping belief. The findings indicate the importance of contextual and individual factors and could help further understand privacy boundaries and enhance the ethical responsibility of Big Data collection strategies.

## Keywords

Surveillance, smart devices, smartphone, conspiracy mentality, privacy

Developments within digital technologies and infrastructures such as high numbers of mobile device penetration worldwide (Statista, 2023) have led to widespread surveillance by different actors, such as government or corporate entities (Lyon, 2017; Zhang et al., 2023). Internet users’ data is collected on a large scale and then used for algorithmic decision-making and communication (Ball and Webster, 2020; Yun et al., 2020), such as personalized advertising, political microtargeting, or tailored health communication (Bol et al., 2018). From an internet user’s perspective, the awareness of data collection and processing by corporations, the government, or other institutions may trigger their perception of being surveilled, whether this is accurate or not (Lyon, 2017; Strycharz and Segijn, 2022).

For example, previous research showed that many internet users believe that their electronic devices are eavesdropping their offline conversations for commercial purposes, such as showing them personalized ads (Frick et al., 2021; Segijn et al., 2024; Vitak et al., 2023), a phenomenon which is called electronic eavesdropping (i.e., e-eavesdropping) (Segijn et al., 2024). However, companies have

denied using microphones for commercial purposes without consent (Hunter, 2021; Smalley, 2025). Given that beliefs regarding the extent and aim of surveillance that went into creating a message could affect how people respond to media messages and shape human behaviors (Strycharz and Segijn, 2022), we are interested in investigating those surveillance beliefs (rather than the use of actual surveillance), and what factors are related to those beliefs. The

<sup>1</sup>Hubbard School of Journalism and Mass Communication, University of Minnesota, Twin Cities, MN, USA

<sup>2</sup>Amsterdam School of Communication Research, University of Amsterdam, Amsterdam, the Netherlands

<sup>3</sup>Institute of Philosophy and Sociology, Polish Academy of Sciences, Warsaw, Poland

<sup>4</sup>Erasmus School of History, Culture and Communication ESHCC, Erasmus University Rotterdam, Rotterdam, the Netherlands

## Corresponding author:

Claire M. Segijn, Hubbard School of Journalism and Mass Communication, University of Minnesota, Twin Cities, MN, USA.  
Email: segijn@umn.edu



current study will utilize a preregistered survey to examine factors related to people's experiences (i.e., whether they have received a personalized ad related to an offline conversation, time perception between conversation and ad, how often they had such an experience, and how often they heard this happening to others), as well as individual characteristics (i.e., conspiracy mentality, tech savviness) and how they relate to the different beliefs.

Moreover, we will conduct the study in three countries, namely the United States, Netherlands, and Poland, to study the universality of surveillance beliefs and related factors. The choice of countries is driven by political differences in terms of privacy regulations and levels of (state) surveillance between the countries (Masur et al., 2025). The Netherlands and Poland both fall under the General Data Protection Regulation in Europe, which aims to strengthen transparency about surveillance practices and individual control regarding online data collection (Reding, 2011). However, in the US such an overarching legal framework is missing resulting in less transparency and control possibilities (Tushnet and Goldman, 2020). Additionally, differences between Western and Eastern European countries may also be expected based on their legal history and (surveillance) culture (Koops et al., 2016).

The current study will advance our theoretical knowledge about perceptions of surveillance by examining internet users' surveillance beliefs, and the factors related to the formation of these beliefs. Studying surveillance beliefs is important because it provides us with a deeper understanding of a surveillance culture that shapes human perception and behaviors. For example, when people believe that their electronic devices are listening to their offline conversations it may lead to the inhibition of legitimate behaviors (i.e., chilling effects; Büchi et al., 2022; Stevens et al., 2023), such as limiting free speech around devices or affecting people's autonomy to behave freely with and around devices (Strycharz and Segijn, 2022). Additionally, such beliefs could potentially lower people's trust in technology, as well as make them more cynical regarding privacy issues (Ranzini et al., 2023). Moreover, the research responds to the call for studying privacy-related topics beyond Western, educated, industrialized, rich, and democratic (WEIRD) societies (Masur et al., 2025) by examining the phenomenon in the United States and the Netherlands as well as in an under-researched Eastern European country (Ford et al., 2023), Poland. The insights of the current study contribute to digital literacy programs by effectively highlighting internet users' beliefs that may result in shifting patterns of their online behavior. Moreover, an emphasis on the recognition of privacy boundaries could enhance the ethical responsibility of communication strategies amongst corporations, politicians, (social) media platforms, and other institutions that collect, store, and process Big Data.

## Theoretical framework

### Online surveillance

Companies in various sectors have been collecting, using, and sometimes sharing information about individuals for decades (Christl, 2017). This Big Data has been used for service optimization, product improvement, and personalized communication (Zhang et al., 2023), leading to surveillance capitalism in which revenue is produced out of predicting and modifying consumer behavior (Zuboff, 2015). Personalized communication relies on the processing of individual data to create and deliver individually targeted messages, such as tailored health messages, political microtargeting, and personalized advertising (Bol et al., 2018). This type of communication is contributing to the creation of Big Data surveillance or dataveillance, which is the automated, continuous, and (unspecific) collection, storage, and processing of large volumes of digital traces (Degli-Esposti, 2014; Van Dijck, 2014).

Technological developments such as cookies placed on personal devices have enabled organizations to track website visits and the online behavior of individuals (Smit et al., 2014). Devices such as smartphones and wearables that are equipped with sensors and connected to the internet have become part of today's dataveillance ecosystems, adding another dimension to it (Christl, 2017). This creates a so-called surveillance culture, in which people's day-to-day activities are being surveilled by government or corporate entities (Penney, 2021). In this surveillance culture, people create surveillance imaginaries that include people's outlooks on surveillance (Lyon, 2017) as well as specific beliefs regarding the extent and purpose of surveillance (Strycharz and Segijn, 2022). The current study focuses specifically on such surveillance beliefs that individuals may have around ads that are seemingly related to a previous offline conversation, which is called conversation-related advertising (Segijn et al., 2024).

### Surveillance beliefs

Beliefs are "mental constructions about the probability that an object or event is associated with a given attribute" (Potter, 2012, p. 141). In line with Strycharz and Segijn (2022), we call beliefs about the extent and aim of surveillance "surveillance beliefs." An example of a surveillance belief that people seem to have, is that electronic devices are listening to their offline conversations (Frick et al., 2021; Segijn et al., 2024), hereafter referred to as e-eavesdropping. These people have faith in a very high probability that their phones (object) are associated with the idea of listening for commercial purposes (attribute). Even though this is technically possible (Kröger and Raschke, 2019) and microphones have been used to collect voice data for

service and algorithm improvement (Deibert, 2020), companies have denied accessing the microphone for commercial purposes (Hunter, 2021; Smalley, 2025). However, research shows that most people who report to have received conversation-related advertising, believe that it is because of an offline conversation (Segijn et al., 2024).

It is likely that internet users would have received the ad even if they did not have a specific offline conversation. However, an ad related to a previous offline conversation may stand out to them more when compared to a message that is not related to that conversation. This mechanism could be explained by priming. Priming is the principle in which activation of a stimulus affects the interpretation or response to a subsequent stimulus (Cofer, 1967). In our context, this means that a conversation about a product could make the subsequent persuasive message that includes that product more salient.

Besides priming, various explanations have been offered about how it is possible that internet users receive a message that is seemingly related to a previous conversation. For example, that is purely coincidental (Hunter, 2021). Additionally, companies have access to a lot of information through digital traces that internet users leave online, and based on that they can make inferences about specific topics someone might be interested in (Yun et al., 2020). Personalized communication is often based on people's interests inferred from online behavior (Bol et al., 2018). Similarly, people might be more likely to talk about things that interest them, which mates with personalized communication tailored to preferences (Segijn et al., 2024). Consideration can be given to the possibility that internet users may not remember looking for certain products online while computers and algorithms do not forget, which leads to the personalized messages that they are receiving. In sum, there are different surveillance beliefs that people may hold regarding conversation-related advertising. Our first aim is to map such surveillance beliefs. To this end, we propose the following research question:

RQ1. What are internet users' surveillance beliefs related to conversation-related advertising?

### **Belief formation**

Surveillance beliefs are developed over time through experiences (Strycharz and Segijn, 2022). This could be people's own experiences (first-hand experiences) or the experiences of others (second-hand experiences). For example, if someone talks about a product while their smartphone is around and they receive an ad for that product, they might attribute this to their smartphone listening. In a surveillance culture, surveillance is becoming part of a way of life and there might be a shared understanding of surveillance (Lyon, 2017). In such a culture, surveillance beliefs might be formed through folk theories, which are in part intuitive ideas that help to understand everyday

phenomena in the world (Gelman and Legare, 2011), such as algorithmic profiling (Büchi et al., 2023). Such lay theories do not necessarily have to be factual but can be purely speculative. They can be perceived as robust because they are generally accepted within a group or culture, and they are not necessarily systematically checked (Gelman and Legare, 2011). That electronic devices are eavesdropping might be such a folk theory reinforcing the belief that this is happening.

Additionally, the e-eavesdropping belief might be strengthened by features of the surveillance episode—an instance of perceived surveillance (Strycharz and Segijn, 2022), such as the ad that is seemingly related to a previous offline conversation. An example is the perceived time between the conversation and the media message, or the frequency with which people notice conversation-related ads. Research showed that most people who had experience with a conversation-related ad indicated that they received it shortly after (within a few hours) or within a day of the conversation. Less people reported receiving such an ad longer than that (Segijn et al., 2024). Therefore, the shorter the message appears after the offline conversation, the more likely people may attribute the ad to the conversation, rather than thinking of other explanations. Additionally, in line with the illusory truth effect (Hasher et al., 1977)—i.e., the more often we see something, the truer it seems—the frequency of the occurrence may play a role. Because people can also learn from the experiences of others (second-hand experiences), we hypothesize that the frequency of second-hand experiences may relate to conversation-related advertising surveillance beliefs similar to first-hand experiences.

H1: People who have had a first-hand experience with conversation-related communication are more likely to believe that it is because of (a) e-eavesdropping, and less likely to believe that it is because of (b) priming, (c) a coincidence, or (d) their digital data traces, than people who have not had this experience.

H2: The closer the time perception of the conversation-related communication appearing after the offline conversation, the more likely people are to believe that it is because of (a) e-eavesdropping, and less likely to believe that it is because of (b) priming, (c) a coincidence, or (d) their digital data traces.

H3: The higher the frequency of first-hand experience with conversation-related communication, the more likely people are to believe that it is because of (a) e-eavesdropping, and the less likely to believe that it is because of (b) priming, (c) a coincidence, or (d) their digital data traces.

H4: The higher the frequency of others' experience (second-hand experience) with conversation-related communication, the more likely people are to believe that it is because of (a) e-eavesdropping, and the less likely to believe that it is because of (b) priming, (c) a coincidence, or (d) their digital data traces.

### Individual differences

Additionally, the beliefs people hold may depend on individual characteristics, such as conspiracy mentality and how tech-savvy people are. Conspiracy mentality is a person's tendency to believe in conspiracy theories (Bruder et al., 2013). This has been found to be a relevant personality trait in the context of personalized communication and perceived surveillance (Boerman and Segijn, 2022; Zhang et al., 2023). Previous research found, for example, that conspiracy mentality is related to awareness and critical evaluation of personalized communication (Boerman and Segijn, 2022). Additionally, conspiracy mentality was found to be a positive predictor of perceived surveillance through social media, smartphones, smart speakers, and other electronic devices (Zhang et al., 2023). Generally, people who believe in one conspiracy theory are more likely to believe in others (Swami et al., 2010). e-Eavesdropping has been labeled as a conspiracy theory related to conversation-related advertising (Tidy, 2019). Therefore, we argue that conspiracy mentality could be positively related to e-eavesdropping beliefs and negatively to the idea of priming, coincidence belief, or digital traces.

H5: The higher the score on the conspiracy mentality scale, the more likely people are to believe that conversation-related communication happens because (a) their phones are listening, and the less likely to believe that it happens because of (b) priming, (c) a coincidence, or (d) digital data traces.

Additionally, we argue that people's tech savviness may play an important role in what beliefs they have regarding conversation-related advertising. Previous research found that higher tech savviness is related to perceptions of personalized communication, reactions to it and related privacy behaviors. For example, Widdicks et al. (2022) found that people with a high level of tech savviness display greater privacy concerns. Regarding behavior, previous studies found that technological skills are a strong predictor of online privacy protection (Büchi et al., 2017). Additionally, people have lower intention to click on a personalized message when they have higher internet competency (Kim and Huh, 2017). This indicates that tech-savvy people may have a better understanding of personalized communication and how to respond to it. Furthermore, previous research has associated lower digital or media literacy skills with susceptibility to fake news (Brashier and Schacter, 2020). Building on that, we expect that more tech-savvy people would be less likely to believe in e-eavesdropping and more likely to believe in other explanations such as priming, that the communication is a coincidence, or is a result of digital trace data.

H6: The more tech-savvy, the less likely people are to believe that conversation-related communication happens because (a) their phones are listening, and the more likely to believe that happens because of (b) priming, (c) a coincidence, or (d) digital data traces.

### Cross-country surveillance cultures

Finally, we will examine surveillance beliefs in three different countries because differences in cultural, social, political, economic, and technological matters can shape privacy-related issues (Masur et al., 2025; Nissenbaum, 2004). Because socio-legal contexts are thought to affect an individual's privacy rule-making process (Petronio, 2002), we selected three countries based on political differences related to contrasting privacy regulations and levels of (state) surveillance, namely the United States, the Netherlands, and Poland.

The United States and European countries (i.e., the Netherlands, Poland) differ in terms of privacy regulations and the amount of protection over personal data offered by these regulations (Tushnet and Goldman, 2020). On the one hand, privacy regulations in the US are fragmented, protecting specific vulnerable populations or sensitive data (e.g., Children's Online Privacy Protection Act, Health Insurance Portability and Accountability Act). Primary enforcement is done through the prohibition of unfair competition under section 5(a) of the Federal Trade Commission Act. With the exception of the California Consumer Privacy Act, the regulations focus less on individual awareness and offer less control mechanisms over data collection processes (Tushnet and Goldman, 2020).

By contrast, the General Data Protection Regulation (GDPR) offers an overarching framework for the European Union and aims to set high standards for data collection and processing of online personal data. A key goal is to increase individual awareness and empowerment concerning online data collection practices (Tushnet and Goldman, 2020). Indeed, past research shows high awareness of the GDPR among Europeans (European Commission, 2019). This could further increase awareness and perceptions of privacy-related topics. However, such protection offered by the law could make individuals less cautious about how they treat their privacy online, a phenomenon known as the control paradox (Brandimarte et al., 2013).

Moreover, differences between European countries exist. The Netherlands was one of the six founding fathers of the European Union in 1957. Poland, however, joined almost 50 years later, in 2004, after transitioning from a communist to a democratic nation. This also meant a transition from a nation with extensive governmental surveillance and limited guarantees of human rights, to a nation in which human rights were integrated into the constitutional orders (Koops et al., 2016). Additionally, more recently, concerns have been raised about the use of surveillance software by the Polish government, which has been the subject of the work of the European Parliament's Committee of Inquiry (European Parliament, 2022). These developments have received significant attention in the media, which could influence people's perceptions of surveillance. To this end, we ask:

RQ2: How do surveillance beliefs, and the factors related to their individual beliefs, manifest in the US, the Netherlands, and Poland?

## Method

### Sample and recruitment

To answer the research questions and test the hypotheses, we conducted an online survey in the United States (US), the Netherlands (NL), and Poland (PL) in Spring 2023 as part of a larger survey on this topic. The projects were identified and preregistered<sup>1</sup> as separate projects each with their own focus and hypotheses/questions before data collection. Additionally, the hypotheses and materials were pilot-tested and approved by the IRB (STUDY00017829) before conducting the study. In each country, respondents were recruited through an online survey company (Prolific, PanelClix, and SoftArchitext respectively) in the first language of that country (i.e., English, Dutch, Polish). Questionnaires were translated from English by a native speaker of that language and verified by two other native speakers independently.

A quota sample based on country demographics was requested for participants 18 years and older, living in that country, and using a smartphone daily. A power analysis for a multiple linear regression with a small effect size ( $f^2 = .02$ ) indicated that 311 responses were needed to achieve power of .80. In total, 912 respondents completed the survey (US  $n = 301$ ; NL  $n = 306$ , PL  $n = 305$ ). Some respondents indicated they did not want their data used and they were removed, resulting in a final sample of 300 US respondents ( $M_{\text{age}} = 45.47$  ( $SD_{\text{age}} = 15.94$ ; 50% female, 48.3% male), 293 Dutch respondents ( $M_{\text{age}} = 47.24$  ( $SD_{\text{age}} = 15.60$ ; 46.1% female, 53.2% male), and 293 Polish respondents ( $M_{\text{age}} = 45.84$  ( $SD_{\text{age}} = 14.48$ ; 49.3% female, 49.8% male).

### Procedure

Respondents were invited to participate through the survey platform and were first asked to read and sign the informed consent form and to answer the screening questions before they could proceed to the survey. The respondents were introduced to the topic with the following text: "Coincidental or not, sometimes people receive an online advertisement on one of their devices (e.g., smartphone, tablet) for a brand or product that they recently talked about with someone else in an offline conversation." We did not use the words "conversational-related advertising" or "surveillance" to prevent priming. We asked whether they have experienced such a situation and whether they knew of someone else who had experienced it. After that, we asked them to report the frequency of this happening to themselves, and hearing about it through others in the last year. Additionally, they

were asked to answer questions about conspiracy mentality and level of tech savviness and to provide demographic information. Finally, they were thanked for their time and received a monetary incentive for participation through the online platform.

### Measures

An overview of the measures and the overall mean and standard deviation per country can be found in Table 1 and 2. The full questionnaire can be found in the OSF repository.<sup>1</sup> Surveillance beliefs were measured through an open-ended question, followed by a closed-ended question on consecutive pages of the questionnaire (see statements in Table 1). When people indicated earlier in the questionnaire that they had experienced conversation-related advertising, they were asked how they thought it worked. The respondents who indicated they did not have such an experience were asked to imagine that they would receive such a message and how they thought that would work. All open-ended answers were coded by one coder, and a second coder coded the answers of about 100 respondents for intercoder reliability. The codebook can be found in the OSF repository.<sup>1</sup> Coders were asked to code for each belief, whether the belief was mentioned by the respondent (1), not mentioned (0), or if the answer was missing or was not understandable (99). The coding showed good to excellent intercoder reliability (Krippendorff's alpha for the four different beliefs are US > .81, NL > .89, PL > .88).

## Results

### Surveillance beliefs

**Open-Ended results.** To answer the first research question about respondents' beliefs in general (RQ1), we analyzed the results from the open-ended (Table 3) and closed-ended questions. e-Eavesdropping, priming, coincidence, and digital data traces were all mentioned by the respondents in all three countries as possible explanations for conversation-related advertising. Additionally, respondents provided new beliefs. In all three countries, respondents mentioned that conversation-related advertising is enabled by advanced technology (e.g., artificial intelligence, algorithms, specialized software, and (smart) technology), without providing further information on the specific workings. They also mentioned illegal or problematic practices (e.g., hacking, spying, or data breaches). Advertising strategies (e.g., aggressive, sneaky advertising, mass communication) were also mentioned by US and Dutch respondents. Finally, a few respondents in the US mentioned that the results could be due to phones of conversation partners being in close proximity, which could explain getting messages related to their conversation partner's interests.

**Table 1.** Overview of beliefs.

Statement	Belief	US		NL		PL	
		M	SD	M	SD	M	SD
I received the ad because my phone or another device was listening to the conversation	e-Eavesdropping	4.69 <sup>a</sup>	1.95	4.02 <sup>b</sup>	1.87	4.23 <sup>b</sup>	1.85
The offline conversation made the ad stand out more to me (made it more noticeable)	Priming	5.04 <sup>a</sup>	1.56	4.58 <sup>b</sup>	1.63	4.12 <sup>c</sup>	1.60
It is a coincidence that I received the ad on my device (e.g., smartphone) related to what I talked about in an offline conversation	Coincidence	3.81 <sup>a</sup>	1.89	3.84 <sup>b</sup>	1.80	3.51 <sup>a</sup>	1.68
I received the ad because it was based on online data on my own preferences and interests	Online available data	4.99 <sup>a</sup>	1.71	4.79 <sup>b</sup>	1.63	4.26 <sup>b</sup>	1.63
I received the ad because of my prior online activities (e.g., search, online shopping) related to the product or brand	Previous online activities	4.98 <sup>a</sup>	1.81	4.97 <sup>b</sup>	1.74	4.58 <sup>b</sup>	1.83

Note. Different superscripts indicate significant differences across countries. Digital traces consist of online available data and previous online activities.

About 20–36 percent of the responses were categorized as “unspecified,” which means that, although they provided an answer, the respondent did not provide a *reason* for receiving the conversation-related advertising. The unspecified group consisted mostly of respondents who: (1) mentioned an example of conversation-related advertising (e.g., I talked about x and then I saw a message about x) without providing a reason for how this worked; or (2) respondents mentioned only how they thought it did *not* work (e.g., it cannot be a coincidence; I do not believe devices are listening; I have not searched for it before). Most answers in the first group hinted at e-eavesdropping, but because the respondents did not explicitly mention a device listening or eavesdropping, we did not code them as such. Therefore, the e-eavesdropping percentages in the Table might be lower than the number of respondents believing in it.

Additionally, in all three countries, we could distinguish between respondents with different degrees of confidence in their e-eavesdropping belief answer. Some respondents indicated they were certain their phones were listening; others were not sure. And again, another group indicated they were certain that this was not happening. Reasons for believing in e-eavesdropping were sometimes mentioned as well, such as frequency of occurrence (e.g., it happens too often to be a coincidence), specificity of the product (e.g., too much a niche product), time between conversation and message (e.g., 2 minutes after), or not seeing another possibility (e.g., I did not search for it and have never thought about it before).

Furthermore, in all three samples, we could distinguish between respondents who indicated they believed the results were from listening versus eavesdropping/spying. Some respondents connected e-eavesdropping to a specific company or brand (e.g., Google, Facebook), yet others kept it more generic (e.g., artificial intelligence, an algorithm). Finally, a few on the fence or unconvinced

respondents explicitly labeled this belief as a (potential) conspiracy theory. They also sometimes mentioned that other people may forget they had searched for the item in the past as an explanation for why they may believe in e-eavesdropping.

**Belief closed-ended results.** Next, we conducted One-Way ANOVAs to compare the answers from closed-ended questions about different beliefs across the three countries, focusing on e-eavesdropping, priming, coincidence, and digital data traces (including online available data and previous online activities) (Table 1; Figure 1). We found that US respondents were more likely to believe in e-eavesdropping ( $M=4.69$ ,  $SD=1.95$ ) than respondents in the European countries (NL  $M=4.02$ ,  $SD=1.87$ ; PL  $M=4.23$ ,  $SD=1.85$ ),  $F(2, 882)=9.549$ ,  $P<.001$ . Figure 1 shows that 72% of US respondents think it is somewhat-to-very likely that eavesdropping is used to show them ads seemingly related to a previous offline conversation, opposed to 55.8% in the Netherlands and 57.1% in Poland.

Additionally, US respondents were the most likely to believe in priming ( $M=5.04$ ,  $SD=1.56$ ), followed by Dutch respondents ( $M=4.58$ ,  $SD=1.63$ ), and finally Polish respondents ( $M=4.12$ ,  $SD=1.60$ ),  $F(2, 881)=24.441$ ,  $P<.001$ . US and Dutch respondents were more likely to believe in digital traces than Polish respondents (Online available data  $F(2, 883)=15.426$ ,  $P<.001$ ; Previous online activities  $F(2, 881)=4.719$ ,  $P=.009$ ). No differences were found among the countries regarding the coincidence belief,  $F(2, 881)=3.016$ ,  $P=.050$ .

### Experience and individual factors related to the beliefs

To test hypothesis 1 regarding the difference between respondents with or without conversation-related advertising

**Table 2.** Measurement overview.

Concept and items	Scale	US M (SD)	NL M (SD)	PL M (SD)
Frequency self		2.92 (0.88)	2.80 (1.02)	2.76 (0.97)
How often have you noticed that you received an online ad that was seemingly related to what you talked about in an offline conversation in the past year?	(1) once (2) A couple times (2-3 instances) (3) Several times (4–5 times) (4) Regularly (more than 5 times)			
Frequency other		2.66 (0.94)	2.55 (0.99)	2.46 (0.91)
How often have you heard that someone else received an online ad that was seemingly related to what they talked about in an offline conversation in the past year?	(1) once (2) A couple times (2–3 instances) (3) Several times (4–5 times) (4) Regularly (more than 5 times)			
Time perception		2.67 (0.77)	2.65 (0.89)	2.45 (0.87)
What was approximately the time between the offline conversation and seeing the ad?	(1) At the same time (ad was seen during the conversation) (2) Ad was seen shortly after the conversation (within a few hours) (3) Ad was seen within a day after the conversation (4) Ad was seen within a few days or a week after the conversation (5) Ad was seen within a month after the conversation			
Conspiracy mentality (Bruder et al., 2013)		4.56 (1.46)	4.43 (1.15)	4.82 (1.20)
I think that many very important things happen in the world, which the public is never informed about	(1) strongly disagree to (7) strongly agree			
I think that organizations usually do not tell us the true motives for their decisions				
I think organizations closely monitor all citizens				
I think that events which superficially seem to lack a connection are often the result of secret activities				
I think that there are secret organizations that greatly influence political decisions				
Tech savviness (Power users) <sup>3</sup> (Sundar and Marathe, 2010)		5.05 (1.00)	4.44 (0.98)	4.51 (1.02)
I have to have the latest available upgrades of the technological devices I use	(1) strongly disagree to (7) strongly agree			
I love exploring all the features that any technological gadget has to offer				
Using information technology makes it easier to do my work				
A little bit of intuition is all that I need to figure out how to use any new technology				
I make good use of most of the features available in any technological device				
I feel like information technology is a part of my daily life				
Using any technological device comes easy to me				
I think most of the technological gadgets are complicated to use (reversed)				

<sup>3</sup>We also preregistered to look into algorithmic awareness. Respondents were asked whether they thought four statements (e.g., “When you go to a website, it can collect information about you even if you do not register”) were true, false, or they did not know. However, the measurement did not distinguish scores between respondents who truly understand how algorithms work and respondents who have a suspicion of data practices based on folk/conspiracy theories. Because of this validity issue, we decided not to use this factor.

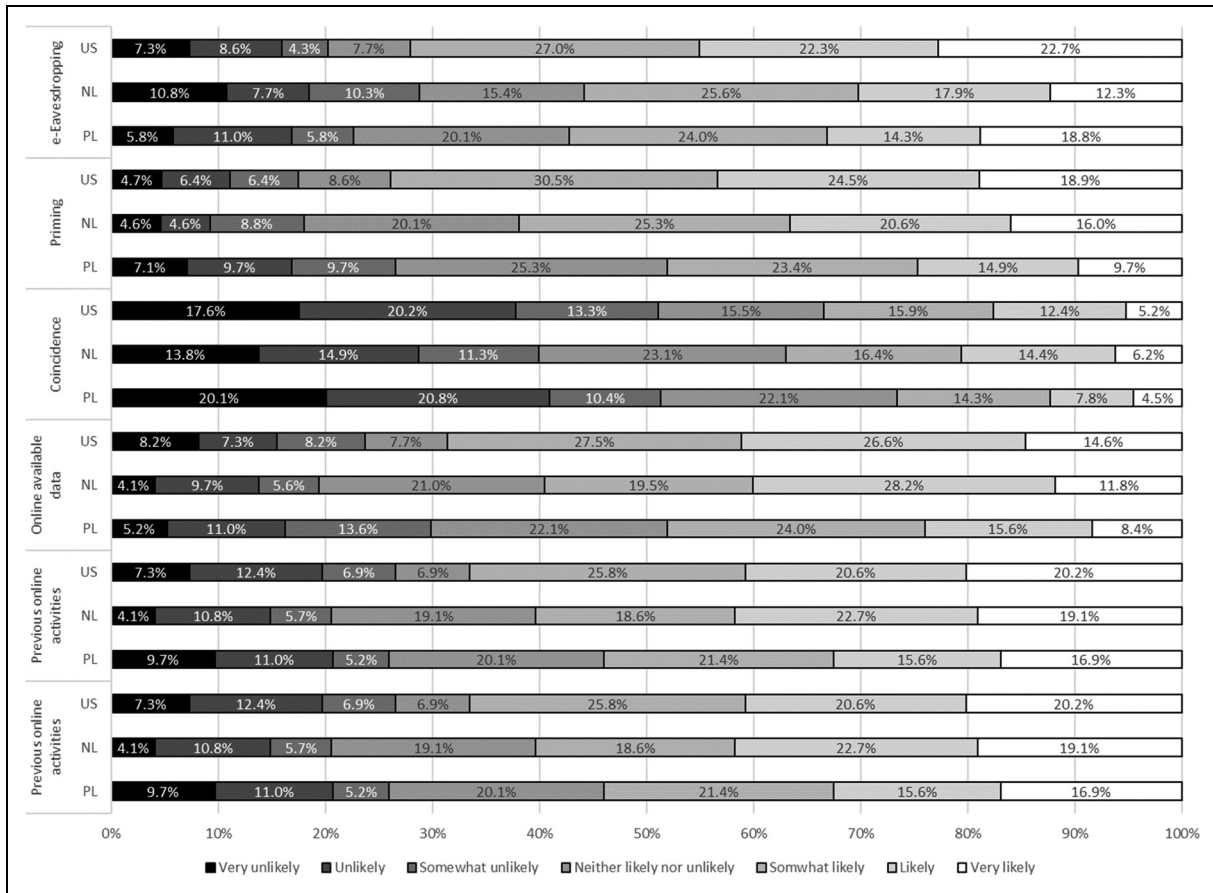
experiences, we conducted ANOVAs per country with experience as the independent variable and the beliefs as the dependent variables. Additionally, we conducted

correlation analyses per country to test the relationship between the other independent variables and the different beliefs.<sup>2</sup>

**Table 3.** Overview of open-ended answers per country and per experience with conversation-related advertising group.

	Experienced		Maybe		Not experienced	
	Ranking beliefs	New beliefs	Ranking beliefs	New beliefs	Ranking beliefs	New beliefs
United States	<p><i>n</i> = 233</p> <ol style="list-style-type: none"> <li>1. e-Eavesdropping (47.2%)</li> <li>2. Data (21%)</li> <li>3. Do not know (12.9%)</li> <li>4. Coincidence (9.0%)</li> <li>5. Priming (2.1%)</li> </ol> Unspecified 19.7%	<ul style="list-style-type: none"> <li>- Advanced technology (e.g., Artificial intelligence, phones, special software, algorithm)</li> <li>- Phone in close proximity of conversation partner's phone (their data)</li> <li>- Popular product</li> <li>- Conversation with customer service</li> <li>- Spying</li> <li>- Cyber advertisement</li> <li>- Magic</li> </ul>	<p><i>n</i> = 33</p> <ol style="list-style-type: none"> <li>1. Data (40.6%)</li> <li>2. Do not know (21.9%)</li> <li>3. E-Eavesdropping (18.8%)</li> <li>4. Coincidence (15.6%)</li> <li>5. Priming (6.3%)</li> </ol> Unspecified (12.5%)	<ul style="list-style-type: none"> <li>- Advanced technology (e.g., Artificial intelligence, algorithm)</li> <li>- Advertising clutter</li> </ul>	<p><i>n</i> = 34</p> <ol style="list-style-type: none"> <li>1. e-Eavesdropping (36.4%)</li> <li>2. Data &amp; Do not know (18.2%)</li> <li>4. Coincidence (6.1%)</li> <li>5. Priming (3.0%)</li> </ol> Unspecified (21.2%)	<ul style="list-style-type: none"> <li>- Advanced/smart technology</li> <li>- Forwarded by conversation partner</li> <li>- Spying</li> <li>- Hacking/bugged phone</li> </ul>
The Netherlands	<p><i>n</i> = 168</p> <ol style="list-style-type: none"> <li>1. e-Eavesdropping (20.2%)</li> <li>2. Do not know (15.5%)</li> <li>3. Data (11.9%)</li> <li>4. Coincidence (10.1%)</li> <li>5. Priming (2.4%)</li> </ol> Unspecified (36.3%)	<ul style="list-style-type: none"> <li>- Advanced technology (e.g., phones, smart devices)</li> <li>- data breach</li> <li>- Very technological</li> <li>- Sneaky or aggressive advertising</li> <li>- Social media</li> <li>- I am part of the target group of the product</li> <li>- General products/brands</li> </ul>	<p><i>n</i> = 44</p> <ol style="list-style-type: none"> <li>1. Do not know (45.5%)</li> <li>2. Data (20.5%)</li> <li>3. Coincidence (6.8%)</li> </ol> Unspecified (22.7%) e-Eavesdropping, Priming (0%)	<ul style="list-style-type: none"> <li>- It is impossible</li> </ul>	<p><i>n</i> = 42</p> <ol style="list-style-type: none"> <li>1. Do not know (23.8%)</li> <li>2. Data (17.7%)</li> <li>3. e-Eavesdropping (9.5%)</li> <li>4. Coincidence (7.1%)</li> <li>5. Priming (2.4%)</li> </ol> Unspecified (28.6%)	<ul style="list-style-type: none"> <li>- It is impossible</li> </ul>
Poland	<p><i>n</i> = 123</p> <ol style="list-style-type: none"> <li>1. e-Eavesdropping (27.6%)</li> <li>2. Do not know (13.8%)</li> <li>3. Data (10.6%)</li> <li>4. Coincidence (4.1%)</li> </ol> Unspecified (41.5%) Priming (0%)	<ul style="list-style-type: none"> <li>- Advanced technology (e.g., Artificial Intelligence, Internet of Things)</li> <li>- Synchronizing keywords from social media</li> <li>- Being watched</li> <li>- Hacking</li> </ul>	<p><i>n</i> = 52</p> <ol style="list-style-type: none"> <li>1. Do not know (26.9%)</li> <li>2. e-Eavesdropping (21.2%)</li> <li>3. Coincidence (11.5%)</li> <li>4. Data &amp; Priming (1.9% each)</li> </ol> Unspecified (40.4%)	<ul style="list-style-type: none"> <li>- Thoughts</li> </ul>	<p><i>n</i> = 62</p> <ol style="list-style-type: none"> <li>1. Do not know (32.3%)</li> <li>2. listening (11.3%)</li> <li>3. Coincidence (6.5%)</li> <li>4. data (3.2%)</li> </ol> Unspecified (41.9%) Priming (0%)	<ul style="list-style-type: none"> <li>- Advanced technology (i.e., Artificial Intelligence)</li> <li>- Someone need to tell it to the other party</li> </ul>

Note. The percentages do not add up to 100% because some respondents' answers fit multiple categories and some fit none of the categories (new belief). The *n* includes the number of respondents with valid answers for that category.



**Figure 1.** Conversation-related advertising beliefs in the US, the Netherlands, and Poland.

**e-Eavesdropping belief.** In line with H1a, we found that in all three countries, respondents who reported having experiences with conversation-related advertising were more likely to believe in e-eavesdropping compared to respondents who reported not having such an experience (US  $F(1, 264) = 10.467, P = .001$ ; NL  $F(1, 241) = 15.840, P < .001$ ; PL  $F(1, 229) = 14.735, P < .001$ ; Table 4). Additionally and in line with the prediction, e-eavesdropping beliefs were positively correlated with the frequency with which it happened to the respondents themselves (US  $r = .32, P < .001$ ; NL  $r = .21, P = .004$ ; PL  $r = .31, P < .001$ ), frequency that it happened to others (US  $r = .34, P < .001$ ; NL  $r = .18, P = .016$ ; PL  $r = .23, P = .006$ ), conspiracy mentality (US  $r = .38, P < .001$ ; NL  $r = .37, P < .001$ ; PL  $r = .28, P < .001$ ), and was negatively correlated with time perception (US  $r = -.23, P < .001$ ; NL  $r = -.18, P = .016$ ; PL  $r = -.20, P = .017$ ), confirming H2a-5a. No significant relationship between tech savviness and the e-eavesdropping belief was found in all three countries (H6a).

**Priming.** Contrary to H1b, we found that Dutch and Polish respondents who received a conversation-related advertising before were more likely to believe it could be due to priming (NL  $F(1, 240) = 12.180, P < .001$ ; PL  $F(1, 229) =$

$6.973, P = .009$ ; Table 4). No significant difference was observed between US respondents with or without a conversation-related advertising experience ( $P = .598$ ). However, the more tech-savvy the US respondents indicated they were, the more likely they believed in priming (US  $r = .14, P = .017$ ), confirming H6b (Table 5). No significant relationship for any of the other factors and priming was found in the US sample and none of the other factors were related to priming in the two European countries (Table 5).

**Coincidence belief.** In line with H1c, US respondents who reported they had never received a conversation-related advertising, were more likely to believe it was a coincidence compared to US respondents who received such a message (US  $F(1, 264) = 26.205, P < .001$ ). We did not find this difference in the two European samples (NL  $F(1, 241) = 1.000, P = .318$ ; PL  $F(1, 229) = 0.871, P = .352$ ; Table 4). Additionally, US respondents were more likely to believe it was a coincidence when they perceived more time between the conversation and the message (US  $r = .20, P = .002$ ) when it happened less often to themselves (US  $r = -.33, P < .001$ ) or others (US  $r = -.24, P < .001$ ), and when they scored lower on conspiracy mentality (US  $r = -.29, P < .001$ ), confirming H2c-5c for the US sample.

**Table 4.** Experience related to the beliefs per country (H1).

	M (SD)	(a) e-Eavesdropping			(b) Priming			(c) Coincidence			(d1) Online available data			(d2) Previous online activities		
		Experience	No experience	Experience	Experience	No experience	Experience	No experience	Experience	No experience	Experience	No experience	Experience	No experience		
		n	n	n	n	n	n	n	n	n	n	n	n	n		
US	4.97 (1.83)**	<b>3.85 (2.06)**</b>	5.03 (1.64)	5.18 (1.16)	<b>3.50 (1.85)***</b>	<b>5.24 (1.73)***</b>	<b>4.77 (1.78)**</b>	<b>5.62 (1.39)**</b>	<b>4.74 (1.89)*</b>	<b>5.59 (1.28)*</b>	233	33	233	33		
NL	4.41 (1.82)***	<b>3.25 (1.72)***</b>	4.82 (1.74)**	3.94 (1.51)**	3.81 (1.80)	3.52 (1.80)	4.74 (1.63)	4.83 (1.67)	4.81 (1.74)	5.04 (1.90)	195	48	194	48		
PL	4.64 (1.77)***	<b>3.66 (1.90)***</b>	4.32 (1.66)**	3.73 (1.48)**	3.31 (1.78)	3.53 (1.52)	4.29 (1.61)	4.08 (1.63)	4.47 (1.88)	4.62 (1.78)	154	77	154	77		

Note. \*\*\*  $P < .001$ , \*\*  $P < .01$ , \*  $P < .05$ . Bolded mean differences confirm the hypothesis.

**Table 5.** Context and individual factors related to the beliefs per country.

	r	n	(a) e-Eavesdropping						(b) Priming						(c) Coincidence						(d1) Online available data						(d2) Previous online activities					
			US		NL		PL		US		NL		PL		US		NL		PL		US		NL		PL		US		NL		PL	
			US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL	US	NL
Time perception (H2)			<b>-.225***</b>	<b>-.181*</b>	<b>-.202*</b>	.080	.080	-.012	<b>.202**</b>	.105	.067	.101	<b>.202**</b>	-.113	.126	<b>.250***</b>	.000															
Frequency self (H3)			<b>.324***</b>	<b>.209**</b>	<b>.310</b>	-.117	.052	.117	<b>-.328***</b>	<b>-.153*</b>	.059	.011	.091	<b>.221**</b>	.065	-.010	.196*															
Frequency other (H4)			<b>.343***</b>	<b>.183*</b>	<b>.228**</b>	-.094	.075	.125	<b>-.238***</b>	-.117	-.050	-.018	.045	.165	-.022	-.040	.209*															
Conspiracy mentality (H5)			<b>.379***</b>	<b>.366***</b>	<b>.276***</b>	-.096	.074	.111	<b>-.286***</b>	-.102	-.069	-.064	.044	<b>.202***</b>	-.069	-.020	.175**															
Tech saviness (H6)			.102	.079	-.004	<b>.138*</b>	.058	.079	.031	.079	.025	.065	.023	<b>.157**</b>	<b>.122*</b>	.002	.175**															

Note. \*\*\*  $P < .001$ , \*\*  $P < .01$ , \*  $P < .05$ . Bolded correlations confirm the hypothesis.

In line with H3c, the less often it happened to Dutch respondents, the more likely they believed it was a coincidence (NL  $r = -.15$ ;  $P = .035$ ). None of the factors were significantly related to coincidence bias for Polish respondents. In addition, tech-savvy respondents said they were not related to the coincidence belief in any of the samples (Table 5).

**Digital traces.** In line with H1d, US respondents who reported they had never received conversation-related advertising, were more likely to believe conversation-related advertising was possible due to online available data (US  $F(1, 265) = 7.011$ ,  $P = .009$ ), or previous online activities (US  $F(1, 265) = 6.403$ ,  $P = .012$ ), as compared to US respondents who reported they had received such a message. No significant differences depending on their experience were found for the two European samples (Table 4). In line with H2d, we found that the longer the perception of time between the offline conversation and message, the more likely Dutch respondents thought it was because of online available data (NL  $r = .20$ ,  $P = .007$ ), or previous online activities (NL  $r = .25$ ,  $P < .001$ ). Additionally, the more tech-savvy they were, the more likely US and Polish respondents believed it was because of previous online activities (US  $r = .12$ ,  $P = .035$ ; PL  $r = .18$ ,  $P = .003$ ). Polish respondents believed it was a result of online available data (PL  $r = .16$ ,  $P = .007$ ). These results confirmed H6d for these samples. Additionally, opposite results were found for several factors for Polish respondents. Polish respondents believed more in online available data when it happened more frequently to them (PL  $r = .22$ ,  $P = .007$ ), or when they scored higher on conspiracy mentality (PL  $r = .20$ ,  $P < .001$ ). Also, Polish respondents were more likely to believe that it was based on previous online activities when this happened more often to them (PL  $r = .20$ ,  $P = .017$ ), to others (PL  $r = .21$ ,  $P = .013$ ), or when they scored higher on conspiracy mentality (PL  $r = .18$ ,  $P = .003$ ).

## Discussion

A concern among internet users is that their electronic devices (e.g., smartphones, smart speakers) are listening in to their offline conversations, and this information is used to personalize communication to them based on these conversations. An example of this is when people talk about a product and receive an advertisement for that same product shortly thereafter. Although companies deny using listening practices, studies report the majority of internet users believe this is happening (Frick et al., 2021; Segijn et al., 2024). Given that perceptions of surveillance could affect people's responses to the act of surveillance (Strycharz and Segijn, 2022), we were interested in perceptions rather than actual surveillance. Specifically, we examined internet users' surveillance beliefs and what factors were related to such beliefs. We conducted a preregistered survey in the

US, the Netherlands, and Poland to study these questions and to examine the universality of the results.

First, we found that the respondents had different surveillance beliefs, including electronic eavesdropping (e-eavesdropping), priming, coincidence, or digital traces. Other beliefs included advanced technology, illegal or problematic practices (e.g., hacking), advertising strategies, or devices between conversation partners being in proximity. Advanced technology was often mentioned in a generic sense, in that respondents mentioned the role of artificial intelligence, algorithms, or the Internet of Things, without explaining how that might work. This may indicate that such terms are central to current folk theories around technology, which people may have heard about in the media but may have a limited understanding of.

From the qualitative responses, experience with conversation-related advertising seemed to be related to confidence in e-eavesdropping, as well as specific factors of the experience, such as the frequency, specificity of the product advertised, and the time between the conversation and the message. The closed-ended questions in our survey confirmed the role of experience, time perception, and frequency in whether respondents believed in e-eavesdropping. Additionally, we found that in the US sample that experience was the factor related to most beliefs, in the Netherlands this was time perception, and in Poland this was frequency. The role of experience and frequency related to e-eavesdropping in all three countries may indicate support for the illusory truth effect in this context. Future research could further examine specificity of the product as it was mentioned by respondents as a contributing factor to people's e-eavesdropping beliefs, but we did not measure this.

Second, our findings confirm that internet users believe that the content of their conversations can be a source of data for personalized communication, which is in line with past research (Frick et al., 2021; Vitak et al., 2023). In fact, e-eavesdropping was spontaneously mentioned by the respondents in the open-ended questions, while the likelihood of e-eavesdropping as a mechanism for conversation-related advertising was somewhat to very likely for most respondents, especially in the United States. However, respondents communicated different degrees of confidence about e-eavesdropping, from being very confident that this is how it works, to being on the fence, to being very confident that this was not happening. Additional differences were found in the open-ended questions regarding whether respondents referred to the occurrence as listening or eavesdropping—equivalents were found in the Dutch answers “(mee)luisteren” vs “affluisteren” and Polish answers “rejestruje” vs “podśluchuje.” The wording chosen by the respondents might suggest different perceived severity and expectations of the individuals. For example, the word “creepy” was mentioned by several respondents in relation to eavesdropping or when

they did not know how e-eavesdropping worked. Similarly, some respondents associated conversation-related advertising with illegal or problematic practices (e.g., hacking, spying, data breach), which may have consequences for how people respond to such media messages. However, future research is needed to further examine such media effects.

Third, the current study is a first step in examining the universality of the phenomenon and we observed that some patterns of the surveillance beliefs in the three countries differed. First, we found that respondents in the US were most likely to believe in e-eavesdropping, compared to respondents from the two European countries. Additionally, no relationship between experience and priming was found in the US, but a positive correlation was found for the two European Union (EU) countries, results which were in the opposite direction from our prediction. A possible explanation for both results is the difference in privacy regulations between the US and the EU. Because of the GDPR, respondents in the EU might be more likely to believe that such practices are not allowed or possible, and therefore, there must be another explanation for the incident. Additionally, future research could further look into the public discourse around surveillance, for example in the (news) media, and how this differs across countries. This can provide further explanation of the results as the media contribute to belief formation and people encounter stories around this phenomenon in the media (Segijn et al., 2024).

Another notable difference is that we found that Polish respondents were less likely to believe in digital trace data as an explanation for conversation-related advertising compared to Dutch and US respondents. Poland is generally considered a less marketing-savvy market regarding personalized communication (Maslowska et al., 2013), which may explain this difference. Furthermore, and contrary to our expectations, we found that the more Polish respondents encountered conversation-related advertising and the higher they scored on conspiracy mentality, the more likely they were to believe in digital traces. This could potentially be explained by the country's history of state surveillance and the large amount of recent news coverage related to the government surveilling citizens (Amnesty International, 2022; European Parliament, 2022). These factors might contribute to a stronger surveillance culture in Poland. Therefore, digital traces and the concept of surveillance might be more salient and have a strong tie in people's associative network. Thus, when surveillance practices are primed, the digital trace belief may be activated as well. Future research is needed to further validate the claims and look into explanations for different results across countries.

### *Theoretical and practical implications*

The current study contributes to the knowledge on people's surveillance beliefs and the belief formation in three countries. It shows that surveillance beliefs are related to

the surveillance episode (e.g., frequency) and individual characteristics (e.g., conspiracy mentality). While experience is important, its characteristics play a crucial role in forming surveillance beliefs. It is not only about one's experiences or those of another but also about their frequency and moment of occurrence that relates to how people explain conversation-related advertising. The role of conspiracy mentality suggests certain individuals might be more susceptible to forming certain beliefs. Future research is needed to test to what extent such factors play a role in media effects.

We should note, however, that with a cross-sectional survey, we cannot establish causality. Therefore, we need to be careful to conclude whether experience leads to e-eavesdropping beliefs or vice versa. In line with confirmation bias (Nickerson, 1998), it is possible that internet users who believe in e-eavesdropping are more likely to categorize (personalized) communication as conversation-related, which in turn could further strengthen their folk and conspiracy theories. This could, for example, explain the higher likelihood of believing in e-eavesdropping in the US sample, in which respondents also report having more experiences with conversation-related advertising. Additionally, survey research relies on self-reporting measures, which could have influenced the results. For example, we measured how tech-savvy respondents *reported* they are, rather than how tech-savvy they actually are. It is possible that some respondents are confident in their ability and knowledge of technology, but this knowledge may be inaccurate. The self-reporting nature of this variable may potentially explain the non-significant relationship between tech savviness and e-eavesdropping. Similarly, side notes could be placed next to the conspiracy mentality scale. Although this scale has been validated to be used in North American and European countries (Bruder et al., 2013) and used in previous research on perceived surveillance and personalized communication (Boerman and Segijn, 2022; Zhang et al., 2023), the level of conspiracy mentality may differ across countries (Bruder et al., 2013) and the scale itself does not include any conspiracies related to smart devices listening.

Furthermore, the current study contributes to our theoretical knowledge by investigating this type of communication in different countries. By doing so, we can challenge the universality of the studied hypotheses (Livingstone, 2003). Indeed, the results in the three different countries differ in some respects. Specifically, most hypotheses were confirmed in the sample from the United States. This could potentially be explained by the fact that many studies about privacy or personalized communication-related topics have been conducted in the US (Baruh et al., 2017; Segijn et al., 2021). Because scientific research builds on previous research, it is not surprising that most hypotheses developed on extant research are more likely to be confirmed in the US context. Therefore, we concur with the call for more comparative research on privacy-related topics (Ford

et al., 2023; Masur et al., 2025). More efforts need to be made to include more and other non-WEIRD countries as insights may differ across various nations. Although some other Eastern European countries may have a similar history with (state) surveillance as Poland, future research is needed to validate the claim and examine whether these results are generalizable across respondents from other countries.

Additionally, whether people believe that conversation-related advertising was enabled by e-eavesdropping, priming, a coincidence or digital traces may affect how internet users respond to such messages (Strycharz and Segijn, 2022). Negative associations (e.g., creepy, hacking, spying) may indicate more negative attitudes toward such communication. Insights into individual factors (e.g., conspiracy mentality) that are related to the different beliefs help to navigate potential negative responses to communication efforts by specific target groups. Furthermore, transparency on how the data is collected and processed for the media message could help to create awareness of such practices (Segijn et al., 2021) and debunk misinformation. This may also be in the best interest of (social) media platforms on which these ads are shown, or companies associated with such practices (e.g., Meta; Segijn et al., 2024). How people feel toward the media message could potentially transfer (i.e., spillover effect) to how internet users feel about or engage with the platform (Strycharz and Segijn, 2022). Moreover, unwanted access to personal data is seen as a privacy violation and may negatively impact individuals and society. For example, it may change the relationship between people and their electronic (smart) devices (Vitak et al., 2023). If people feel that they are being surveilled through their smartphones or smart speakers, it may change how people interact with their phones or smart devices or limit free speech when being around their devices. Additionally, powerful and difficult-to-understand technologies may make people more cynical toward privacy issues, subsequently, this could lower people's trust in technology (Ranzini et al., 2023).

The findings of the current study also have implications for digital literacy. Belief formation happens through people's experiences as well as information sources. A low number of people hear about the phenomenon through news sources or talks (Segijn et al., 2024). Therefore, there is an opportunity for academic institutions, the government, and journalists to further educate people on this phenomenon. The results of the current study showed that e-eavesdropping was seen as a potential reason for conversation-related advertising when people could not think of any alternative explanations. This suggests an opportunity for digital literacy around this topic to educate people on alternative explanations, such as priming or digital traces. Given the various degrees of confidence in e-eavesdropping existence, a first step might be to focus on the people who indicate they do not know how it happens or the ones who seem to be on the fence about whether

e-eavesdropping is happening or not. These people might be more open to correcting information on the topic compared to people who are more certain in their beliefs (Bode and Vraga, 2015).





## Conclusion

In sum, the current study is the first, to our knowledge, to examine internet users' surveillance beliefs about conversation-related advertising. People are aware that personalized communication is not a coincidence, but they have mixed beliefs about what data is used as input (e.g., offline conversations, digital traces) or what psychological mechanisms (e.g., priming) underlie perceptions of conversation-related advertising. Factors related to the experience (e.g., frequency of experience), individual difference factors (e.g., conspiracy mentality), and cross-cultural factors (US vs. Europe) provide some context to these variations, but more research is needed to systematically unravel people's beliefs and belief formation. The current study is a first step in examining this in the context of conversation-related advertising and serves as a stepping stone for future research in this area. Furthermore, the study serves as a starting point for a broader debate on digital literacy in the current age.

## Acknowledgments

The authors would like to thank Alicja Strycharz for their help with the Polish survey.

## ORCID iDs

Claire M Segijn  <https://orcid.org/0000-0002-2424-5737>  
 Joanna Strycharz  <https://orcid.org/0000-0001-7739-3349>  
 Anna Turner  <https://orcid.org/0000-0003-2963-7462>  
 Suzanna J Oprea  <https://orcid.org/0000-0001-7509-8311>

## Statements and declarations

### Funding

The research was funded with research funds from the Hubbard School of Journalism and Mass Communication, University of Minnesota.

### Conflicting interests

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

## Notes

1. OSF project [doi.org/10.17605/OSF.IO/YP5VD](https://doi.org/10.17605/OSF.IO/YP5VD) and preregistration <https://osf.io/x2daq> Note: The wording of the hypotheses has been adjusted, but the directions tested are as pre-registered.
2. Separate analyses were conducted because of a different  $n$  per variable (Table 4 and 5). For example, only respondents with conversation-related experience were asked to complete the

questions about frequency and time perception. Similarly, only respondents with second-hand experiences were asked about the frequency of these experiences.

## References

- Amnesty International (2022). Poland: Use of Pegasus spyware to hack politicians' highlights threat to civil society. Retrieved from: <https://www.amnesty.org/en/latest/news/2022/01/poland-use-of-pegasus-spyware-to-hack-politicians-highlights-threat-to-civil-society/>.
- Ball K and Webster W (2020) Big data and surveillance: Hype, commercial logics and new intimate spheres. *Big Data & Society* 7(1): 2053951720925853.
- Baruh L, Secinti E and Cemalcilar Z (2017) Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67(1): 26–53.
- Bode L and Vraga EK (2015) In related news, that was wrong: The correction of misinformation through related stories functionality in social media. *Journal of Communication* 65(4): 619–638.
- Boerman SC and Segijn CM (2022) Awareness and perceived appropriateness of synced advertising in Dutch adults. *Journal of Interactive Advertising* 22(2): 187–194.
- Bol N, Dienlin T, Kruikeimeier S, et al. (2018) Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication* 23(6): 370–388.
- Brandimarte L, Acquisti A and Loewenstein G (2013) Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4(3): 340–347.
- Brashier NM and Schacter DL (2020) Aging in an era of fake news. *Current Directions in Psychological Science* 29(3): 316–323.
- Bruder M, Haffke P, Neave N, et al. (2013) Measuring individual differences in generic beliefs in conspiracy theories across cultures: Conspiracy mentality questionnaire. *Frontiers in Psychology* 4: 225.
- Büchi M, Festic N and Latzer M (2022) The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society* 9(1): 20539517211065368.
- Büchi M, Fosch-Villaronga E, Lutz C, et al. (2023) Making sense of algorithmic profiling: User perceptions on Facebook. *Information, Communication & Society* 26(4): 809–825.
- Büchi M, Just N and Latzer M (2017) Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society* 20(8): 1261–1278.
- Christl W (2017) *Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Vienna: Cracked Labs: Cracked Labs.
- Cofer CN (1967) Conditions for the use of verbal associations. *Psychological Bulletin* 68(1): 1.
- Degli-Esposti S (2014) When big data meets dataveillance: The hidden side of analytics. *Surveillance and Society* 12(2): 209–225.
- Deibert RJ (2020) *Reset: Reclaiming the Internet for Civil Society*. London, UK: House of Anansi.
- European Commission (2019) Special Eurobarometer: The General Data Protection Regulation, 487a. Retrieved June 1 from <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=69701>.
- European Parliament (2022) Setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware. Retrieved September 8 from: [https://www.europarl.europa.eu/doceo/document/TA-9-2022-0071\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0071_EN.html).
- Ford JB, Mueller B and Mueller S (2023) Forty years of cross-cultural advertising research in the international journal of advertising: A bibliometric analysis. *International Journal of Advertising* 42(1): 119–127.
- Frick NR, Wilms KL, Brachten F, et al. (2021) The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications* 47: 101046.
- Gelman SA and Legare CH (2011) Concepts and folk theories. *Annual Review of Anthropology* 40(1): 379–398.
- Hasher L, Goldstein D and Toppino T (1977) Frequency and the conference of referential validity. *Journal of Verbal Learning and Verbal Behavior* 16(1): 107–112.
- Hunter T (2021) Ask Help Desk: No, your phone isn't listening to your conversations. Seriously. *Washington Post*. Retrieved June 1 from: <https://www.washingtonpost.com/technology/2021/11/12/phone-audio-targeting-privacy/>.
- Kim H and Huh J (2017) Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising* 38(1): 92–105.
- Koops BJ, Newell BC, Timan T, et al. (2016) A typology of privacy. *University of Pennsylvania Journal of International Law* 38: 483.
- Kröger JL and Raschke P (2019) Is my phone listening in? On the feasibility and detectability of mobile eavesdropping. In *Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, Proceedings* 33 (pp. 102–120). Springer International Publishing.
- Livingstone S (2003) On the challenges of cross-national comparative media research. *European Journal of Communication* 18(4): 477–500.
- Lyon D (2017) Digital citizenship and surveillance| surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication* 11: 19.
- Maslowska E, Smit EG and Van den Putte B (2013) Assessing the cross-cultural applicability of tailored advertising: A comparative study between the Netherlands and Poland. *International Journal of Advertising* 32(4): 487–511.
- Masur PK, Epstein D, Quinn K, et al. (2025) Comparative privacy research: Literature review, framework, and research agenda. *The Information Society* .41(2): 69–90.
- Nickerson RS (1998) Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology* 2(2): 175–220.

- Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79: 119.
- Penney JW (2021) Understanding chilling effects. *Minnesota Law Review* 106: 1451.
- Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY, USA: Suny Press.
- Potter WJ (2012) *Media Effects*. Sage publications.
- Ranzini G, Lutz C and Hoffmann CP (2023) Resignation in the face of agency constraints. In: Trepte S and Masur PK (eds) *The Routledge Handbook of Privacy and Social Media*. New York, NY: Routledge, 134–143.
- Reding V (2011) The upcoming data protection reform for the European union. *International Data Privacy Law* 1(1): 3–5.
- Segijn CM, Strycharz J, Riegelman A, et al. (2021) A literature review of personalization transparency and control: Introducing the transparency-awareness-control framework. *Media and Communication* 9(4): 120–133.
- Segijn CM, Strycharz J, Turner A, et al. (2024) Conversation-related advertising and electronic eavesdropping: Mapping perceptions of phones listening for advertising in the United States, The Netherlands, and Poland. *Social Media + Society* 10(4).
- Smalley S (2025) Apple says it does not use Siri audio for advertising. Retrieved January 29, 2025 from <https://therecord.media/apple-says-siri-audio-not-used-advertising>.
- Smit EG, Van Noort G and Voorveld HA (2014) Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* 32: 15–22.
- Statista (2023) Mobile advertising and marketing worldwide. Retrieved February 16, 2024 from <https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country>.
- Stevens A, Fussey P, Murray D, et al. (2023) ‘I started seeing shadows everywhere’: The diverse chilling effects of surveillance in Zimbabwe. *Big Data & Society* 10(1): 20539517231158631.
- Strycharz J and Segijn CM (2022) The future of dataveillance in advertising theory and practice. *Journal of Advertising* 51(5): 574–591.
- Sundar SS and Marathe SS (2010) Personalization versus customization: The importance of agency, privacy, and power usage. *Human Communication Research* 36(3): 298–322.
- Swami V, Chamorro-Premuzic T and Furnham A (2010) Unanswered questions: A preliminary investigation of personality and individual difference predictors of 9/11 conspiracist beliefs. *Applied Cognitive Psychology* 24(6): 749–761.
- Tidy J (2019) Why phones that secretly listen to us are a myth. Retrieved from: <https://www.bbc.com/news/technology-49585682>.
- Tushnet R and Goldman E (2020) *Advertising & Marketing Law: Cases & Materials*. Santa Clara: Faculty Book Gallery.
- Van Dijck J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208.
- Vitak J, Kumar PC, Liao Y, et al. (2023) Boundary regulation processes and privacy concerns with (non-) use of voice-based assistants. *Human-Machine Communication* 6(1): 10.
- Widdicks K, Remy C, Bates O, et al. (2022) Escaping unsustainable digital interactions: Toward “more meaningful” and “moderate” online experiences. *International Journal of Human-Computer Studies* 165: 102853.
- Yun JT, Segijn CM, Pearson S, et al. (2020) Challenges and future directions of computational advertising measurement systems. *Journal of Advertising* 49(4): 446–458.
- Zhang D, Boerman SC, Hendriks H, et al. (2023) A peak into Individuals’ perceptions of surveillance. In: *Advances in Advertising Research (Vol. XII) Communicating, Designing and Consuming Authenticity and Narrative*. Wiesbaden: Springer Fachmedien Wiesbaden, 163–178.
- Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.