Understanding public acceptance of data collection by intelligence services in the Netherlands

A factorial survey experiment

Oomens, E. C.; van Wegberg, R. S.; van Eeten, M. J.G.; Klievink, A. J.

DOI
10.1016/j.giq.2025.102077

Publication date
2025

Document Version
Final published version

Published in
Government Information Quarterly

Citation (APA)
Oomens, E. C., van Wegberg, R. S., van Eeten, M. J. G., & Klievink, A. J. (2025). Understanding public acceptance of data collection by intelligence services in the Netherlands: A factorial survey experiment. *Government Information Quarterly*, *42*(4), Article 102077. https://doi.org/10.1016/j.giq.2025.102077

Government Information Quarterly 42 (2025) 102077

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Understanding public acceptance of data collection by intelligence services in the Netherlands: A factorial survey experiment

E.C. Oomens *, R.S. van Wegberg, M.J.G. van Eeten, A.J. Klievink

Technology, Policy & Management, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, the Netherlands

ARTICLE INFO

Keywords:
Factorial survey experiment
Vignettes
Public opinion
Acceptance
Data collection
Intelligence services
National security

ABSTRACT

Intelligence services must balance values such as national security and privacy when collecting data, with each scenario involving specific contextual trade-offs. While citizens benefit from effective intelligence operations, they also risk having their rights infringed upon. This makes citizen perspectives on acceptable data collection for intelligence and national security salient, as their legitimacy is also contingent upon public support. Yet, important aspects of citizen perspectives are understudied, such as the influence of contextual factors related to the use of intelligence collection methods. This study, inspired by Nissenbaum's contextual integrity framework, uses a factorial survey experiment with vignettes among a representative sample of 1423 Dutch citizens to examine the influence of threat type, duration, data subject, collection method, data type, and data retention on public acceptance of surveillance. Additionally, the study considers the impact of respondents' trust and privacy attitudes. The findings reveal significant influence of both contextual variables – particularly threat type, data subject, and data retention – and respondent predispositions – particularly trust in institutions, trust in intelligence services' competence, and privacy concerns for others. The findings imply that more in-depth contextual knowledge among the public may foster support for intelligence activities.

1. Introduction

In democratic societies, the principles that guide and justify data collection by governments are generally codified in legal frameworks and enforced through oversight mechanisms. One domain where this is particularly salient and contentious is the data collection by intelligence services. On the one hand their data collection serves a critical objective: national security. On the other hand, data collection in this domain is seen as a form of surveillance that infringes upon privacy rights and reduces people's willingness to express opinions (Eck, Hatz, Crabtree, & Tago, 2021; Macnish, 2015). Finding a balance in intelligence collection entails making trade-offs between privacy and security. However, research has suggested that people are generally unwilling to compromise on privacy or security (Cayford, Pieters, & van Gelder, 2019; Pavone & Esposti, 2012).

Intelligence services do not have unrestricted autonomy to employ any method at any given time, as they must adhere to and account for a set of principles to justify their use of collection methods. The legal frameworks and oversight mechanisms specify such principles, including proportionality – the benefits of the activity and the value of the intelligence gathered must outweigh potential harms, such as privacy violations; necessity – the operation must be essential to achieving the desired outcome; subsidiarity – less intrusive methods must be unavailable or insufficient; and specificity – intelligence efforts should be directed at legitimate targets (Aerdts, 2023). However, legal frameworks are by necessity somewhat abstracted from the myriad contexts in which they need to be applied. This leaves intelligence practitioners and oversight bodies with a degree of discretion in interpreting and applying the rules, as each case presents its own specific circumstances and trade-offs.

Citizens do not make these operational decisions and typically do not directly hold intelligence services accountable. Yet, given what is at stake in terms of citizens' rights and freedoms, it is essential that intelligence services operate within established expectations, and that their practices are generally perceived as acceptable and justified by the citizens of the democratic legal order they seek to protect. After all, the legitimacy of state power in a democracy depends on public support. Moreover, while citizens benefit from effective intelligence operations, they also risk having their rights infringed upon – thus, intelligence practices inherently affect and concern them. This makes citizen

* Corresponding author.
E-mail address: e.c.oomens@tudelft.nl (E.C. Oomens).

https://doi.org/10.1016/j.giq.2025.102077
Received 30 October 2024; Received in revised form 26 August 2025; Accepted 5 September 2025
Available online 29 October 2025

perspectives on acceptable data collection for intelligence and national security salient. Yet, important aspects of citizen perspectives are understudied, such as the influence of contextual factors in the use of intelligence collection methods. This gap is addressed by this paper.

Research of citizen perspectives in this domain is complicated by the secretive nature of intelligence practices (Jaeger, Bertot, & McClure, 2003). Information available to the public is often limited to whistleblower revelations of scandals or official reports from intelligence agencies and oversight bodies, which are frequently redacted or supplemented with classified details. Consequently, the public has only a limited understanding of the "rules of the game" that dictate when, how, and why intelligence services operate (Hijzen, 2014). Thus, it is difficult for citizens to form an informed opinion and challenging for researchers to capture citizen views regarding intelligence practices – particularly given the multitude of contextual complexities that are not easily conveyed or made explicit.

Previous research on public acceptance of surveillance has predominantly examined broad support for government surveillance (e.g., Reddick, Chatfield, & Jaramillo, 2015; Valentino, Neuner, Kamin, & Bailey, 2020; Westerlund, Isabelle, & Leminen, 2021) or attitudes toward specific surveillance technologies (e.g., Ball, Degli Esposti, Dibb, Pavone, & Santiago-Gomez, 2019; Degli Esposti & Santiago Gómez, 2015; Hallinan & Friedewald, 2012; Kostka, Steinacker, & Meckel, 2021), as well as respondent attributes that influence attitudes. These studies provide insight into the predispositions that either heighten or mitigate concerns about surveillance. A much smaller portion of the literature has examined the influence of contextual factors on public perceptions regarding intelligence and surveillance practices (e.g., Offermann-van Heek, Arning, & Ziefle, 2019; Sulitzeanu-Kenan, Kremnitzer, & Alon, 2016; Trüdinger & Ziller, 2022). However, there is substantial evidence suggesting that public acceptance of data collection is strongly influenced by the contextual factors of said data collection, as demonstrated by research on privacy as contextual integrity (e.g., Martin & Nissenbaum, 2016, 2017, 2020; Trein and Varone, 2023). So, how does the public perceive the acceptability of various intelligence collection scenarios, and what factors – both contextual and respondent-related – drive this acceptability?

Moving beyond previous studies on surveillance acceptance and inspired by contextual integrity research, we focus on citizen perceptions of acceptability regarding the conditions of intelligence power deployment. In other words, an intelligence collection method (e.g. wiretapping, hacking) can be acceptable or unacceptable in a given threat context depending on contextual factors relating to its use; for instance, the type of data gathered, the people targeted, and the length and the scope of an operation may all influence whether intelligence practices are viewed as appropriate. Thus, our primary question is: How do contextual factors relating to the deployment of intelligence resources influence participants' acceptance of intelligence collection? Furthermore, acknowledging prior research on the significant influence of respondent characteristics (e.g., trust, privacy concerns) on public perceptions of surveillance, we also seek to explore: How do respondent characteristics affect their acceptance of intelligence practices? By integrating both contextual factors and respondent characteristics, we aim to establish a link between studies on individual predispositions and those examining the role of context in intelligence collection.

We use a factorial survey experiment in which participants (N = 1423) are presented with brief stories, or vignettes, depicting scenarios where data is collected by an intelligence service. Our study is conducted in the Netherlands. We systematically vary six factors – type of threat, timing of data collection, data subject, data collection method, data type, and data retention – to assess their impact on participants' overall acceptance ratings. This approach allows us to analyze the nuanced interplay of these factors in shaping public acceptance. Additionally, we examine how respondents' attitudes on trust and privacy influence acceptance ratings, along with other factors such as political orientation, news interest, and demographics. Lastly, we examine the interaction effects between threat type and data subject, as well as between collection method and data type.

2. Theory and hypotheses

In this section, we provide a theoretical discussion of various factors influencing the acceptance of intelligence collection, drawing on previous research into support for surveillance and data collection in other contexts. Balancing the imperatives of national security and individual privacy entails navigating what Nissenbaum (2010) terms contextual integrity: the socially embedded norms that specify who may access what information, by which means, for how long, and for what purposes. When an intelligence-gathering scenario diverges from these contextual expectations, by altering, for example, the threat type, number or nationality of data subjects, or retention period, citizens can experience it as a breach of privacy norms, lowering its legitimacy. Yet acceptance is not dictated by context alone. According to the *Antecedents-Privacy Concerns-Outcomes (APCO)* model (Smith, Dinev, & Xu, 2011), individuals' privacy-related outcomes, such as acceptance of data collection, are also shaped by their privacy concerns, which are influenced by factors like prior privacy experiences and demographic characteristics. Drawing on the privacy-calculus theory (Dinev, Hart and Mullen, 2008; Smith et al., 2011), individuals also weigh the anticipated security benefits of surveillance against perceived privacy risks. This cost-benefit analysis is complicated by the secretive nature of the intelligence domain, making it difficult for citizens to assess the true benefits and risks (Acquisti & Grossklags, 2005). As a result, individuals may rely on predispositions such as institutional trust, personal privacy attitudes, and broader surveillance concerns to navigate this uncertainty (Trüdinger & Steckermeier, 2017).

Together, contextual-integrity theory and concepts from the APCO model provide the lens for the analyses that follow. Based on this lens, this section develops theoretical hypotheses that this study answers. The first subsection examines how *contextual factors* linked to the deployment of specific intelligence powers modulate public acceptance. The second subsection turns to *individual predispositions* – trust, privacy attitudes, and surveillance concerns, that tilt the privacy calculus toward or away from acceptance. Finally, we consider the impact of additional variables, such as demographic characteristics, on perceptions of intelligence gathering.

2.1. Influence of contextual factors related to deployment of intelligence powers

Intelligence agencies have a variety of methods and technologies at their disposal for collecting intelligence. However, not every situation warrants the same approach. Urgent, high-stakes scenarios, for example those where lives are at risk, may justify more intrusive methods compared to situations where the stakes are less clear-cut. Therefore, the appropriateness of intelligence collection heavily depends on the context of the situation. This is demonstrated by several studies that have examined the influence of contextual factors on support for surveillance (e.g., Arsenault, Kreps, Snider, & Canetti, 2024; Jardine, Porter, & Shandler, 2024; Potoglou, Dunkerley, Patil, & Robinson, 2017; Snider, Hefetz, Shandler, & Canetti, 2025; Trüdinger & Ziller, 2022). For example, findings from Trüdinger and Ziller (2022) indicate that the severity and target of an attack significantly affect support levels, with attacks that result in death (as opposed to injuries) and those targeting civilians (as opposed to politicians) increasing support. In contrast, the timeframe and method of attack showed no significant effect. Our research delves deeper into the contextual factors related to the use of investigatory powers, acknowledging that their deployment does not occur in a vacuum. Instead, their acceptability depends on a complex interplay of factors, including the nature, source, and handling of the data collected, as well as the motivations driving the investigation.

Our study draws inspiration from Nissenbaum's framework of

privacy as contextual integrity (Nissenbaum, 2010). It is a theory of privacy which posits that the appropriateness of data collection is largely dependent on factors relating to the context, such as how data is collected and by whom. The contextual integrity framework suggests that informational norms guide people's expectations regarding how data should flow within a specific context. These norms are shaped by five key parameters: the type of information, the subject (to whom the information pertains), the sender (who shares the information), the recipient (who receives the information), and the transmission principle (conditions under which information dissemination occurs). Together, these parameters define the "what," "how," and "who" of a data dissemination scenario. Additionally, data inference (what the data reveal) and the purpose for which the data are used can shape information norms. If any of these parameters do not meet the informational norms, the appropriateness of the data flow decreases (Nissenbaum, 2010).

Given that previous studies have demonstrated that these contextual parameters influence perceived appropriateness of data collection across various settings (e.g., Gilbert, Vitak, & Shilton, 2021; Martin & Nissenbaum, 2020; Roeber, Rehse, Knorrek, & Thomsen, 2015; Vitak et al., 2023; Vliegenthart et al., 2024), it is not unreasonable to suggest that similar factors affect perceptions of intelligence collection. However, intelligence collection distinguishes itself from other data collection contexts due to its high stakes and potential benefits (i.e., the protection of national security), which could lead to greater acceptance of certain data practices compared to other contexts. For example, Vitak et al. (2023) found that Dutch citizens were less concerned about data collection by law enforcement compared to other entities like online data brokers or local government agencies. Similarly, data collection aimed at combating terrorism generated fewer concerns than efforts focused on other purposes, such as reducing binge drinking. On the other hand, the inherent risks, potential infringements, and secrecy associated with intelligence collection can have serious individual and societal repercussions, which can foster criticism and distrust. Moreover, intelligence agencies operate differently from other law enforcement bodies such as the police, utilizing distinct methods and pursuing unique objectives, which can further complicate public perceptions (Oomens, van Wegberg, Klievink, & van Eeten, 2023).

In our study, we consider six factors inspired by the contextual integrity parameters, which are detailed further in section 3.2. The first factor we include is the *type of threat* that is being investigated. Threat type captures the purpose of intelligence collection, which determines the stakes. According to the principle of proportionality, more intrusive measures may be more justified when stakes are high and potential benefits outweigh potential harms. Prior research has shown that the acceptance of data collection and willingness to share data may vary depending on the specific purpose behind collection (Gilbert et al., 2021; Trein & Varone, 2023; Vitak et al., 2023), with some purposes deemed more legitimate than others. We therefore expect that public acceptance will vary across different threat types.

Hypothesis 1. *Different threat types are associated with varying levels of public acceptance.*

Intelligence agencies monitor a wide array of threats, ranging from terrorism to espionage, sabotage, and foreign interference. However, previous research on support for surveillance and willingness to trade civil liberties for security has predominantly focused on terrorism-related threats (e.g., Conrad, Croco, Gomez, & Moore, 2018; Davis & Silver, 2004; Finkelstein et al., 2017; Garcia & Geva, 2016; Han, Kim, & Gordon, 2024; Trüdinger & Ziller, 2022), while other threats have received less attention (e.g., Dvir, Geva, & Vedlitz, 2023). Other threats investigated by intelligence agencies are often less known to the public or citizens mistakenly assume that intelligence services deal with issues that are actually the responsibility of police forces, such as combating crime (Del-Real & Díaz-Fernández, 2022). In addition, perceptions of probability and severity differ across threats: terrorist attacks are generally seen as more likely and more severe than, for instance, cyber-attacks (Dvir et al., 2023). Accordingly, we expect terrorism-related scenarios to elicit higher acceptance than other threat types.

Hypothesis 2. *Intelligence scenarios involving terrorism as threat type are associated with higher public acceptance than scenarios with other threat types.*

The other five factors relate to the way intelligence is gathered. The second factor we include is the *duration* of collection. Intelligence operations can range from short-term investigations to long-term surveillance. In some cases, data may be gathered systematically, as exemplified by the NSA's PRISM program (Greenwald & MacAskill, 2013). As noted in previous research, extended surveillance can uncover information that short-term surveillance cannot, such as individual's habits and other patterns in behavior (Martin & Nissenbaum, 2020). Furthermore, it has been suggested that extended collection periods and data retention are generally less acceptable to the public (Potoglou et al., 2017). Based on these insights, we hypothesize the following:

Hypothesis 3. *Intelligence collection with a longer duration is associated with lower public acceptance than intelligence collection with a shorter duration.*

The third factor is the *data subject* of the intelligence collection. Previous research indicates that public support for state surveillance increases when it targets potential criminals rather than the general populace (Ziller & Helbling, 2021). This suggests that acceptance of intelligence collection is influenced by the specificity of the target, with targeted collection aimed at legitimate suspects seen as more appropriate than indiscriminate surveillance of a broad population.

Hypothesis 4. *Intelligence collection of fewer data subjects is associated with higher public acceptance than intelligence collection of more data subjects.*

Similarly, the origin of the data subject may influence support. There is some evidence that people are less willing to accept reductions in civil liberties when the source of a terrorist attack is domestic as opposed to transnational, regardless of the level of threat (Garcia & Geva, 2016). Consequently, we propose the following hypothesis:

Hypothesis 5. *Intelligence collection of foreign data subjects is associated with higher public acceptance than intelligence collection of domestic data subjects.*

Fourth, we include the *collection method* itself. This dimension relates to the contextual integrity parameter *transmission principle*, which suggests that the conditions of collection matter in determining the appropriateness of information flow (Nissenbaum, 2010). For instance, data can be collected because it is voluntarily shared by the data subject, but also through coercion and stealing. By law, some intelligence collection methods (e.g., hacking) are considered more intrusive and are subject to stricter checks-and-balances than others (e.g., open-source intelligence) (Aerdts, 2023). Hacking, for instance, can be used to extract information without the owner's knowledge, while open-source intelligence typically involves collecting data that everyone can access. Though we might expect citizen perceptions to mirror this perceived intrusiveness pattern from legislation, it should be noted that reality is more complex, as data from open sources can be sensitive and involuntarily shared as well (Oomens et al., 2023). Thus, we propose hypothesis 6:

Hypothesis 6. *Different methods of intelligence collection are associated with varying levels of public acceptance.*

The fifth factor is the *type of data* collected. Certain data types are considered more sensitive than other data (Schomakers, Lidynia, Müllmann, & Ziefle, 2019) and a higher data sensitivity has been found to reduce surveillance acceptability (Nam, 2018). For instance, collecting the content of conversations has been found to be perceived as more

sensitive than the websites one has visited or what someone has searched on the internet (Nam, 2018). However, contextual integrity research also shows that the sensitivity of information varies strongly per context (Martin & Nissenbaum, 2016). We hypothesize the following:

Hypothesis 7. *The collection of different data types is associated with varying levels of public acceptance.*

Sixth, we include *data retention*. Previous research has found that data retention practices influence data collection acceptance (Martin & Nissenbaum, 2020), with findings suggesting a preference for minimal data storage (Potoglou et al., 2017). In the Netherlands, there have been controversies surrounding the storage of information by intelligence services, with data security cited as a primary argument for limiting the data that is stored (e.g., Hulsen, 2022). Additionally, Ziller and Helbling (2021) found that concerns about data security reduce support for state surveillance. Accordingly, we propose hypothesis 8:

Hypothesis 8. *Intelligence collection where data is stored in full is associated with lower public acceptance than intelligence collection where data is filtered, and irrelevant information is destroyed.*

2.2. Influence of trust, privacy attitudes, and surveillance concerns

Acceptance of data collection is not only influenced by contextual factors. Beyond contextual integrity, other privacy models exist that emphasize the role of individual characteristics in shaping perceptions of data collection. For instance, the *Antecedents-Privacy Concerns-Outcomes (APCO)* macro model (Smith et al., 2011) posits that privacy-related outcomes, such as individuals' willingness to disclose information or accept data collection, are influenced by the level of privacy concerns they experience. These concerns are in turn shaped by factors such as previous privacy experiences, privacy awareness, and demographic characteristics.

In the APCO model, trust is understood as influential in determining privacy-related outcomes, though its precise relationship to these outcomes – whether as a mediator, moderator, or antecedent – is unclear (Smith et al., 2011). Regarding surveillance, there is robust evidence that trust influences acceptance. Generally, a higher level of trust in institutions correlates with more positive attitudes toward surveillance policies and technologies (Ball et al., 2019; Budak & Rajh, 2018; Liu, 2021; Nam, 2018, 2019; Svenonius & Björklund, 2018; Thompson, McGill, Bunn, & Alexander, 2020; Trüdinger & Steckermeier, 2017; Valentino et al., 2020). We therefore expect a positive relation between participants' general trust in institutions and support.

Hypothesis 9. *Higher levels of general institutional trust are associated with higher acceptance of intelligence collection.*

Li (2024) suggests that institutional trustworthiness hinges on three aspects: ability, benevolence, and integrity. According to Li, ability refers to skills, expertise, and knowledge in institutions. Institutions that are competent are also more likely to be effective in achieving their goals. Benevolence is the degree to which institutions are perceived to act in the public interest rather than their own. Integrity denotes the consistency of institutions in adhering to principles, including social norms and moral values (Li, 2024). These three aspects of institutional trustworthiness are expected to all play a role but likely influence acceptance differentially. Accordingly, we expect that higher trust in intelligence agencies – rooted in perceptions of their competence and integrity – translates into greater acceptance of intelligence collection by those agencies.

Hypothesis 10. *Higher levels of trust in intelligence agencies are associated with higher acceptance of intelligence collection.*

Simultaneously, oversight bodies play a crucial role in checking intelligence services and preventing power abuse. Oomens et al. (2023) show that for some of their participants, trust in these checks and balances is more influential than trust in the intelligence services themselves, as oversight is seen to hold agencies accountable and to "force" them to be critical and take responsibility. Thus, effective oversight mechanisms may alleviate public concerns about intelligence collection. We therefore expect trust in oversight to foster acceptance.

Hypothesis 11. *Higher levels of trust in oversight are associated with higher acceptance of intelligence collection.*

There is strong evidence that individuals with greater privacy concerns are less accepting of surveillance. Prior studies consistently find that people who worry more about the collection, use, or misuse of personal data show lower levels of support for surveillance measures (Dinev, Hart, & Mullen, 2008; Kininmonth, Thompson, McGill, & Bunn, 2018; Thompson et al., 2020). We propose the following hypothesis:

Hypothesis 12. *Greater privacy concerns are associated with lower acceptance of intelligence collection.*

Privacy concerns are closely related to surveillance concerns. Individuals with "negative views about the gathering and processing of personal information and monitoring of online behavior by the government" are less accepting of surveillance (Dinev et al., 2008; Nam, 2018). Therefore, we anticipate that respondents with heightened surveillance concerns will be less likely to accept the intelligence collection scenarios presented.

Hypothesis 13. *Greater surveillance concerns are associated with higher acceptance of intelligence collection.*

Lastly, the privacy-security trade-off framework posits that a degree of intrusion upon privacy and other fundamental rights is necessary to achieve a higher level of security (Davis & Silver, 2004; Trüdinger & Ziller, 2022). This trade-off implies that the more importance individuals attach to privacy, the less willing they may be to accept surveillance practices that intrude upon it – especially when the security benefits are uncertain or abstract. We propose the following hypothesis:

Hypothesis 14. *Higher perceived importance of privacy is associated with lower acceptance of intelligence collection.*

2.3. Context of the Netherlands

Our research is set in the Netherlands, an EU member state with two intelligence agencies: the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). In recent years, there has been ongoing public debate surrounding the Intelligence and Security Services Act from 2017 (Wiv 2017), which outlines the powers of both services and the checks-and-balances around their operations. This debate gained significant attention during a 2018 consultative referendum, in which the Dutch public could vote for or against the law, which granted the services new powers for extensive data collection as well as introducing new oversight mechanisms. Discussions have persisted, particularly among professionals in the field (Oomens et al., 2023). News outlets frequently report on conflicts between oversight bodies and intelligence agencies, as well as irregularities and legal changes (e.g., Hulsen, 2022). This ongoing visibility in the public discourse, coupled with the Netherlands' strict compliance with GDPR regulations, may lead Dutch citizens to be more attuned to privacy and data-related issues in the context of intelligence services.

3. Methodology

The goal of this study is to explore how citizens perceive the acceptability of various intelligence collection scenarios and how these perceptions are influenced by contextual factors related to the collection process, as well as participants' individual characteristics, such as demographics and attitudes. To achieve this, we administered a factorial

survey experiment with vignettes among a sample of 1423 participants that is representative of the Dutch population. In this method, participants are presented with a series of vignettes – short, hypothetical yet real-world stories with factors (i.e., dimensions) that are systematically varied – that they must evaluate. This allows us to explore how changes along these dimensions affect respondents' evaluations.

Factorial surveys are widely used in sociological research to investigate the underlying principles behind human judgments (Wallander, 2009). Factorial survey and choice experiments have also been commonly used in technology and privacy research to study participants' judgments on multidimensional phenomena, such as their acceptance of technology use and data collection practices in different contexts (e.g., Gilbert et al., 2021; Horvath, James, Banducci, & Beduschi, 2023; Martin, 2012; Martin & Nissenbaum, 2020). Traditional survey approaches, which rely on self-reporting and direct questions, have long been found prone to various response biases, such as social desirability bias, acquiescence bias, and satisficing (Hainmueller, Hangartner, & Yamamoto, 2015; Schwarz, 1999). Such biases can undermine the validity of survey results. Research suggests that vignette and other survey experiments (e.g., conjoint) are less susceptible to these types of biases, thereby proving to be more reliable (Hainmueller et al., 2015).

3.1. Survey procedure

Participants were recruited via the LISS panel (Longitudinal Internet studies for the Social Sciences) during February 2024. The LISS panel is managed by non-profit research institute Centerdata (Tilburg University, the Netherlands) and is based on a true probability sample of Dutch households drawn from the population register by Statistics Netherlands (Scherpenzeel & Das, 2010). The panel consists of approximately 7500 individuals who participate in monthly questionnaires. Participants complete the surveys online, always in the same lay-out style, and receive compensation for their participation.

The survey was sent to a total of 2000 LISS panel members, who are randomly sampled from the larger population of panel members. The response rate was 82,6 %, meaning that a total of 1652 people participated in the survey. We excluded participants with missing data and respondents suspected of speeding. Our final sample consisted of 1423 respondents.

Demographic data on sex, age category, and education level were provided by Centerdata. The demographics of our final sample of participants are summarized in Table 1. The table also shows how the variables were coded. Previous research has demonstrated that matching the characteristics of a survey sample to the target population as closely as possible is crucial for drawing externally valid conclusions from survey experiments (Hainmueller et al., 2015). Therefore, recruiting a sample representative of the Dutch population was a priority. Compared to the overall population of Dutch people, older age categories are overrepresented in our sample, while younger age categories are underrepresented. Furthermore, there is an overrepresentation of individuals with higher education levels.

At the beginning of the survey (see Appendix A for the full survey instrument), participants were given a brief explanation of the roles and responsibilities of the AIVD (the General Intelligence and Security Service of the Netherlands) to ensure they were informed about the agency's nature and primary objectives. This was done to minimize misunderstandings and avoid inconsistent interpretations of what an intelligence agency is and does, as previous research has shown that public knowledge of intelligence agencies is generally low (Del-Real & Díaz-Fernández, 2022). Respondents were then asked to express their level of agreement with a series of statements regarding their privacy attitudes and trust using a 5-point Likert scale. These questions were positioned ahead of the vignette valuations to minimize the potential influence of the vignettes on participants' trust and privacy ratings. Their operationalization is further discussed in section 3.5.

Table 1
Distribution of sex, age and education level in the sample ($N = 1423$).

		N	Dutch population
Sex	0. Male	712 (50.0 %)	49.7 %
	1. Female	711 (50.0 %)	50.2 %
Age	0. 18–24 years	102 (7.2 %)	8.9 %
	1. 25–34 years	160 (11.2 %)	13.0 %
	2. 35–44 years	158 (11.1 %)	12.0 %
	3. 45–54 years	210 (14.8 %)	13.5 %
	4. 55–64 years	270 (19.0 %)	13.8 %
	5. 65 years and older	523 (36.8 %)	20.2 %
Education level	0. primary school	70 (4.9 %)	8.6 %
	1. vmbo (intermediate secondary education)	226 (15.9 %)	17.7 %
	2. havo/vwo (higher secondary education/preparatory university education)	151 (10.6 %)	9.6 %
	3. mbo (intermediate vocational education)	323 (22.7 %)	32.1 %
	4. hbo (higher vocational education)	410 (28.8 %)	20.1 %
	5. wo (university)	243 (17.1 %)	11.9 %

Note. Source: CBS StatLine (2022a, 2022b).

Next, participants were randomly assigned to a set of six vignettes, with each vignette describing a situation with the same structure. Within each vignette, the following six dimensions were varied: (1) threat type, (2) duration, (3) data subject, (4) collection method, (5) data type, and (6) data retention. Participants rated the acceptability of each vignette on a 7-point Likert scale, ranging from very unacceptable to very acceptable. The choice and operationalization of the vignette dimensions and levels are further detailed in section 3.2.

Upon completing the survey, participants were asked to evaluate its clarity and understandability using a 1–5 Likert scale. They were then debriefed and thanked for their participation. On average, participants were neutral regarding the difficulty of the questions ($M = 2.70$, $SD = 1.46$). They found the questions clear ($M = 4.04$, $SD = 0.97$) and perceived the topic as both interesting ($M = 3.80$, $SD = 1.05$) and thought-provoking ($M = 3.56$, $SD = 1.18$). The estimated duration to complete the survey was 10 min. Demographic data were provided by Centerdata. Subsequently, the dataset was combined with a selection of variables from the LISS Politics & Values questionnaire wave 16, which is part of the LISS Core Study, a longitudinal survey about a broad range of social topics (Elshout, 2024).

3.2. Choice of vignette dimensions and levels

The dimensions for our vignettes were determined based on a review of existing literature, as outlined in Section 2.1. We settled on six dimensions to vary within the vignettes: (1) threat type, (2) duration, (3) data subject, (4) collection method, (5) data type, and (6) data retention. In this section we will elaborate on the operationalization of the vignette variables. An overview of all the dimensions and levels is presented in Table 2.

3.2.1. Threat type

The first dimension, threat type, was included to provide participants with a purpose for the data collection. Intelligence services investigate a range of threats, each with varying levels of urgency and visibility. We

Table 2
Overview of vignette dimensions and levels.

Dimension	Levels
Threat type	1. a terrorist attack is being planned on a Dutch target 2. attempts are being made to steal trade secrets from a Dutch company 3. disinformation is spread with the aim of influencing Dutch citizens 4. digital attacks are taking place with the goal of causing disruptions in the electricity network in the Netherlands
Duration	1. once 2. for three months 3. systematically
Data subject	1. a few residents of the Netherlands 2. a few residents of a country outside the European Union 3. thousands of residents of the Netherlands 4. thousands of residents of a country outside the European Union
Collection method	1. collected the information by searching on the internet (for example, leaked datasets, social media, and internet forums) 2. received the information from a foreign intelligence service 3. received the information from an informant (this can be either a person or an organization) 4. requested the information from another organization (for example, a municipality, bank, or internet provider) 5. gathered the information by hacking a device (breaking into a computer) 6. collected the information by wiretapping an internet connection
Data type	1. passenger data from air travel, such as passport and flight information. This information can be used to infer where someone has travelled and when. 2. contact details from chat and email services. This information can be used to the infer with whom someone is in contact and when. 3. communication between individuals. This information can be used to infer someone's motivations and beliefs. 4. internet traffic. This information can be used to infer what someone does on the internet.
Data retention	1. Only data useful to the investigation is retained. The remaining information is destroyed. 2. All collected information is retained.

included four threat types that have been part of the public discourse in the Netherlands but differ in visibility – potentially affecting citizens' sense of urgency and feelings of threat. Therefore, these different threats may correlate with varying levels of acceptance. The first two threat types, *terrorism* and *cyber-attacks,* represent collective safety concerns, though they manifest differently – terrorism is visible and familiar, while cyber-attacks are more invisible and relatively new to the public. The third threat type, *theft of trade secrets*, pertains to economic and knowledge security and might be perceived differently due to its less immediate impact on collective security compared to a terrorist attack. Lastly, the spread of *disinformation* presents ambiguous immediate consequences, potentially resulting in lower perceived urgency.

3.2.2. Duration

The second dimension, duration, was added because previous research shows that when duration is not explicitly mentioned, participants tend to judge scenarios as more acceptable compared to scenarios that do contain an indication of time, even if the duration is only 'a few minutes' (Martin & Nissenbaum, 2020). We specified three levels for this dimension: *one time only*, *for three months*, and *systematically*. These time periods are based on the specifications in Dutch law, where Dutch intelligence services typically receive permission to collect data for a three-month period, after which they must request an extension.

3.2.3. Data subject

The third dimension, data subject, was inspired by the theory of privacy as contextual integrity. As mentioned in Section 2.1, contextual integrity suggests that the norms surrounding information flow are related to five parameters: *information type*, *transmission principle*, and three actor-related parameters: *data receiver*, *sender*, and *subject* (Martin & Nissenbaum, 2020). The receiver, the actor that ultimately obtains the information, remains constant across vignettes, because in each scenario the same Dutch intelligence agency (AIVD) is the receiver of the data. We chose the AIVD as sole receiver, as this is the intelligence agency best known to Dutch citizens. The sender, the actor providing the data, is integrated into the collection method dimension, as the AIVD sometimes collects its own intelligence and at other times receives information from informants or foreign intelligence services. The data subject, the actor whose information is collected, was included as a separate dimension, as the 'target' of intelligence gathering varies per case.

In selecting the dimension levels, we focused on two aspects: the *specificity* of data collection and the *origin* of the data subject. We distinguished between highly targeted data collection involving only a few subjects and collection in bulk from thousands of people at the same time. Additionally, we differentiated between Dutch residents and individuals residing outside the European Union. We included a sentence emphasizing that data subjects may include potential suspects, victims, or individuals associated with suspects and/or victims. This addition was informed by observations during the pilot phase, where participants interpreted the data subject differently – some assumed a random individual, while others assumed a suspect. To mitigate potential confounding variables, we standardized this aspect across vignettes while retaining a degree of ambiguity by design.

Unlike previous research (e.g., Martin & Nissenbaum, 2016), which often uses the participant as the data subject (i.e., 'your data is being collected'), we chose not to do this. Discussions on data collection by intelligence agencies often lack clarity regarding whose data is being collected. However, one would assume that intelligence services are most interested in information about people related to their investigations rather than most regular citizens, though their data could be part of larger datasets.

3.2.4. Collection method

The fourth dimension, collection method, specifies how the AIVD obtains information in the scenarios. Previous research suggests that people feel more comfortable with the collection of data that is voluntarily shared or already public, as opposed to private data (Gilbert et al., 2021). Therefore, we focused on including different sources and methods for obtaining publicly available or private information. Furthermore, as mentioned, we included different senders, the actors providing the data, in this dimension.

We specified six levels for this dimension, aligning with intelligence powers outlined in Dutch law (Wiv 2017): collection by the intelligence service through *searching the internet*, *hacking*, or *wiretapping an internet connection*, and receiving data from a *foreign intelligence service*, *informant*, or *another organization*. The levels reflect various degrees of assumed intrusiveness. For example, open-source intelligence (i.e., searching the internet) and data acquisition via third parties (e.g., informants) are typically perceived as less intrusive, since those data are publicly available or collected through standard procedures. Conversely, hacking and wiretapping are generally considered more intrusive and are subject to strict and tightened oversight within the Dutch system of checks-and-balances (Oomens et al., 2023).

3.2.5. Data type

For the fifth dimension, data type, we found it important to include not only the type of information that was collected but also what can be inferred from said information. Previous research has found that data inference is an important factor to include, as it provides participants with clarity on what can be learned from different kinds of information and helps them make better informed judgments (Martin & Nissenbaum, 2020).

Since much of the work of intelligence services is secretive, we based the four levels of this dimension on known data types from reports and other public sources (e.g., CTIVD, 2020). We aimed to align these levels

with data categories encompassing location, network, and content, which form significant facets of intelligence gathering. Much of the intelligence amassed by intelligence services relates to these elements, shedding light on where a target has been, their social connections, and their motivations. The four data types included are *passenger*, *contact*, *communication*, and *internet traffic* data. For each level, we included a sentence that specified the data inference, clarifying what kind of information the AIVD could derive from the data.

3.2.6. Data retention

Lastly, data retention was included as a dimension to provide context on what happens to the data after collection, specifically whether all data is used and stored or only a limited amount. We chose two levels for this dimension: *full retention*, where data is not filtered and everything is stored, and *partial retention*, where some form of filtering has been applied.

The vignettes were originally presented to participants in Dutch and have been translated to English for the purposes of this paper (Appendix B). The following is a translated example of the vignettes, with added bracketed numbers denoting the corresponding dimensions:

> The AIVD has received indications that [1] *a terrorist attack is being planned on a Dutch target*. That is why the AIVD gathers information [2] *systematically* from [3] *a few residents of the Netherlands*. These residents may include people who are suspected of involvement, or who may be victims, or who have dealings with those involved or victims. The AIVD has [4] *requested the information from another organization (for example, a municipality, bank, or internet provider)*. It concerns [5] *passenger details from air travel, such as passport and flight information. This information can be used to infer where someone travelled and when*. [6] *All collected information is retained*.

3.3. Vignette design

Combining all possible level combinations ($4 \times 3 \times 4 \times 6 \times 4 \times 2$) as depicted in Table 2 led to a total of 2.304 combinations (i.e., a *full factorial* design). It is common practice to use blocking techniques to sample a subset of vignettes (*fractional factorial*) from the full factorial design. This approach is necessary to prevent participants from having to evaluate all possible vignette combinations, as doing so would require an unrealistically large respondent sample (Auspurg & Hinz, 2015). The most commonly used blocking technique is random sampling (Wallander, 2009), although its use has been declining in recent years (Treischl & Wolbring, 2022). Random sampling has been criticized for potentially causing imbalances and confounding main and interaction effects (Auspurg & Hinz, 2015; Dülmer, 2007; Treischl & Wolbring, 2022).

Given these limitations, we opted for *D-efficient sampling*, as recommended by Auspurg and Hinz (2015). D-efficient sampling is regularly applied in recent survey experiments (e.g., Jeune, Juhel, Dessus, & Atal, 2024; Kustosch, Gañán, van't Schip, van Eeten, & Parkin, 2023; Seehuus, 2023; Trüdinger & Ziller, 2022) and has several key advantages. First, D-efficient sampling minimizes the confounding of parameters within vignette decks and optimizes the balance and orthogonality of main and interaction effects (Auspurg & Hinz, 2015; Treischl & Wolbring, 2022). Second, it allowed us to control which specific interaction terms were included in the design, ensuring that these interactions were adequately represented in the final sample. Third, predefined vignette blocks provided the most practical solution in our collaboration with the LISS panel.

We used freeware macro %Mktex within software package SAS studio for D-efficient sampling of the vignettes (Kuhfeld, 2010). We constructed a design of 20 sets (or blocks), where each set consisted of 6 vignettes. Thus, in total 120 unique vignettes were rated by participants. The D-efficiency score was 93.06, which aligns with established recommendations and offers sufficient statistical power (Auspurg & Hinz, 2015). Higher D-efficiency scores signify a more robust design, with 100 indicating the maximum possible efficiency.

Participants were randomly allocated to one of the 20 sets of 6 vignettes. After excluding respondents with missing data, each vignette was rated by at least 58 individuals. To counteract order effects, the order of the vignettes within each block was randomized for every respondent. We furthermore ensured that in every set, each dimension level appeared at least once over the 6 vignettes, so that every participant would encounter all dimension levels at least once in one of the vignettes. Finally, we ensured that combinations of dimension levels occurred equally often over the entire sample of 120 vignettes. A total of 8538 vignettes were rated by 1423 respondents.

3.4. Dependent variable

For each vignette, respondents were asked to rate its acceptability. Acceptance was measured using the question: *How unacceptable (in other words: unreasonable, not okay) or acceptable (in other words: reasonable, okay) do you find this situation?* Answers ranged from 1 (very unacceptable) to 7 (very acceptable) with 4 (neither unacceptable nor acceptable) indicating a neutral position.

3.5. Respondent variables

Before evaluating the vignettes, respondents were asked about their privacy attitudes and trust. We included seven independent variables that pertained to participants general attitudes: (1) privacy importance, (2) privacy concerns for self, (3) privacy concerns for others, (4) surveillance concerns, (5) trust in the competence of the AIVD, (6) trust in the integrity of the AIVD, and (7) trust in oversight. See Table 3 for the operationalization. The included privacy and surveillance attitudes were inspired by previous research (Nam, 2017, 2018, 2019). Additionally, we distinguished between trust in integrity and trust in competence, since previous research suggests that institutional trust depends on these different aspects (Li, 2024). Participants were shown statements and indicated their agreement on a Likert scale, ranging from 1 (completely disagree) to 5 (completely agree).

Participants' general trust in various governmental and non-governmental institutions was measured using the question: *Can you indicate, on a scale from 0 to 10, how much trust you personally have in each of the following institutions?* Answer categories ranged from 0 (no trust at all) to 10 (full trust). The included institutions were the Dutch government, parliament, legal system, police, politicians, political parties, media, army, education, science, and democracy. The items formed a reliable scale (Cronbach's alpha = 0.93) and were combined into a composite variable, *trust in institutions* ($M = 5.69$, $SD = 1.58$).

Additionally, we included controls for participants' self-identified political orientation and interest in the news. First, *political orientation* was based on self-placement on an 11-point left-right scale, relying on the following question: *Where would you place yourself on a political scale, where 0 means left and 10 means right?* ($M = 5.30$, $SD = 2.38$). Second,

Table 3
Operationalization and mean scores for respondent variables.

Variable	Statement	M	SD
Privacy importance	I think privacy is important.	4.32	0.63
Privacy concerns self	I am concerned about my privacy.	3.34	0.95
Privacy concerns others	I am concerned about the privacy of others.	3.12	0.98
Surveillance concerns	I am afraid the government is spying on me.	2.43	0.98
Trust competence	I trust that the AIVD is good at its work.	3.84	0.75
Trust integrity	I trust that the AIVD will adhere to the rules that apply to it.	3.77	0.85
Trust oversight	I trust that the AIVD is properly supervised.	3.72	0.86

news interest as measured by the following question: *Are you very interested in the news, a little interested or not interested?* With answer categories (1) very interested, (2) a little interested, (3) not interested ($M = 1.53$, $SD = 0.58$). We also controlled for the demographics age, sex, and education level.

3.6. Pilot study

A pilot study was carried out using Qualtrics, involving a convenience sample of 34 participants. The aim was to evaluate the survey's functionality and assess the participants' comprehension of the vignettes. For each vignette, participants were asked to rate them on realism and understandability. If vignettes were rated as unrealistic or unclear, respondents were asked why they thought so. The pilot phase did not reveal significant issues, and the changes made were primarily related to rephrasing and adjustments to response scales. We also decided to remove some vignette levels to reduce the number of total combinations. The prototype vignettes underwent further testing with volunteers in an iterative manner to address any remaining points of interest. Researchers from Centerdata conducted a thorough analysis of the survey, resulting in simplified phrasing to meet Dutch language level B1. This adjustment ensures that individuals with varying reading abilities can comprehend the survey more easily.

3.7. Data analysis

Given that each respondent evaluated multiple vignettes, our data were hierarchical with vignettes nested within respondents. Therefore, we ran multilevel models with maximum likelihood estimation using the LME4 package in .R (Bates, Mächler, Bolker, & Walker, 2015). Specifically, we utilized multilevel regressions with random intercepts to test the main effects of vignette dimensions and respondent variables on the dependent variable, *vignette acceptance*. Vignette dimensions were used as explanatory categorical variables, and the dependent variable was treated as continuous. Random intercepts were included to account for individual differences between participants. Additionally, we conducted a multilevel analysis to examine interaction effects among several vignette dimensions. Our model-building approach was step-wise: we began with a baseline random intercept model, then sequentially added vignette dimensions, control variables, and respondent variables, assessing whether each addition significantly improved model fit. Finally, we included possible interaction terms to evaluate their impact on model fit.

4. Results

We conducted a factorial survey experiment with vignettes to answer the following research question: How do contextual factors relating to the deployment of intelligence resources influence participants' acceptance of intelligence collection? And: How do respondent characteristics affect their acceptance of intelligence practices? In Section 4.1, we examine the results from a multilevel regression model with a random intercept. First, the findings for the dependent variable, vignette acceptance, are discussed. Next, we assess the main effects of each vignette dimension on vignette acceptance, followed by an analysis of respondent characteristics. Finally, we discuss model fit and explained variance. In Section 4.2, we expand on these findings by discussing an extended model that includes interaction effects.

4.1. Main effects

4.1.1. Vignette acceptance

Across the sample, the vignettes received an average acceptance score of 5.19 ($SD = 1.54$). Given that vignette acceptance was evaluated on a scale ranging from 1 (very unacceptable) to 7 (very acceptable) with 4 being neutral, this mean score suggests that the vignettes were generally evaluated as more acceptable than unacceptable. As Fig. 1 reveals, the distribution of vignette acceptance is left-skewed with most vignettes receiving an acceptance score of 6 (acceptable).

4.1.2. Main effects of vignette variables on vignette acceptance

We will now discuss the main effects of the multilevel regression model (Appendix C, Table C1, Model 4), starting with the effects of the vignette variables on vignette acceptance. Their effects are visualized in Fig. 2.

4.1.2.1. Threat type. The results indicate that vignettes featuring terrorism as the threat type were evaluated as most acceptable, followed by digital attacks aimed at disrupting an electricity network. Vignettes with trade secrets or disinformation as threat types were found to be least acceptable, with disinformation being most unacceptable. Threat type had the largest effects out of all vignette variables. These findings support hypotheses 1 and 2.

4.1.2.2. Duration. Vignettes wherein data was collected one time only were rated most acceptable. This was followed by a data collection period of three months, while systematic data collection received the least favorable evaluation. This corresponds with hypothesis 3, which posits that intelligence collection with a longer duration is associated with lower acceptance.

4.1.2.3. Data subject. Vignettes involving data collection from a few residents of a country outside the European Union were regarded as the most acceptable, followed by those involving data collection from a few residents of the Netherlands. Vignettes suggesting data collection from thousands of residents outside the European Union received significantly lower acceptance, and data collection from thousands of residents of the Netherlands was deemed the least acceptable. These findings support Hypotheses 4 and 5, indicating that intelligence collection involving fewer data subjects and targeting foreign individuals is associated with higher levels of public acceptance.

4.1.2.4. Collection method. No significant differences were found between data collection via a foreign intelligence service, through informants, and by searching the internet. These methods emerged as the most acceptable methods. There were significant differences for the other collection methods. Requesting information from another organization was evaluated as significantly less acceptable than the aforementioned methods. This was followed by wiretapping an internet connection, which was viewed significantly less favorably. Hacking a device was deemed the least acceptable method. These results support hypothesis 6, as some collection methods were rated significantly less acceptable than others, although not all methods showed significant differences.

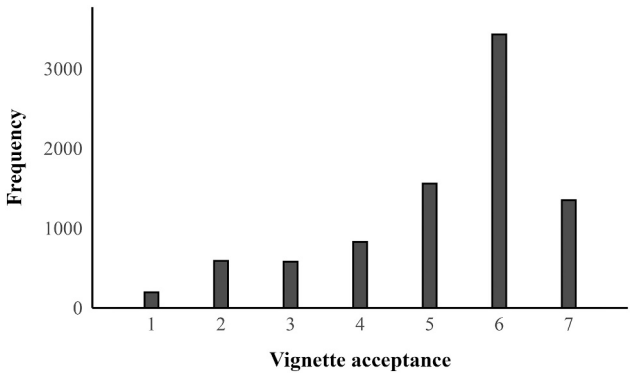

Fig. 1. Frequency distribution of vignette acceptance scores ($N = 8538$).

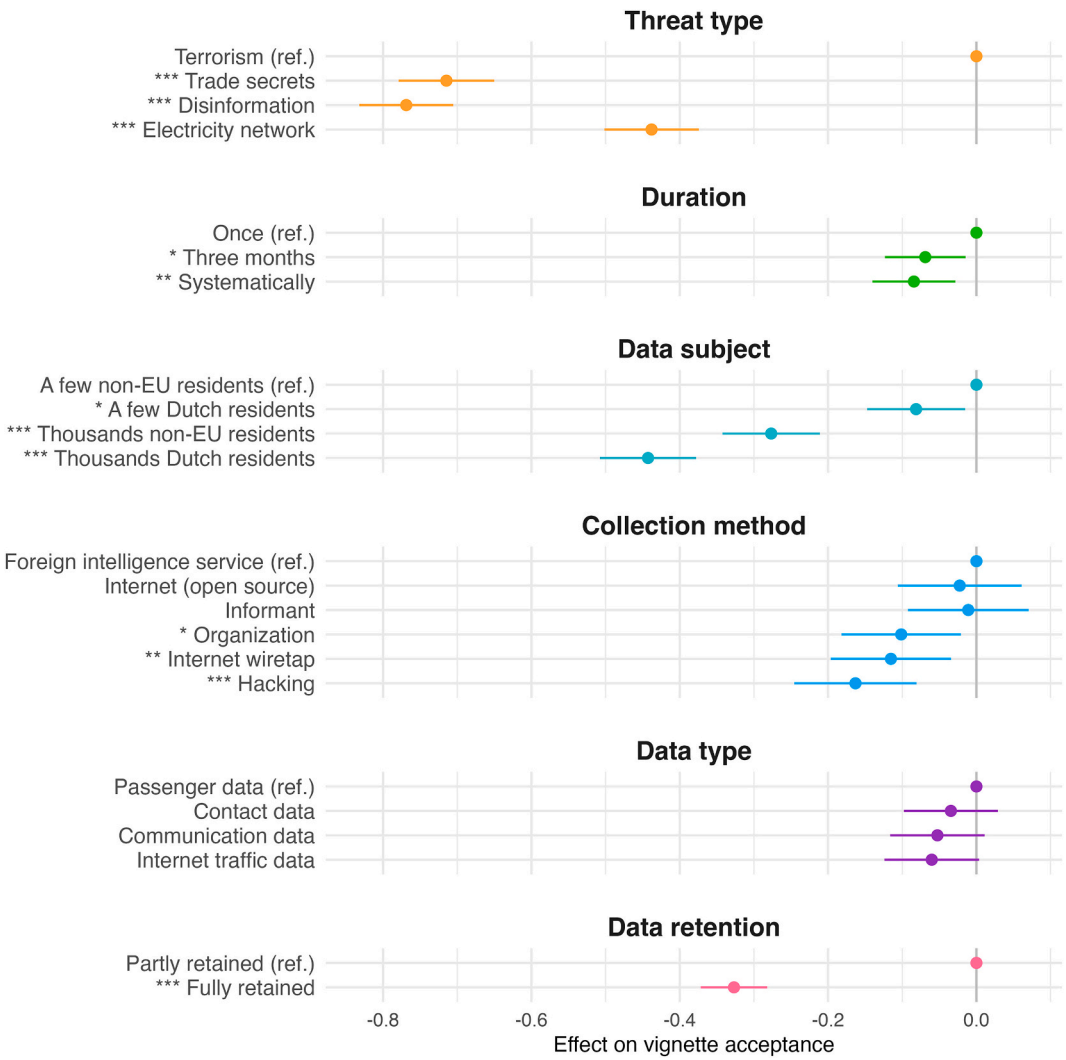

Fig. 2. The effects of vignette levels on vignette acceptance for each vignette dimension. *Note.* The figure displays point estimates (dots) and corresponding cluster-robust 95 % confidence intervals (horizontal lines) from a multilevel regression model with random intercept (Model 4, Appendix C, Table C1). The dots on the zero line without confidence intervals represent the reference category for each variable. Significance levels indicate whether vignette levels significantly differ from their reference categories, with significance denoted as: * $p < .05$; ** $p < .01$; *** $p < .001$.

4.1.2.5. Data type. The collection of passenger data was rated the most acceptable. However, no significant differences with the other three data types were found. Thus, hypothesis 7 is unsupported.

4.1.2.6. Data retention. Vignettes wherein only data useful to the investigation was retained and the remaining information was destroyed were evaluated as significantly more acceptable than vignettes in which all information was retained. These findings support hypothesis 8.

4.1.3. Main effects of respondent variables on vignette acceptance

Next, we examine the main effects of the respondent and control variables, which were treated as continuous. Unsurprisingly, some variables showed moderate to strong correlations. Privacy concerns for self and others were strongly correlated ($r = 0.753$), as were the trust-related variables. Additionally, surveillance and privacy concerns exhibited weak to moderate negative correlations with trust. In contrast, the control variables showed no strong correlations. A correlation matrix plot is provided in Appendix D, Fig. D1. Variance inflation factor (VIF) tests confirmed no multicollinearity (all VIFs <2.0). Notably, despite these correlations, the variables had distinct effects in the regression model, with varying significance levels.

The effects of the respondent variables and controls on vignette acceptance are visualized in Fig. 3.

Participants with higher levels of general trust in institutions rated the vignettes more favorably, supporting hypothesis 9. A strong positive effect was also observed for participants who expressed greater trust in the competence of the AIVD, indicating that higher trust in the intelligence service's competence is associated with greater acceptance of the vignettes. However, no significant effect was found for trust in the integrity of the AIVD, providing partial support for hypothesis 10. Similarly, hypothesis 11 was not supported, as trust in oversight was not significantly associated with vignette acceptance.

Partial support for hypothesis 12 was found: participants with greater privacy concerns for others rated the vignettes significantly less favorably, while no significant effect was observed for privacy concerns regarding themselves. Hypothesis 13 remains unsupported, as no significant effects were found for surveillance concerns. Finally, hypothesis 14 is supported, as a significant negative effect was found for privacy importance, suggesting that participants who place greater importance on privacy rated the vignettes as less acceptable.

As for the control variables, we observed a significant positive effect for *political orientation*, indicating that participants who identify as right-wing tended to find the vignettes more acceptable compared to those on the left end of the political spectrum. This is consistent with previous

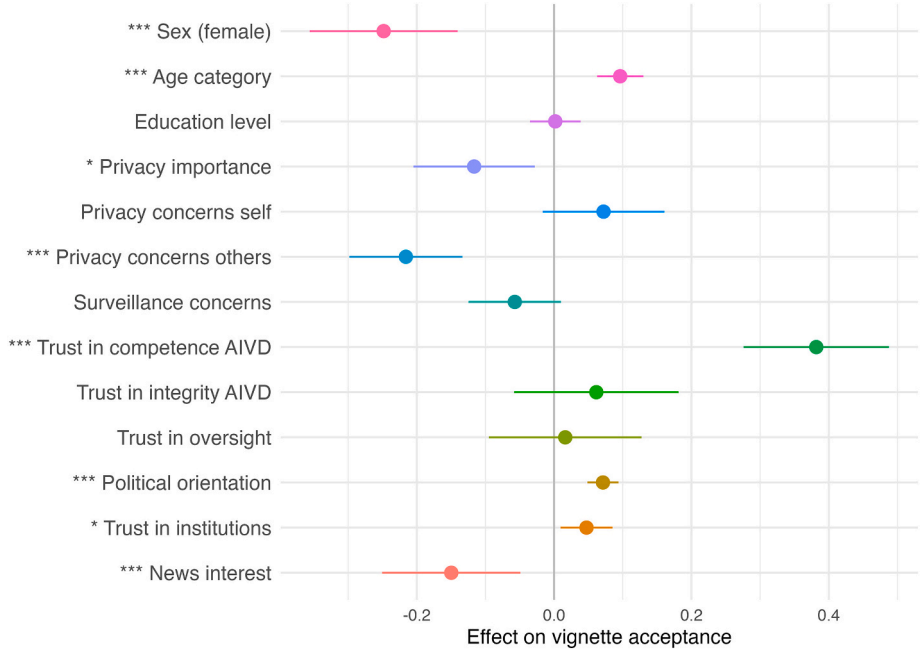

Fig. 3. The effects of respondent and control variables on vignette acceptance. *Note.* The point estimates represent the effect of a one-unit increase in each predictor variable. Specifically, for each one-unit increase in the scale of a variable, the estimated change in the outcome (vignette acceptance) is given by the point estimate (Model 4, Appendix C, Table C1). Note that scales differ across variables: for instance, political orientation and trust in institutions are rated on an 11-point scale, while most others use a 5-point Likert scale. For more details, see Section 3.5. *Note.* The "Sex (female)" estimate shows the difference in vignette acceptance between females and males, with males as the reference category (estimate = 0).

research (Finkelstein et al., 2017; Nam, 2017; van Wilsem & van der Woude, 2011). Finkelstein et al. (2017) suggest that this is because liberals, relative to other groups, are more likely to view surveillance policies as ineffective and susceptible to government abuse while also perceiving a lower threat of terrorism. The significant effect associated with *news interest* suggests that participants with more interest in the news tended to display more acceptance of the vignettes. This pattern may reflect the specific context of the Netherlands, where intelligence services and the Wiv 2017 law have received extensive coverage in the media. It may also suggest that transparency can play a significant role in fostering public support for intelligence practices.

For *age category* (see Table 1 for the categories), the results show a positive effect consistent with previous research (Nam, 2018), suggesting that older participants rated the vignettes significantly more acceptable compared to younger participants. No significant effect was found for *education level*.

Regarding *sex* (0 = male, 1 = female), our findings reveal that female respondents rated the vignettes on average as significantly less acceptable. This contradicts previous research (Messick, 2023; Trüdinger & Steckermeier, 2017), though it is in line with findings that women are generally more concerned than men regarding the impact of information collection on their privacy (Smith et al., 2011). This outcome is challenging to interpret using our data alone; there are weak correlations between gender and political orientation and news interest (Appendix D, Fig. D1), with female participants being slightly more left-wing and less interested in the news – both factors associated with lower acceptance.

4.1.4. Model fit and explained variance

The model fit statistics indicate a good overall fit. The marginal R^2 value of the main effects model shows that the fixed effects (i.e., the variables included in the model) account for 20.8 % of the total variance. The conditional R^2 value indicates that the full model, which includes both fixed and random effects, explains 54 % of the variance in the data. The random effects capture variation in vignette scores across respondents that is not explained by the fixed variables, suggesting that some respondents consistently rate vignettes higher or lower regardless of factors such as age, trust, privacy concerns, or vignette characteristics. This implies there may be additional unmeasured factors, such as personal experiences or differences in how respondents interpret the vignettes, that influence vignette scores. Overall, the R^2 values suggest that the model performs well in explaining the variance in the data.

Beyond overall model fit, we examined the relative explanatory power of different components of our model to determine which vignette dimensions or respondent variables had the strongest impact on vignette scores. To assess this, we compared the marginal R^2 values across isolated components of the main effects model, focusing separately on vignette dimensions, demographics, and respondent attitudes (Model 1 to 4, Appendix C, Table C1). However, comparing R^2 values requires caution, because variables have different scales, and the vignette variables are categorical. Therefore, there could be many reasons why one model has a higher R^2 than another and we should be cautious in drawing strong conclusions. To gain further insights, we used the PartR2 package in R (Stoffel, Nakagawa, & Schielzeth, 2021) to calculate the R^2 values for individual variables in the main effects model.

Interestingly, the model with only vignette variables has a relatively low marginal R^2 (6.3 %) compared to the model with only respondent variables, which explains 13 % of the variance. This suggests that variation in vignette scores between respondents is better explained by their attitudes than by the specific conditions of the vignettes. In other words, respondents' trust and privacy attitudes seem stronger determinants of their acceptance ratings than the scenarios themselves. However, somewhat paradoxically, the PartR2 analysis reveals that among individual predictors, threat type – a vignette variable – was the single most influential factor, explaining 3.9 % of the variance in the main effects model. This was notably higher than any other individual variable, including respondent variables. These findings suggest that while respondent variables collectively explain a larger share of the variance in acceptance ratings – indicating that predispositions shape how individuals interpret a vignette – threat type remains the most powerful individual predictor of vignette acceptance.

4.2. Interaction effects

Following the main effects analysis, we sought to determine whether the effects of certain vignette variables on the dependent variable would change based on the values of other vignette variables. To achieve this, we incrementally added interaction terms to the main effects model to evaluate their effects. Our analysis revealed modest but significant effects for two interactions: *threat type x data subject* and *data type x collection method*. Other interaction terms did not produce significant results. The regression model with the significant interaction terms can be found in Appendix C, Table C2. As with the main effects model, estimates for each level should be interpreted relative to their reference category. Significant interactions highlight deviations from the expected relationship of the reference category. The interaction effects did not substantially change our core findings, so we discuss these results only briefly.

Threat type x data subject: First, we examined the interaction between data subject and threat type to understand how their variations impact vignette acceptability. The effects are visualized in Fig. 4.

While the main effects model showed it was more acceptable to collect data from fewer people compared to thousands, and from non-EU residents compared to Dutch residents, the model with interaction terms reveals that only the specificity of data collection remains significant: vignettes involving data collection from thousands of subjects are viewed as significantly less acceptable than from just a few. There are no significant differences between non-EU and Dutch residents, suggesting that the origin of data subjects generally does not influence vignette acceptance.

An exception occurs with vignettes involving trade secrets as the threat type, where collecting data from non-EU residents is significantly more acceptable than from Dutch residents. In this case, the origin of the data subjects does matter. These findings suggest that for certain threat types, participants may have specific expectations about the likely perpetrators. For example, participants may perceive it as more likely that individuals from another country, rather than their own, would attempt to steal trade secrets. This finding has implications for hypothesis 5. While this hypothesis was supported in the main effects model, the interaction model shows that this is only the case in a specific context, which suggests that the relationship proposed holds only under certain conditions. Thus, we conclude that hypothesis 5 is partly supported (Table 4).

Data type x Collection method: Second, we examined whether vignette acceptance for different data types would change based on the collection method used. The effects are visualized in Fig. 5.

While the main effects model showed no significant differences between data types, the addition of an interaction term did reveal significant differences. Each data type exhibited a distinct pattern of acceptability concerning different collection methods. For instance, in vignettes featuring the collection of passenger data, using a foreign intelligence service was more acceptable compared to other methods, while hacking was the least acceptable. However, this pattern did not hold for the other data types. For contact and communication data, for instance, receiving information from an informant was viewed as the most acceptable method, while this was the least acceptable method for internet traffic data.

These variations across collection methods help explain the insignificant differences between data types in the main effects model, as overall effects balance out. The distinct patterns for each data type indicate that participants have specific expectations about which methods should be used for collecting certain types of data and perceive some combinations of data type and collection method as more appropriate than others. For example, with passenger data, there are clearer expectations about acceptable and unacceptable collection methods. However, for other data types, like internet traffic, the differences in acceptability between methods are much smaller. We cautiously conclude that hypothesis 7 is partly supported, as data type acceptability seems to be related to the collection method used to gather the data, though effects are small.

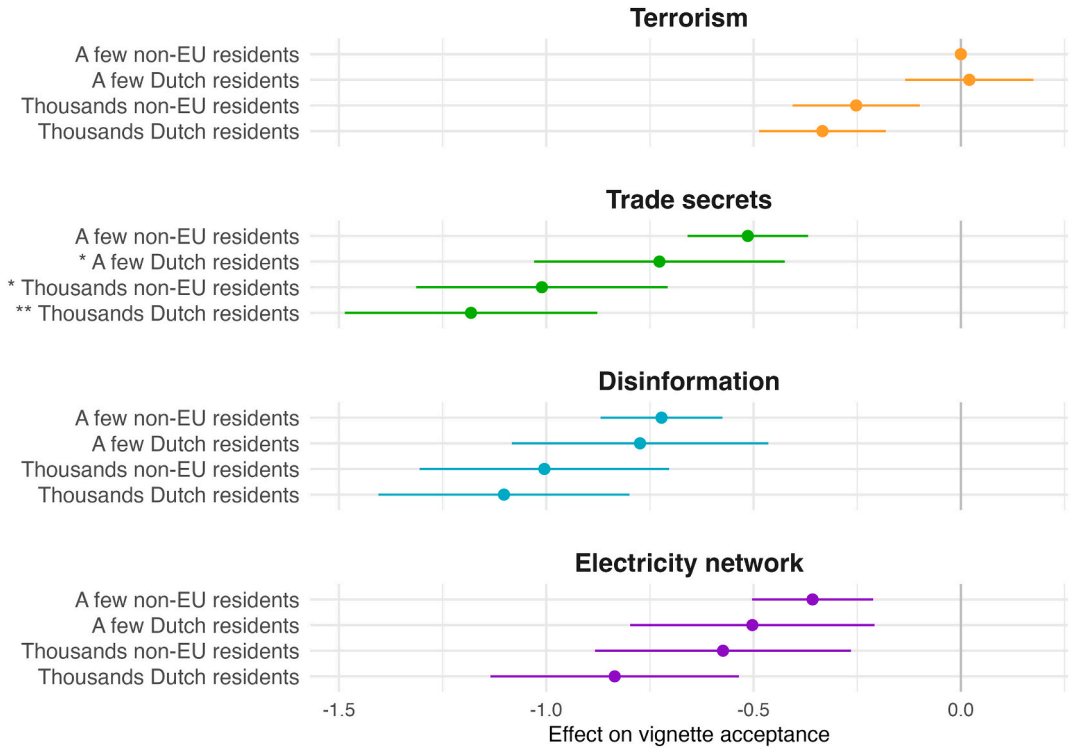

Fig. 4. Interaction effect of *threat type x data subject* on vignette acceptance. *Note.* Significance levels indicate whether the interaction effect is statistically significant, meaning that the interaction significantly deviates from the expected relationship as established for the reference category. Significance is denoted as: * $p < .05$; ** $p < .01$.

Table 4
The results of hypothesis tests.

	Hypothesis	Result
1	Different threat types are associated with varying levels of public acceptance.	Supported
2	Intelligence scenarios involving terrorism as threat type are associated with higher public acceptance than scenarios with other threat types.	Supported
3	Intelligence collection with a longer duration is associated with lower public acceptance than intelligence collection with a shorter duration.	Supported
4	Intelligence collection of fewer data subjects is associated with higher public acceptance than intelligence collection of more data subjects.	Supported
5	Intelligence collection of foreign data subjects is associated with higher public acceptance than intelligence collection of domestic data subjects.	Partly supported
6	Different methods of intelligence collection are associated with varying levels of public acceptance.	Supported
7	The collection of different data types is associated with varying levels of public acceptance.	Partly supported
8	Intelligence collection where data is stored in full is associated with lower public acceptance than intelligence collection where data is filtered, and irrelevant information is destroyed.	Supported
9	Higher levels of general institutional trust are associated with higher acceptance of intelligence collection.	Supported
10	Higher levels of trust in intelligence agencies are associated with higher acceptance of intelligence collection.	Partly supported
11	Higher levels of trust in oversight are associated with higher acceptance of intelligence collection.	Not supported
12	Greater privacy concerns are associated with lower acceptance of intelligence collection.	Partly supported
13	Greater surveillance concerns are associated with higher acceptance of intelligence collection.	Not supported
14	Higher perceived importance of privacy is associated with lower acceptance of intelligence collection.	Supported

5. Discussion

5.1. Contextual factors

5.1.1. Threat type most influential, with vignettes featuring terrorism most acceptable

Of all vignette dimensions, *threat type* exerted the strongest influence on acceptance, indicating that the acceptability of data collection by intelligence services depends foremost on *why* the data are collected. Vignettes featuring a terrorism threat were by far found most acceptable, followed in order by a cyber threat (digital attacks against an electricity network), espionage threat (theft of trade secrets), and a democracy threat (the spread of disinformation).

Several explanations can account for these results. Evidence suggests that people tend to overestimate the risks of terrorist attacks and the likelihood of being personally affected (Braithwaite, 2013; Dvir et al., 2023), which heightens perceived urgency and legitimizes invasive surveillance. In contrast, the impact of other threats like digital attacks or trade secret theft may be less immediately visible and harder to quantify, often unfolding gradually or becoming apparent only over time. Moreover, cyber-attacks or industrial espionage typically target governments, organizations, information and materials, public opinion, or strategic targets rather than lives. Therefore, these threats may be viewed as less threatening to citizens personally. This explanation is supported by recent research suggesting that only cyber-attacks causing lethal consequences – compared to attacks with non-lethal consequences – generate heightened support for surveillance policies (Snider et al., 2025). Furthermore, addressing threats such as the spread of disinformation may be more controversial; efforts to counter disinformation could be seen as infringing on free speech. Likewise, participants may not view disinformation or corporate espionage as national security issues, raising questions about whether such cases warrant investigation by intelligence services at all.

5.1.2. Specific and small-scale data collection more acceptable

Consistent with previous research indicating that smaller-scale data collection is generally perceived as more acceptable (Vitak et al., 2023), vignettes involving single-instance data collection from a limited number of subjects were typically viewed more favorably than those depicting systematic collection from larger groups. These findings suggest that participants are less comfortable with extensive data collection – characterized by more subjects and longer collection periods – compared to more targeted approaches. This preference is further reflected in the finding that vignettes featuring data filtering after collection were deemed more acceptable than those involving full data retention. These findings clearly show support among participants for the principle of specificity established in legal frameworks (Aerdts, 2023).

5.1.3. Limited influence of data subject's origin

Overall, vignettes featuring data subjects from outside the EU were deemed more acceptable than those involving Dutch data subjects. However, interaction effects revealed that data subject origin only influenced acceptability in vignettes involving a trade secret threat. This pattern diverges from prior work that suggests people more readily endorse the collection of data or restriction of rights from out-group members compared to in-group members in counter-terrorism settings (Geedy-Gill & Carriere, 2024; Reimer & Johnson, 2023). One possible explanation is that industrial espionage may be perceived as an *international* rather than a domestic threat, making foreign actors the assumed culprits and surveillance feel more justified. Thus, support for surveillance targeting different groups appears *context dependent*. This finding is interesting, considering that the Dutch Intelligence and Security Services Act (Wiv 2017) grants equal legal protections to both nationals and non-nationals – an uncommon feature in intelligence legislation. In many countries, citizens receive a higher level of protection compared to individuals outside the jurisdiction of intelligence services (Kniep et al., 2024). This finding suggests that Dutch citizens generally support the principle of universality embedded in their intelligence legislation, though our research cannot say whether such attitudes are prevalent among citizens from other countries.

5.1.4. Acceptance of collection method and data type context dependent

Generally, hacking and wiretapping an internet connection were found significantly less acceptable than other methods. This viewpoint is also reflected in Dutch law, where these methods are considered more severe and intrusive, thereby subjecting them to stricter procedural safeguards and oversight (Oomens et al., 2023). Interestingly, requesting data from another organization was also found less acceptable by participants, despite being a collection method with relatively limited oversight under Dutch law. One possible explanation is that participants did not anticipate organizations in the vignettes sharing certain types of data with intelligence services. This interpretation is bolstered by interaction effects, which indicated that the acceptability hierarchy among collection methods varied depending on the type of data and thus is more complex than a straightforward hierarchy of intrusiveness or sensitivity. This complexity challenges the notion that one data type or collection method is consistently less acceptable across scenarios, which contradicts research on information sensitivity, where conclusions have often been drawn about the overall sensitivity of specific data types (e.g., Milne et al., 2017; Schomakers et al., 2019).

5.2. Respondent characteristics

5.2.1. Privacy concerns for others and privacy importance lower acceptance

In line with previous research on surveillance acceptance and the APCO model (Dinev et al., 2008; Smith et al., 2011; Thompson et al.,

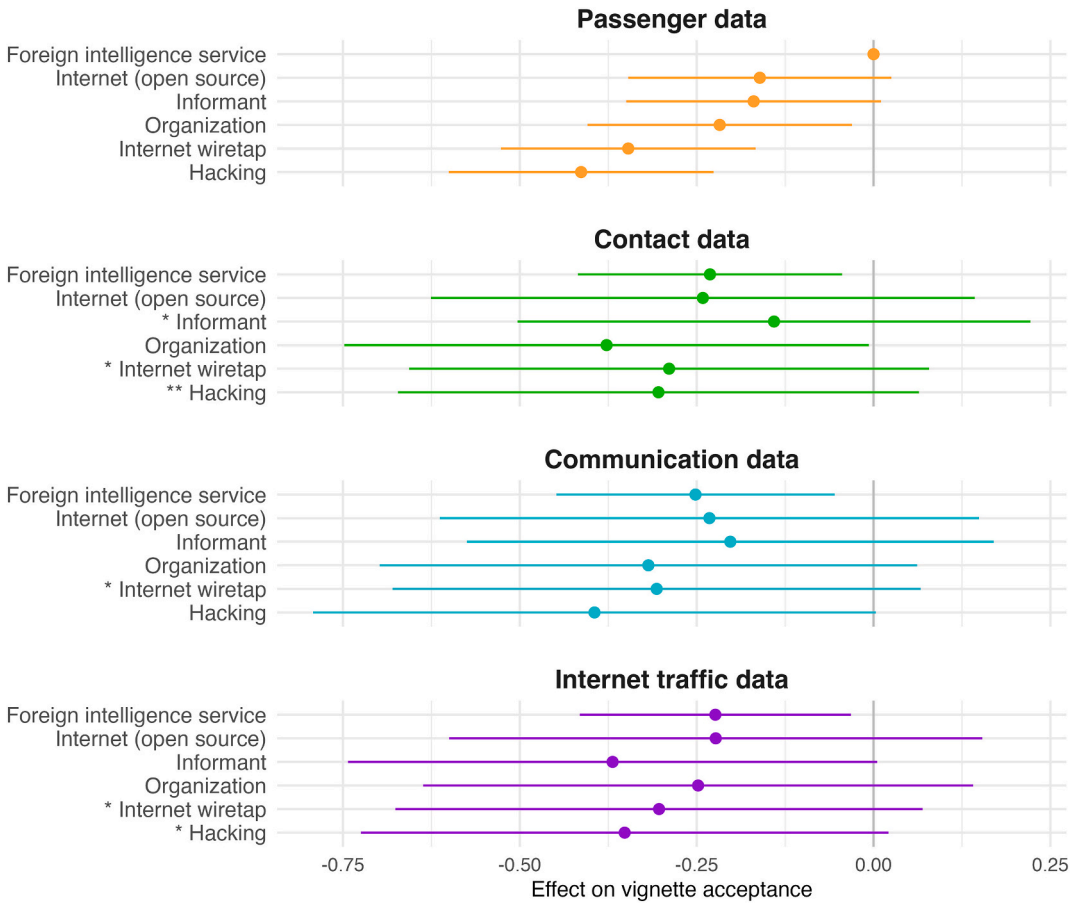

Fig. 5. Interaction effect of *collection data type x collection method* on vignette acceptance. *Note.* The effects in Fig. 5 are smaller than those in Fig. 4, which results in a different x-axis scale, causing the confidence intervals to appear much wider. However, their absolute size is only slightly larger. Interaction effects tend to have larger standard errors, which introduces greater uncertainty into the estimates. Consequently, caution is needed when interpreting the results. This increased uncertainty raises the threshold for significance, but despite this, some effects remain statistically significant, indicating that interaction effects are likely present in the data.

2020), our findings indicate that participants with more privacy concerns for others found the vignettes generally less acceptable. Surprisingly, no significant effects were found regarding privacy concerns for self nor regarding surveillance concerns. A possible explanation is that participants did not see themselves as potential data subjects, possibly making them less concerned about surveillance and threats to their privacy from intelligence services. Those with increased privacy concerns for others might be more sensitive to intelligence collection involving other people, influencing their perceptions of the scenarios. This explanation is supported by previous research, which found that empathy for vulnerable out-groups strongly predicts opposition to surveillance policies (Valentino et al., 2020).

5.2.2. *Trust in institutions and competence increase acceptance*

Consistent with previous research (Ball et al., 2019; Budak & Rajh, 2018; Liu, 2021; Nam, 2018, 2019; Svenonius & Björklund, 2018; Thompson et al., 2020; Trüdinger & Steckermeier, 2017; Valentino et al., 2020), our study shows that greater trust in institutions and in the intelligence service's competence is linked to higher acceptance of intelligence collection scenarios. By contrast – and contrary to expectations – trust in the service's *integrity* and in *oversight* had no significant effect. One plausible explanation is that believing the agency follows the rules does not mean one endorses those rules or finds far-reaching surveillance acceptable. Competence appears decisive: when citizens think the service can effectively prevent threats (e.g., a terrorist attack), they are more willing to tolerate privacy intrusions and the associated use of public resources. If that competence is in doubt, the same costs seem unjustified. This pattern echoes findings from research on acceptance of AI technology where perceived legitimacy is closely tied to expectations of efficiency and accuracy (Horvath et al., 2023).

5.3. *Theoretical contributions and implications*

This study examines public acceptance of intelligence-gathering across *six contextual dimensions*: one that captures *why* data are collected (threat type) and five that capture *how* collection is conducted (duration, data subject, collection method, data type, and retention period). We also consider the role of key respondent predispositions – such as trust and privacy attitudes. By combining these contextual cues with individual characteristics in a factorial survey experiment, we extend and refine current theorizing on public perceptions of institutional surveillance and data collection.

The findings reveal a two-layered judgment process that reinforces the importance of considering both contextual features and respondent characteristics for understanding public support for intelligence collection. First, individual predispositions function as a *lens* through which a vignette is judged. Participants with strong trust in institutions and their competence approach scenarios more favorably, whereas those with low trust and pronounced privacy concerns judge them more critically. This aligns with previous research indicating that participants' predispositions are amplified when confronted with a security threat scenario; individuals already inclined to perceive cyberattacks as threatening experience a significant increase in their perceptions of threat after reading a cyberattack scenario, while those with lower

threat perceptions also have their existing views reinforced (Dor et al., 2024).

Second, contextual cues determine how a respondent evaluates different scenarios *relative* to each other. In other words, respondents with varying predispositions draw similar conclusions about which scenarios are more (or less) acceptable compared to others. These results align with Nissenbaum's framework of privacy as contextual integrity (Nissenbaum, 2010), which holds that people evaluate data practices against context-specific informational norms.

Our evidence nuances this theory in two important ways. First, we find only weak support for an independent effect of information type – at least in a national-security context – which is one of the core parameters proposed by the theory to describe information flow and determine its appropriateness. Second, the purpose of collection emerges as the single strongest predictor of acceptance, outweighing every "how" factor. Though more contextual integrity studies have started to include purpose (e.g., Trein & Varone, 2023; Vitak et al., 2023), it is not always treated as a core parameter of information flow; our results suggest that this is an important omission in the field and that, particularly in security contexts, it should occupy a central place in models and theory of public support for data collection.

A notable finding from our study is that, on average, respondents found the vignettes more acceptable than unacceptable; even the least acceptable scenarios were generally rated slightly more acceptable than unacceptable. This contrasts with earlier research that highlights public opposition toward government surveillance (Tsapogas, 2017; Valentino et al., 2020). A possible explanation is that opposition may be amplified by *abstract questions* about surveillance in general, whereas *concrete scenarios,* clarifying the purpose, methods, and targets, provoke less resistance. For example, asking citizens whether their government's cellphone wiretapping powers has 'gone way too far' or 'not gone nearly far enough', invites associations of government overreach and thus magnifies opposition. It makes categorical what is inherently a trade-off. By contrast, when presented with realistic scenarios, the question becomes more about whether power use is proportional given the conditions. This further underscores the benefits of presenting participants with contextual information, as it reveals nuances that broad, decontextualized questions can obscure.

It should be noted that the high acceptance rate may also reflect the generally favorable views Dutch people have toward their intelligence services. Previous research has found considerable cross-national differences in support for surveillance (Arsenault et al., 2024) and van Wilsem and van der Woude (2011) have reported strong support among Dutch citizens for various counterterrorism measures. While participants in our survey indicated that they consider privacy important ($M = 4.32$), their relatively low concern about surveillance ($M = 2.43$) may support this interpretation. It suggests that, although participants care about privacy, they may be less concerned about the activities of the Dutch intelligence services compared to those of other entities. Similarly, Dutch citizens generally exhibit relatively high institutional trust compared to other countries (Torcal, 2017). Given that trust is associated with higher acceptance, this could help explain the overall high levels of acceptance in our study.

5.4. Implications for practice and policy

Previous research and political debates tend to assume that public attitudes toward intelligence operations are rooted in fixed political or personal preferences, such as strong views on privacy or trust in government, that then neatly divide society into different camps. However, our findings challenge this view, which has important implications for practice. When citizens are asked to consider concrete scenarios with realistic trade-offs, acceptance is not only possible across the board, but actually quite high – despite the influence of prior preferences. Therefore, rather than framing public communication around abstract principles ("privacy is paramount" or "you want security, don't you?"), intelligence agencies and political leaders should focus on explaining the practical dilemmas they face and how they navigate them. This approach resonates with a broader public than sometimes suggested, which may be taking to imply a more hopeful, depolarizing way to looking at legitimacy of intelligence. In this section, we explore the implications for policymakers and -executors on how to go about intelligence work, how to see public acceptance, and how to communicate to the public.

In a broader sense, our research illustrates how transparency regarding the considerations and criteria behind decision-making might enhance institutions' legitimacy. This is especially relevant to the intelligence domain, where the extra element of secrecy further complicates public understanding and knowability of the practical implications of policy, beyond the typical information asymmetry between experts and citizens found in other sectors. Indeed, intelligence agencies tend to reveal little about their work out of concern for revealing modus operandi, compromising sources, or endangering personnel. Intelligence officials' communication usually sticks to emphasizing national security benefits without much explanation, which leaves the public guessing about how principles such as proportionality, necessity, and specificity are applied.

Our study demonstrates that when citizens are given even minimal contextual information – why the data are collected and for how long, whose data are involved, and with what safeguards – they can differentiate between operations they find justified and those they deem excessive. In fact, they evaluate most operations as quite acceptable, at least for the scenarios we put in front of them. Intelligence services do not need to disclose operational details to achieve this effect; outlining the parameters and trade-offs that shape their decisions is enough to foster understanding and, by extension, support. In short, contextualizing power-use, rather than merely invoking "national security," helps citizens recognize the need for power use under certain circumstances.

In addition to increasing transparency around decision-making processes, intelligence agencies must ensure that their activities internally consistently align with the core principles of proportionality, necessity, subsidiarity, and specificity. While our results show that scenarios involving terrorism threats are generally perceived as more acceptable than those involving other types of threats, this should not be interpreted as a license to justify overreach or mass surveillance under the guise of counterterrorism, as has been the case for certain post-9/11 practices. Our findings underscore that public acceptance of intelligence operations is highly conditional. Participants clearly preferred less intrusive collection methods, limited data retention, and favored targeted surveillance over indiscriminate collection. Furthermore, the significance of respondent trust in institutional competence suggest that the perceived effectiveness of intelligence services is a critical factor in shaping public support. In other words, intelligence agencies must not only act proportionately but also demonstrate professional competence and efficacy. This is something that may be achieved by providing transparent explanations.

For policy and governments, this implies several things. First, it means that the public understands that context matters, so they do not expect blanket prohibitions or unqualified mandates. Previous studies that operate on categorical declarations of support or rejection cannot reveal this nuance, but our experiment does. This also means that public communication could emphasize the careful balancing act and the safeguards applied, rather than rely on sweeping assertions of national security. Highlighting the process can enhance legitimacy more effectively than presenting about results alone.

Second, it means that citizens value policies that leave room for principled weighing, such as proportionality and subsidiarity, rather than assume that policies reflect one-size-fits-all approaches. In other words, flexibility in policy design is not a "necessary evil" forced on lawmakers by the complexities of policy implementation or by the dynamics of the security domain; it can be seen as the articulation of a public value. When drafting policies, when implementing them, and

when accounting for them afterwards, agencies can reference this insight as salient values held by the public.

Third, trust in the competence of the agencies affects acceptance. Our study displays how competence is not only demonstrated through successful operations, but also through transparent accounts of how trade-offs are approached, documented, and reviewed. This means that for instance publishing anonymized case studies or decision frameworks could serve a dual purpose: it informs oversight bodies and demonstrates the competence of the agency in operationalizing abstract values as they are present in the legislation. Dutch services have begun publishing richer public-facing threat assessments, for example in a recent report on anti-institutional extremism, as well as providing more examples in their annual report, which explain *why* powers are needed in accessible language (AIVD, 2023, 2025). Our findings suggest that this trend supports legitimacy of the service's use of powers.

Of course, formal oversight remains crucial for political accountability, yet surprisingly, trust in oversight bodies had no significant effect in our data. This implies that intelligence services should therefore consider speaking for themselves, of course within the limits of their trade, rather than relying exclusively on the formal oversight reports or parliamentary discussions for public accountability. Even if not native to many of these agencies, proactive communication about methods, safeguards, and limitations fits with the public's understanding and can increase acceptance and ultimately legitimacy of their work in a democratic context.

Furthermore, our findings suggest that citizens could be invited into the reasoning process, rather than treating them as passive receptors to information, which then may or may not get their approval. It could even be considered to institutionalize this more, for instance with selected citizen juries, briefed under a secrecy oath, that review hypothetical scenarios and advise parliament, government, oversight bodies and the agencies themselves. This leverages the public's demonstrated ability to understand nuance.

A final point, our study was fielded *before* some major geopolitical shocks in the Netherlands (e.g. NATO enlargement debates, more autonomy on defense). Early polling indicates an overall rise in public concern for security (van der Schelde & Kanne, 2025), which may further increase acceptance and perceived legitimacy of the work of intelligence and security services.

5.5. Limitations and future research directions

There are several limitations related to this study that need to be acknowledged. First, while we aimed to recruit a sample representative of the Dutch population, our study had an overrepresentation of older individuals. Given that older participants generally found the vignettes more acceptable than younger ones, this skew may have contributed to a higher overall acceptance score.

Second, practical constraints necessitate limiting the number of factors and variables included in the vignettes and survey. Vignettes are recommended to not exceed a certain number of combinations, as to not overburden respondents and avoid fatigue, boredom, and unwanted methodological effects (Auspurg & Hinz, 2015). However, excluding certain factors means we cannot rule out that those factors also influence how participants evaluate the acceptability of data collection by intelligence services, such as oversight mechanisms, or the perceived likelihood, urgency, and certainty of a potential threat. While vignettes offer a controlled way to assess how various factors shape attitudes, they are nonetheless simplified representations of reality and cannot capture all the nuances of real-life intelligence scenarios and the complexities of participants' reasoning behind their acceptance ratings.

Third, the way participants interpret a vignette can depend heavily on the wording, assumptions they make, or prior knowledge. Likewise, we provided participants with information about the intelligence service (AIVD) before answering any questions. This may have shaped how participants evaluated the AIVD's trustworthiness or their general concerns about privacy.

Despite these limitations, this study contributes to a more contextualized understanding of public acceptance of intelligence practices. As with all experimental research, there is the question of external validity; how results from a study in a controlled and simulated environment translate to real-life scenarios. Though most of our findings, such as participants' preference for targeted, proportionate surveillance, are consistent with legal principles and prior literature, there may be some real-life nuances we fail to capture. Future research could explore these nuances in greater detail, for instance by investigating why certain data types are deemed more acceptable when collected through specific methods. Qualitative and mixed-method studies may be especially useful in uncovering the reasoning behind such patterns. Furthermore, future work could expand the scope of contextual factors studied, particularly those related to the purpose of intelligence collection, or test variations in different political or cultural settings. Lastly, research must show whether increased transparency and specific communication regarding decision-making processes by intelligence agencies indeed positively affects public acceptance.

6. Conclusion

Our study highlights the significant influence of both contextual factors and individual predispositions on people's perceptions of intelligence collection. Contextual factors affect the relative acceptability of specific scenarios, while individual predispositions shape general attitudes toward these scenarios.

However, the importance of context cannot be understated, as evidenced by the fact that the type of threat being investigated emerged as the most influential variable. This finding indicates that perceived benefits in an intelligence collection scenario can significantly outweigh and justify associated costs. It also implies that research on public acceptance of government surveillance or data collection should include detailed information on the purposes, aims, or benefits associated with the data collection to capture all relevant predictors of acceptance.

Interaction effects in our study revealed that the interplay among certain contextual factors is more intricate and nuanced than initially apparent. While some questions remain about the specifics of how and why these interactions occur, understanding these complex dynamics is crucial for accurately assessing public attitudes and developing policies that are both effective and publicly acceptable. Further research is needed to delve deeper into these dynamics.

Lastly, our findings carry implications for practice: transparency about the rationale, safeguards, and conditions of intelligence operations may foster more informed and supportive public attitudes. In addition, intelligence agencies must ensure their activities remain both proportionate and demonstrably effective to maintain legitimacy and public trust.

CRediT authorship contribution statement

E.C. Oomens: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **R.S. van Wegberg:** Writing – review & editing, Supervision, Methodology, Conceptualization. **M.J.G. van Eeten:** Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization. **A.J. Klievink:** Conceptualization, Methodology, Writing – review & editing, Supervision, Funding acquisition.

Funding details

This work was supported by the Ministry of the Interior and Kingdom Relations of the Netherlands and Delft University of Technology under Grant M75B07.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Survey instrument

Q1: introduction

This questionnaire is part of a study by Delft University of Technology, which investigates what Dutch citizens think of data collection by the General Intelligence and Security Service (AIVD). The next page provides more information about the AIVD.

The questionnaire starts with some general statements about privacy and trust. For each statement, indicate the extent to which you agree. You will then be shown 6 situations in which the AIVD collects information. For each situation, indicate what you think of the described situation. The situations were created by the TU Delft research team and are not real situations.

Q2: explanation about the AIVD

The *AIVD* (General Intelligence and Security Service) investigates *threats to national security and the democratic legal order*. This includes (digital) espionage, terrorism, extremism, the spread of weapons of mass destruction and secret political influence.

In its investigations, the AIVD may (under certain conditions) use many different methods to collect information about threats. This includes searching open sources (such as newspapers and social media), wiretapping, hacking, and requesting data from other organizations. With these methods, the service can collect many different types of data from various individuals or groups.

The activities of the AIVD are regulated by the Intelligence and Security Services Act (WIV) 2017. The service must adhere to this law and is overseen by regulatory bodies.

The AIVD aims to detect and prevent threats to national security, such as preventing a terrorist attack. This is mainly done by collecting and analyzing information. With this information, the service can inform, advise and call upon other organizations to take action against the threat (for example, the police). In some cases, the AIVD can also take action itself, such as counteracting a threat ('disruption').

Because the AIVD can collect a lot of information, choices must constantly be made about balancing security and privacy. On the one hand, it is important to keep the Netherlands safe, and on the other hand, it is important that people's privacy is not unnecessarily violated. The aim of this research is to determine what Dutch citizens find acceptable and unacceptable regarding data collection by the AIVD.

The questionnaire starts on the next page.

Q3: Respondent variables about trust and privacy attitudes

Please indicate the extent to which you agree with the following statements:

[1–5 Likert: 1. Strongly disagree 2. Disagree 3. Neither disagree nor agree 4. Agree 5. Strongly agree].

1. I think privacy is important.
2. I am concerned about my privacy.
3. I am concerned about the privacy of others.
4. I am afraid that the government is spying on me.
5. I trust that the AIVD is good at its job.
6. I trust that the AIVD adheres to the rules applicable to it.
7. I trust that the AIVD is properly supervised.

Q4: Vignettes

Starting from the next page, you will be shown 6 scenarios one by one. The scenarios are similar but also differ from each other.

Read the scenarios carefully and indicate how unacceptable (i.e., not tolerable, not okay) or acceptable (i.e., tolerable, okay) you find the situation. Perhaps you think some information is missing or that you don't have enough knowledge to judge the scenario? Try to answer anyway.

Q4.1–4.6: Question for each vignette

How unacceptable (i.e., not tolerable, not okay) or acceptable (i.e., tolerable, okay) do you find this situation?

[1–7 Likert] 1. Very unacceptable 2. Unacceptable 3. Somewhat unacceptable 4. Not unacceptable or acceptable 5. Somewhat acceptable 6. Acceptable 7. Very acceptable.

Q5: Debriefing

Thank you for completing this questionnaire about the acceptance of data collection by the General Intelligence and Security Service.

The results of this research will be public and processed in a scientific publication.

What were your thoughts about the questionnaire?

What did you think of this questionnaire:

Did you find it difficult to answer the questions?

Did you find the questions clear?

Did the questionnaire make you think?

Did you find the topic interesting?

Did you enjoy filling in the questions?

[1–5 Likert] 1 Definitely not – 5 Definitely yes.

Do you have any comments about this questionnaire? [Open text field]

Other questions included in data: (https://www.dataarchive.lissdata.nl/study-units/view/1478).

Are you very interested in the news, fairly interested or not interested?	1. very interested 2. fairly interested 3. not interested −9. I don't know
In politics, a distinction is often made between "the left" and "the right". Where would you place yourself on the scale below, where 0 means left and 10 means right?	1. left 10. Right −9. I don't know
Can you indicate, on a scale from 0 to 10, how much trust you personally have in each of the following institutions? *The Dutch government; the Dutch parliament; the legal system; the police; politicians; political parties; the media; the military; the education system; science; the democracy*	0 = no trust at all 10 = full trust −9. I don't know

Demographics (https://www.dataarchive.lissdata.nl/study-units/view/322).

Sex	0 Male 1 Female Missing: Other
Age in categories	0 15–24 years 1 25–34 years 2 35–44 years 3 45–54 years 4 55–64 years 5 65 years and older
Level of education in CBS (Statistics Netherlands) categories	1 primary school 2 vmbo (intermediate secondary education, US: junior high school) 3 havo/vwo (higher secondary education/preparatory university education, US: senior high school) 4 mbo (intermediate vocational education, US: junior college) 5 hbo (higher vocational education, US: college) 6 wo (university)

Appendix B

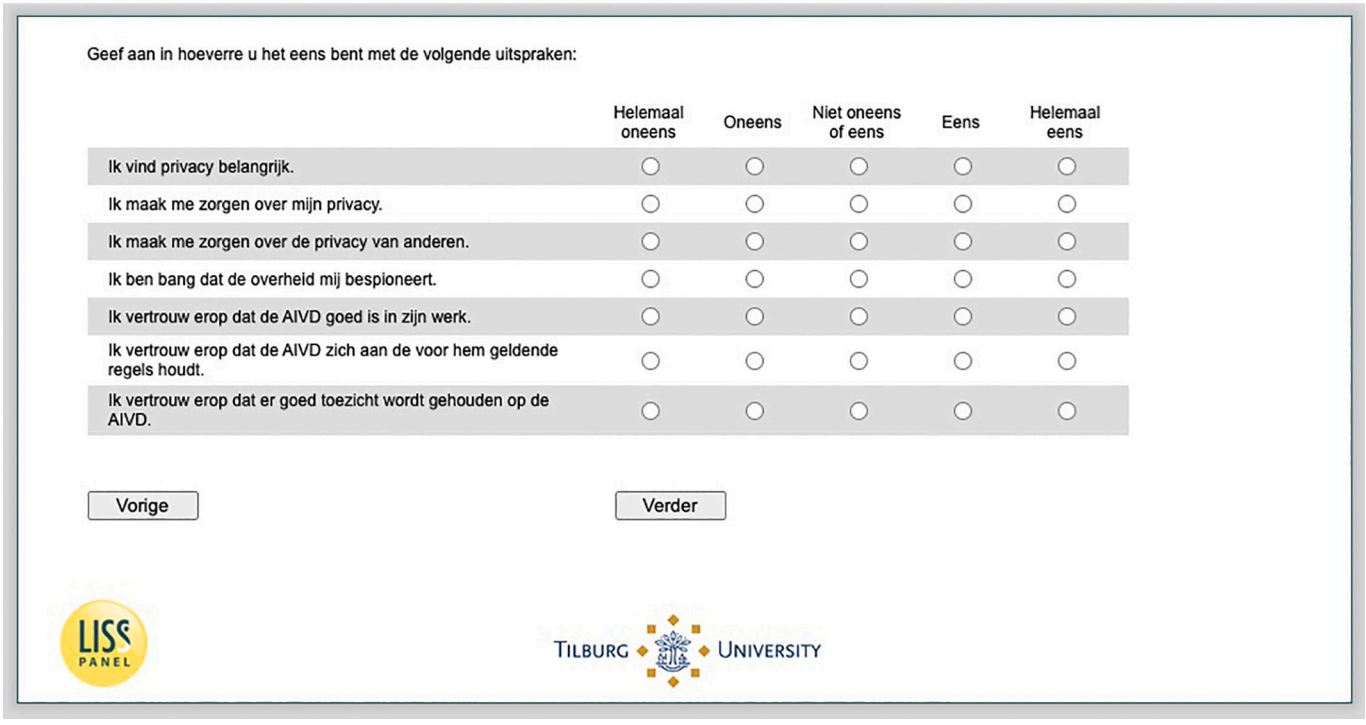

Fig. B1. Privacy attitudes and trust in survey as presented to participants.

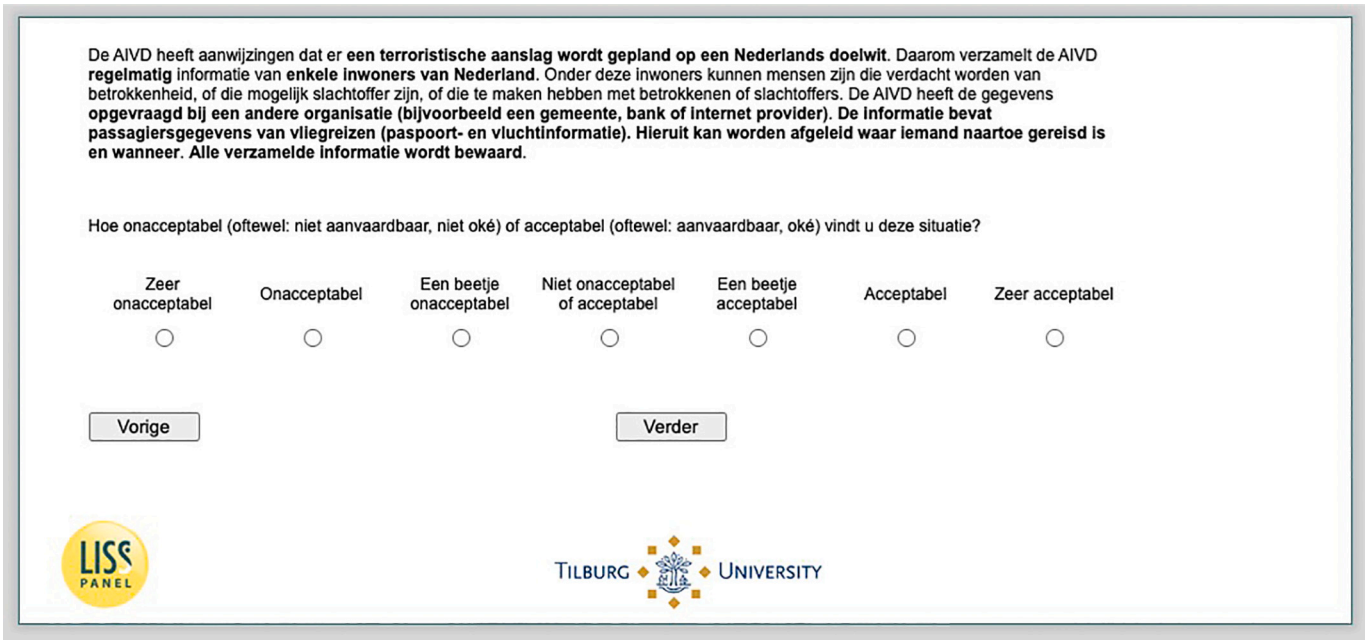

Fig. B2. Example of a vignette in survey as presented to participants.

Appendix C

Table C1
Multilevel regression models predicting vignette acceptance.

Coefficient	Model 1		Model 2		Model 3		Model 4		
	Vignette dimensions		*Demographic variables*		*Respondent attitudes*		*Main effects model*		
	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error	PartR2
Intercept	6.197***	0.059	4.836***	0.119	4.267***	0.298	4.890***	0.330	
Vignette variables									
Threat type									0.039
Terrorism (reference)									
Trade secrets	−0.714***	0.033					−0.715***	0.033	
Disinformation	−0.770***	0.032					−0.769***	0.032	
Electricity network	−0.439***	0.033					−0.438***	0.033	
Duration									0.001
Once (reference)									
Three months	−0.069*	0.028					−0.069*	0.028	
Systematically	−0.084**	0.029					−0.084**	0.029	
Data subject									0.012
A few non-EU residents (reference)									
A few Dutch residents	−0.081*	0.034					−0.081*	0.034	
Thousands non-EU residents	−0.275***	0.034					−0.277***	0.034	
Thousands Dutch residents	−0.442***	0.033					−0.443***	0.033	
Collection method									0.002
Foreign intelligence service (reference)									
Internet (open source)	−0.023	0.043					−0.023	0.043	
Informant	−0.011	0.042					−0.011	0.042	
Organization	−0.101*	0.041					−0.101*	0.041	
Internet wiretap	−0.117**	0.041					−0.115**	0.041	
Hacking	−0.163***	0.042					−0.163***	0.042	
Data type									0.000
Passenger data (reference)									
Contact data	−0.035	0.032					−0.034	0.032	
Communication data	−0.054	0.033					−0.053	0.033	
Internet traffic data	−0.061	0.033					−0.060	0.033	
Data retention									0.011
Partly retained (reference)									
Fully retained	−0.327***	0.023					−0.327***	0.023	
Respondent variables									

(*continued on next page*)

Table C1 (*continued*)

Coefficient	Model 1		Model 2		Model 3		Model 4		
	Vignette dimensions		*Demographic variables*		*Respondent attitudes*		*Main effects model*		
	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error	PartR2
Sex (0 = male, 1 = female)			−0.292***	0.059			−0.248***	0.055	0.006
Age category (0–5)			0.120***	0.018			0.096***	0.017	0.009
Education level (0–5)			0.023	0.020			0.002	0.019	0.000
Privacy importance (1–5)					−0.107*	0.046	−0.117**	0.045	0.002
Privacy concerns self (1–5)					0.045	0.046	0.072	0.045	0.001
Privacy concerns others (1–5)					−0.198***	0.043	−0.216***	0.042	0.007
Surveillance concerns (1–5)					−0.052	0.035	−0.057	0.034	0.001
Trust in competence AIVD (1–5)					0.361***	0.055	0.382***	0.054	0.014
Trust in integrity AIVD (1–5)					0.062	0.062	0.061	0.061	0.000
Trust in oversight (1–5)					0.024	0.058	0.016	0.057	0.000
Political orientation (0 = left, 10 = right)					0.083***	0.012	0.071***	0.012	0.011
Trust in institutions (0−10) (composite)					0.047*	0.019	0.047*	0.019	0.002
News interest (1 = very interested, 3 = not)					−0.287***	0.048	−0.150**	0.051	0.002
Model fit									
Loglikelihood	−13,881.2		−14,376.2		−14,222.4		−13,665.5		
ICC	0.509		0.450		0.385		0.438		
Marginal R^2	0.063		0.027		0.130		0.208		
Conditional R^2	0.540		0.465		0.465		0.540		

Note. Multilevel random intercept models. $N = 1.423$.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

Table C1: Regression models predicting vignette acceptance, with Model 4 as the full main effects model, along with three separate models focusing on vignette variables (Model 1), demographic variables (Model 2), and respondent characteristics (Model 3). This breakdown helps clarify the contributions of each set of variables. Since the vignette dimensions are categorical, estimates for each level should be interpreted relative to their reference category (Model 1 and 4). The intercept indicates the average acceptance rate for a vignette with the following reference levels: (1) terrorism, (2) one-time only, (3) a few residents of a country outside the EU, (4) foreign intelligence service, (5) passenger data, and (6) partly retained. For each vignette dimension, the reference category represents the most acceptable vignette level. Estimates for other vignette levels should be interpreted in relation to their respective reference categories, with all other reference categories remaining constant.

In Model 1, the intercept of 6.197 indicates that vignettes with the reference categories were, on average, rated as acceptable. In this model, changing the reference categories to their least acceptable levels (e.g., disinformation, thousands of Dutch residents, hacking, internet traffic data, and fully retained as reference categories) would substantially lower the intercept to 4.350, making vignettes with these levels only slightly more acceptable than unacceptable. In the full model (Model 4), respondent variables are included, which also lowers the intercept. However, the intercept of 4.890 still suggests that vignettes with the reference categories were, on average, rated as more acceptable than unacceptable when accounting for respondent characteristics.

Table C2
Model 5: Multilevel regression model for vignette acceptance with interaction effects.

Coefficient	Estimate	SE	Coefficient	Estimate	SE
Intercept	4.996***	0.339	Interaction effects		
Vignette variables			*Threat type * data subject*		
Threat type			Terrorism * A few non-EU residents (ref.)		
Terrorism (reference)			Trade secrets * A few Dutch residents	−0.234*	0.110
Trade secrets	−0.514***	0.074	Disinformation * A few Dutch residents	−0.072	0.104
Disinformation	−0.722***	0.075	Electricity network * A few Dutch residents	−0.166	0.104
Electricity network	−0.358***	0.075	Trade secrets * Thousands non-EU residents	−0.244*	0.111
Duration			Disinformation * Thousands non-EU residents	−0.030	0.109
Once (ref.)			Electricity network * Thousands non-EU residents	0.037	0.114
Systematically	−0.089**	0.029	Trade secrets * Thousands Dutch residents	−0.334**	0.112
Three months	−0.077*	0.030	Disinformation * Thousands Dutch residents	−0.046	0.110
Data subject			Electricity network * Thousands Dutch residents	−0.143	0.108
A few non-EU residents (ref.)			*Collection method * Data type*		
A few Dutch residents	0.020	0.079	Foreign Intelligence Service * Passenger data (ref.)		
Thousands non-EU residents	−0.253**	0.078	Internet * Contact data	0.151	0.143
Thousands Dutch residents	−0.334***	0.078	Informant * Contact data	0.260*	0.129
Collection method			Organization * Contact data	0.071	0.133
Foreign intelligence service (ref.)			Internet wiretap * Contact data	0.289*	0.133
Internet (open source)	−0.161	0.095	Hacking * Contact data	0.340**	0.131
Informant	−0.169	0.092	Internet * Communication data	0.180	0.137
Organization	−0.217*	0.095	Informant * Communication data	0.219	0.133
Internet wiretap	−0.347***	0.092	Organization * Communication data	0.151	0.136
Hacking	−0.413***	0.096	Internet wiretap * Communication data	0.292*	0.133
Data type			Hacking * Communication data	0.271	0.148
Passenger data (ref.)			Internet * Internet traffic data	0.161	0.136

(*continued on next page*)

Table C2 (*continued*)

Coefficient	Estimate	SE	Coefficient	Estimate	SE
Contact data	−0.231*	0.095	Informant * Internet traffic data	0.024	0.136
Communication data	−0.252*	0.100	Organization * Internet traffic data	0.193	0.144
Internet traffic data	−0.224*	0.098	Internet wiretap * Internet traffic data	0.267*	0.132
Data retention			Hacking * Internet traffic data	0.285*	0.132
Partly retained (ref.)			Model fit		
Fully retained	−0.326***	0.023	Loglikelihood	−13,642.6	
Respondent variables			ICC	0.420	
Sex (0 = male, 1 = female)	−0.248***	0.055	Marginal R^2	0.211	
Age category	0.096***	0.017	Conditional R^2	0.542	
Education level	0.002	0.019			
Privacy importance (1–5)	−0.117**	0.045			
Privacy concerns self (1–5)	0.072	0.045			
Privacy concerns others (1–5)	−0.217***	0.042			
Surveillance concerns (1–5)	−0.057	0.034			
Trust in competence AIVD (1–5)	0.380***	0.054			
Trust in integrity AIVD (1–5)	0.061	0.061			
Trust in oversight (1–5)	0.018	0.057			
Political orientation (0 = left, 10 = right)	0.070***	0.012			
Trust in institutions (0–10) (composite)	0.047*	0.019			
News interest (1 = very interested, 3 = not)	−0.151**	0.051			

Note. Multilevel random intercept model. N = 1.423; *p < .05; **p < .01; ***p < .001.

Appendix D

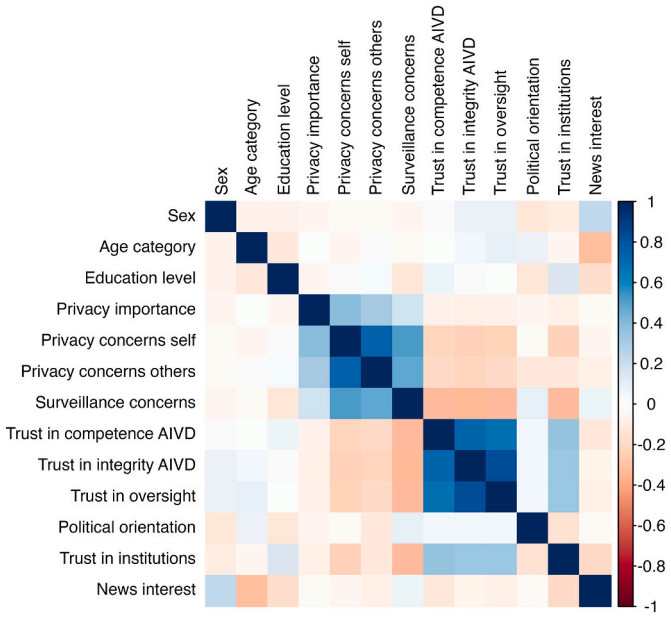

Fig. D1. Correlation matrix of demographic and respondent variables.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Aerdts, W. J. M. (2023). *Diensten met geheimen: Hoe de AIVD en MIVD Nederland veilig houden*. Ambo/Anthos.

AIVD. (2023). Anti-institutioneel extremisme in Nederland: een ernstige dreiging voor de democratische rechtsorde?. Retrieved from https://www.aivd.nl/publicaties/documenten/publicaties/2023/05/25/anti-institutioneel-extremisme-in-nederland-een-ernstige-dreiging-voor-de-democratische-rechtsorde.

AIVD. (2025). Jaarverslag 2024. Retrieved from https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2025/04/24/jaarverslag-2024.

Arsenault, A. C., Kreps, S. E., Snider, K. L., & Canetti, D. (2024). Cyber scares and prophylactic policies: Crossnational evidence on the effect of cyberattacks on public support for surveillance. *Journal of Peace Research, 61*(3), 413–428. https://doi.org/10.1177/00223433241233960

Auspurg, K., & Hinz, T. (2015). *Factorial survey experiments*. Sage Publications.

Ball, K., Degli Esposti, S., Dibb, S., Pavone, V., & Santiago-Gomez, E. (2019). Institutional trustworthiness and national security governance: Evidence from six European countries. *Governance, 32*(1), 103–121. https://doi.org/10.1111/gove.12353

Bates, D., Mächler, M., Bolker, B., & Walker, S. (2015). Fitting linear mixed-effects models using lme4. *Journal of Statistical Software, 67*(1), 1–48. https://doi.org/10.18637/jss.v067.i01

Braithwaite, A. (2013). The logic of public fear in terrorism and counter-terrorism. *Journal of Police and Criminal Psychology, 28*, 95–101. https://doi.org/10.1007/s11896-013-9126-x

Budak, J., & Rajh, E. (2018). Citizens' online surveillance concerns in Croatia. *Surveillance & Society, 16*(3), 347–361. https://doi.org/10.24908/ss.v16i3.6907

Cayford, M., Pieters, W., & van Gelder, P. H. A. J. M. (2019). Wanting it all–public perceptions of the effectiveness, cost, and privacy of surveillance technology. *Journal of Information, Communication and Ethics in Society*.. https://doi.org/10.1108/JICES-11-2018-0087

CBS StatLine. (2022a). Bevolking; geslacht, leeftijd en burgerlijke staat, 1 januari. Retrieved from https://opendata.cbs.nl/statline/#/CBS/nl/dataset/7461bev/table?dl=9E851.

CBS StatLine. (2022b). Bevolking; hoogstbehaald onderwijsniveau en regio. Retrieved from https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85525NED/table?dl=A9DC7.

Conrad, C. R., Croco, S. E., Gomez, B. T., & Moore, W. H. (2018). Threat perception and American support for torture. *Political Behavior, 40*, 989–1009. https://doi.org/10.1007/s11109-017-9433-5

CTIVD. (2020). Review report 71 on the collection and further processing of airline passenger data by the AIVD and the MIVD. https://english.ctivd.nl/documents/review-reports/2020/09/22/review-report-71.

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28–46. https://doi.org/10.1111/j.0092-5853.2004.00054.x

Degli Esposti, S., & Santiago Gómez, E. (2015). Acceptable surveillance-orientated security technologies: Insights from the surprise project. *Surveillance and Society, 13*(3–4), 437–454. https://doi.org/10.24908/ss.v13i3/4.5400

Del-Real, C., & Díaz-Fernández, A. M. (2022). Public knowledge of intelligence agencies among university students in Spain. *Intelligence and National Security, 37*(1), 19–37. https://doi.org/10.1080/02684527.2021.1983984

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–an empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Dor, G., Shandler, R., Gomez, M. A., & Canetti, D. (2024). Fear over facts: how preconceptions explain perceptions of threat following cyberattacks. *Journal of Information Technology & Politics*, 1–16. https://doi.org/10.1080/19331681.2024.2420669

Dülmer, H. (2007). Experimental plans in factorial surveys: Random or quota design? *Sociological Methods & Research, 35*(3), 382–409. https://doi.org/10.1177/0049124106292367

Dvir, R., Geva, N., & Vedlitz, A. (2023). Unpacking public perceptions of terrorism: Does type of attack matter? *Studies in Conflict & Terrorism, 46*(9), 1575–1598. https://doi.org/10.1080/1057610X.2021.1886427

Eck, K., Hatz, S., Crabtree, C., & Tago, A. (2021). Evade and deceive? Citizen responses to surveillance. *The Journal of Politics, 83*(4), 1545–1558. https://doi.org/10.1086/715073

Elshout, S. (2024). *Politics and values – Wave 16*. Centerdata. https://doi.org/10.57990/xhw0-9614

Finkelstein, E. A., Mansfield, C., Wood, D., Rowe, B., Chay, J., & Ozdemir, S. (2017). Trade-offs between civil liberties and National Security: A discrete choice experiment. *Contemporary Economic Policy, 35*(2), 292–311. https://doi.org/10.1111/coep.12188

Garcia, B. E., & Geva, N. (2016). Security versus liberty in the context of counterterrorism: An experimental approach. *Terrorism and Political Violence, 28*(1), 30–48. https://doi.org/10.1080/09546553.2013.878704

Geedy-Gill, T., & Carriere, K. R. (2024). Rights for me but not for thee: Restriction of human rights based on group membership and threat perceptions. *International Journal of Psychology, 59*(2), 246–256. https://doi.org/10.1002/ijop.12941

Gilbert, S., Vitak, J., & Shilton, K. (2021). Measuring Americans' comfort with research uses of their social media data. *Social Media + Society, 7*(3), 1–13. https://doi.org/10.1177/20563051211033824

Greenwald, G., & MacAskill, E. (2013). NSA prism program taps in to user data of apple, google and others. *The Guadian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Hainmueller, J., Hangartner, D., & Yamamoto, T. (2015). Validating vignette and conjoint survey experiments against real-world behavior. *Proceedings of the National Academy of Sciences, 112*(8), 2395–2400. https://www.pnas.org/doi/10.1073/pnas.1416587112.

Hallinan, D., & Friedewald, M. (2012). *Public perception of modern surveillance technologies: A selected survey analysis of the public perception and acceptance of new surveillance technologies*. SSRN. https://doi.org/10.2139/ssrn.2376651

Han, S., Kim, W., & Gordon, Q. (2024). Why Americans support strict counterterrorism measures: Examining the relationship between concern about terrorism and public support for counterterrorism. Peace economics, peace. *Science and Public Policy, 0*. https://doi.org/10.1515/peps-2023-0056

Hijzen, C. (2014). More than a ritual dance. The Dutch practice of parliamentary oversight and control of the intelligence community. *Security and Human Rights, 24*(3–4), 227–238. https://doi.org/10.1163/18750230-02404002

Horvath, L., James, O., Banducci, S., & Beduschi, A. (2023). Citizens' acceptance of artificial intelligence in public services: Evidence from a conjoint experiment about processing permit applications. *Government Information Quarterly, 40*(4), Article 101876. https://doi.org/10.1016/j.giq.2023.101876

Hulsen, S. (2022). *Oud-toezichthouders verdeeld over nieuwe wet die aivd meer ruimte geeft*. RTL. Retrieved from https://www.rtl.nl/nieuws/binnenland/artikel/5343479/toezichthouders-aivd-mivd-verdeeld-over-nieuwe-wet-aftappen.

Jaeger, P. T., Bertot, J. C., & McClure, C. R. (2003). The impact of the USA patriot act on collection and analysis of personal information under the foreign intelligence surveillance act. *Government Information Quarterly, 20*(3), 295–314. https://doi.org/10.1016/S0740-624X(03)00057-1

Jardine, E., Porter, N., & Shandler, R. (2024). Cyberattacks and public opinion–the effect of uncertainty in guiding preferences. *Journal of Peace Research, 61*(1), 103–118. https://doi.org/10.1177/00223433231218178

Jeune, N., Juhel, J., Dessus, P., & Atal, I. (2024). Six factors facilitating teachers' use of research. An experimental factorial survey of educational stakeholders perspectives. *Frontiers in Education, 9*, 1–14. https://doi.org/10.3389/feduc.2024.1368565

Kininmonth, J., Thompson, N., McGill, T., & Bunn, A. (2018). Privacy concerns and acceptance of government surveillance in Australia. In *Australasian conference on information systems 2018*. https://doi.org/10.5130/acis2018.cn. Sydney, Australia.

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., Mc Cluskey, E., & Aradau, C. (2024). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies, 50*(1), 209–229. https://doi.org/10.1017/S0260210523000013

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science, 30*(6), 671–690. https://doi.org/10.1177/09636625211001555

Kuhfeld, W. F. (2010). *Marketing research methods in SAS: Experimental design, choice, conjoint, and graphical techniques*. Cary, NC: SAS Institute.

Kustosch, L., Gañán, C., van't Schip, M., van Eeten, M., & Parkin, S. (2023). Measuring up to (reasonable) consumer expectations: Providing an empirical basis for holding {IoT} manufacturers legally responsible. In *32nd USENIX security symposium (USENIX security 23)* (pp. 1487–1504).

Li, R. G. (2024). Institutional trustworthiness on public attitudes toward facial recognition technology: Evidence from US policing. *Government Information Quarterly, 41*(3), 1–21. https://doi.org/10.1016/j.giq.2024.101941

Liu, C. (2021). Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems. *International Sociology, 37*(3), 391–412. https://doi.org/10.1177/02685809221084446

Macnish, K. (2015). An eye for an eye: Proportionality and surveillance. *Ethical Theory and Moral Practice, 18*, 529–548. https://doi.org/10.1007/s10677-014-9537-5

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science and Technology Law Review, 18*(1), 176–218.

Martin, K., & Nissenbaum, H. (2017). Privacy Interests in Public Records: An Empirical Investigation. *Harvard Journal of Law & Technology (Harvard JOLT), 31*(1), 111–144.

Martin, K., & Nissenbaum, H. (2020). What is it about location? *Berkeley Technology Law Journal, 35*(1), 251–326. https://doi.org/10.15779/Z382F7JR6F

Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics, 111*, 519–539. https://doi.org/10.1007/s10551-012-1215-8

Messick, J. (2023). The impact of gender on the acceptance of surveillance technology. *Sigma: Journal of Political and International Studies, 40*(1), 7. https://scholarsarchive.byu.edu/sigma/vol40/iss1/7.

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs, 51*(1), 133–161. https://doi.org/10.1111/joca.12111

Nam, T. (2017). Does ideology matter for surveillance concerns? *Telematics and Informatics, 34*(8), 1572–1585. https://doi.org/10.1016/j.tele.2017.07.004

Nam, T. (2018). Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management, 38*(1), 262–269. https://doi.org/10.1016/j.ijinfomgt.2017.10.007

Nam, T. (2019). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal, 56*(4), 530–544. https://doi.org/10.1016/j.soscij.2018.10.001

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Offermann-van Heek, J., Arning, K., & Ziefle, M. (2019). All eyes on you! Impact of location, camera type, and privacy-security-trade-off on the acceptance of surveillance technologies. In *Smart cities, green technologies, and intelligent transport systems: 6th international conference, SMARTGREENS 2017, and third international conference, VEHITS 2017, Porto, Portugal, April 22-24, 2017, revised selected papers 6* (pp. 131–149). Springer International Publishing. https://doi.org/10.1007/978-3-030-02907-4_7.

Oomens, E. C., van Wegberg, R. S., Klievink, A. J., & van Eeten, M. J. G. (2023). To trust or to restrict? –mapping professional perspectives on intelligence powers and oversight in the Netherlands using Q-methodology. *Intelligence and National Security*, 1–24. https://doi.org/10.1080/02684527.2023.2239037

Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science, 21*(5), 556–572. https://doi.org/10.1177/0963662510376886

Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior, 75*, 811–825. https://doi.org/10.1016/j.chb.2017.06.007

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly, 32*(2), 129–141. https://doi.org/10.1016/j.giq.2015.01.003

Reimer, T., & Johnson, N. (2023). Public support for counterterrorism efforts using probabilistic computing technologies to decipher terrorist communication on the internet. *Current Psychology, 42*(20), 16908–16922. https://doi.org/10.1007/s12144-022-02753-4

Roeber, B., Rehse, O., Knorrek, R., & Thomsen, B. (2015). Personal data: How context shapes consumers' data sharing with organizations from various sectors. *Electronic Markets, 25*(2), 95–108. https://doi.org/10.1007/s12525-015-0183-0

van der Schelde, A., & Kanne, P. (2025). *Zorgen over veiligheid vergroten draagvlak Europees leger*. Ipsos I&O. https://www.ipsos-publiek.nl/actueel/veranderende-wereldorde-baart-nederlander-zorgen/.

Scherpenzeel, A. C., & Das, M. (2010). "True" longitudinal and probability-based internet panels: Evidence from the Netherlands. In M. Das, P. Ester, & L. Kaczmirek (Eds.), *Social and Behavioral research and the internet: Advances in applied methods and research strategies* (pp. 77–104). Boca Raton: Taylor & Francis.

Schomakers, E. M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity–insights from Germany. *International Journal of Information Management, 46*, 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Schwarz, N. (1999). Self-reports: How the questions shape the answers. *American Psychologist, 54*(2), 93. https://doi.org/10.1037/0003-066X.54.2.93

Seehuus, S. (2023). Gender differences and similarities in work preferences: Results from a factorial survey experiment. *Acta Sociologica, 66*(1), 5–25. https://doi.org/10.1177/00016993211060241

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015. https://doi.org/10.2307/41409970

Snider, K. L., Hefetz, A., Shandler, R., & Canetti, D. (2025). Experimenting with threat: How cyberterrorism targeting critical infrastructure influences support for surveillance policies. *Terrorism and Political Violence, 1-14*. https://doi.org/10.1080/09546553.2025.2457746

Stoffel, M. A., Nakagawa, S., & Schielzeth, H. (2021). partR2: Partitioning R2 in generalized linear mixed models. *PeerJ, 9*, Article e11414. https://doi.org/10.7717/peerj.11414

Sulitzeanu-Kenan, R., Kremnitzer, M., & Alon, S. (2016). Facts, preferences, and doctrine: An empirical analysis of proportionality judgment. *Law & Society Review, 50*(2), 348–382. https://doi.org/10.1111/lasr.12203

Svenonius, O., & Björklund, F. (2018). Explaining attitudes to secret surveillance in post-communist societies. *East European Politics, 34*(2), 123–151. https://doi.org/10.1080/21599165.2018.1454314

Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology, 71*(9), 1129–1142. https://doi.org/10.1002/asi.24372

Torcal, M. (2017). Political trust in western and southern Europe. In S. Zmerli, & T. W. G. van der Meer (Eds.), *Handbook on political trust* (pp. 418–439). Edward Elgar Publishing. https://doi.org/10.4337/9781782545118.00037.

Trein, P., & Varone, F. (2023). Citizens' agreement to share personal data for public policies: Trust and issue importance. *Journal of European Public Policy, 1-26*. https://doi.org/10.1080/13501763.2023.2205434

Treischl, E., & Wolbring, T. (2022). The past, present and future of factorial survey experiments: A review for the social sciences. *Methods, Data, Analyses: A Journal for Quantitative Methods and Survey Methodology (MDA), 16*(2), 141–170. https://doi.org/10.12758/mda.2021.07

Trüdinger, E. M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly, 34*(3), 421–433. https://doi.org/10.1016/j.giq.2017.07.003

Trüdinger, E. M., & Ziller, C. (2022). Considered effective? How policy evaluations and threat perceptions affect support for surveillance in the context of terrorism. *Politics & Policy, 50*(5), 894–912. https://doi.org/10.1111/polp.12498

Tsapogas, D. (2017). The importance of social and political context in explaining citizens' attitudes towards electronic surveillance and political participation 1. In M. Friedewald, J. P. Burgess, J. Čas, R. Bellanova, & W. Peissl (Eds.), *Surveillance, privacy and security: Citizens' perspectives* (pp. 212–232). Routledge.

Valentino, N. A., Neuner, F. G., Kamin, J., & Bailey, M. (2020). Testing Snowden's hypothesis does mere awareness drive opposition to government surveillance? *Public Opinion Quarterly, 84*(4), 958–985. https://doi.org/10.1093/poq/nfaa050

Vitak, J., Liao, Y., Mols, A., Trottier, D., Zimmer, M., Kumar, P. C., & Pridmore, J. (2023). When do data collection and use become a matter of concern? A cross-cultural comparison of US and Dutch privacy attitudes. *International Journal of Communication, 17*, 28.

Vliegenthart, R., Vrielink, J., Dommett, K., Gibson, R., Bon, E., Chu, X., … Kruikemeier, S. (2024). Citizens' acceptance of data-driven political campaigning: A 25-country cross-National Vignette Study. *Social Science Computer Review, 0*(0), 1–19. https://doi.org/10.1177/08944393241249708

Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research, 38*(3), 505–520. https://doi.org/10.1016/j.ssresearch.2009.03.004

Westerlund, M., Isabelle, D. A., & Leminen, S. (2021). The acceptance of digital surveillance in an age of big data. *Technology Innovation Management Review, 11*(3), 32–44. https://doi.org/10.22215/timreview/1427

van Wilsem, J. A., & van der Woude, M. A. H. (2011). Zijn Nederlandse burgers écht enthousiast over de nieuwe antiterrorismemaatregelen? Een vergelijking van attitudes en willingness to pay. *Tijdschrift voor Veiligheid, 10*(3), 17–35. https://scholarlypublications.universiteitleiden.nl/handle/1887/17867.

Ziller, C., & Helbling, M. (2021). Public support for state surveillance. *European Journal of Political Research, 60*(4), 994–1006. https://doi.org/10.1111/1475-6765.12424

E.C. Oomens is a PhD candidate at Delft University of Technology, whose research is primarily focused on the perceptions of citizens on the proportionality of intelligence powers. She studied Sociology at Utrecht University.

R.S. van Wegberg is an associate professor of cybercrime governance at the Faculty of Technology, Policy and Management of Delft University of Technology, in the Organisation & Governance section.

M.J.G. van Eeten is a Professor of Public Administration in the Organisation & Governance research group at Delft University of Technology, and a specialist in Internet security.

A.J. Klievink is a Professor of Public Administration at Leiden University, with a special focus on Digitalisation and Public Policy.