MUNI
FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Liu, W., Lee, S. Y., & Yao, M. Z. (2024). Acceptance and self-protection in government, commercial, and interpersonal surveillance contexts: An exploratory study. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18*(4), Article 9. https://doi.org/10.5817/CP2024-4-9

Acceptance and Self-Protection in Government, Commercial, and Interpersonal Surveillance Contexts: An Exploratory Study

Weizi Liu[1], *Seo Yoon Lee*[2], *& Mike Z. Yao*[3]

[1] Bob Schieffer College of Communication, Texas Christian University, Fort Worth, USA
[2] Digital Media Program, Department of Information Science Technology, University of Houston, Sugar Land, USA
[3] Institute of Communications Research, University of Illinois at Urbana-Champaign, Champaign, USA

Abstract

Digital surveillance is pervasive in cyberspace, with various parties continuously monitoring online activities. The ways in which internet users perceive and respond to such surveillance across overlapping contexts warrants deeper exploration. This study delves into the acceptance of digital surveillance by internet users and their subsequent self-protective actions against it in three distinct contexts: government, commercial, and interpersonal surveillance. Survey responses collected from 356 internet users in the U.S. showed that acceptance levels for surveillance varied between institutional and interpersonal contexts. However, the degree of self-protection remained consistent across all three contexts. Privacy concerns, algorithm awareness, and perceived privacy control played nuanced roles to both surveillance acceptance and self-protection measures in each context. Interestingly, political orientation emerged as a significant moderating factor on surveillance acceptance. Conservative-leaning participants were less accepting of surveillance overall, especially government surveillance. For conservatives, higher privacy concerns meant less acceptance of both government and corporate surveillance. Liberals' acceptance levels remained fairly consistent and were less affected by privacy concerns. These findings underscore the significance of contextual differences in privacy and surveillance research and provide implications for refining the existing theoretical frameworks.

Keywords: digital surveillance; online privacy; algorithm awareness; privacy concerns; privacy control; political orientation; acceptance; self-protection

Editorial Record

First submission received:
May 2, 2023

Revisions received:
August 30, 2023
December 21, 2023
March 11, 2024
July 4, 2024

Accepted for publication:
July 10, 2024

Editor in charge:
Jan Serek

Introduction

Digital surveillance, enabled by information technologies, extends the watch of the powerful and touches upon complicated issues such as privacy, ethics, and human rights. Carried out by different parties, digital surveillance is omnipresent: government agencies are increasingly relying on AI and big data to generate social intelligence (e.g., Dinev et al., 2008); corporations use behavioral tracking and algorithms for marketing and advertising purposes (e.g., Christi et al., 2017); social media enable individuals to follow and stalk other users with ease (e.g., Trottier, 2012). The complexity and nuances of digital surveillance call for continuing research efforts into user attitudes and behaviors. Previous related work has predominantly focused on active information management and voluntary information disclosure, there is a growing need to examine individuals' acceptance of and self-protection against the seamless digital surveillance practices, which are beyond their immediate control (e.g., S. Barth et al., 2019; Baruh et al., 2017).

Surveillance is defined as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon, 2007, p. 14). It is about observing, watching, and potentially compromising personal privacy (Segijn et al., 2022). Surveillance in the digital age is more intense and extensive than its traditional forms (Marx, 2015). As social and communication contexts collapse into one online setting (Marwick & boyd, 2011), personal information and other forms of online data could expose users' digital identities across professional, social, political, economic, and cultural contexts, thus threatening different aspects of privacy. Data about internet users can be monitored and shared across different parties (Gangadharan, 2017), leading to potential legal, security, financial, and interpersonal consequences (Vitak, 2012). On the institutional level, the term "dataveillance" (Büchi et al., 2022; Degli-Esposti, 2014) was defined as "the automated, continuous, and unspecific collection, retention, and analysis of digital traces" (Büchi et al., 2022, p. 1), eliciting concerns of the general public. On the individual level, surveillance by intimate partners, parents, and other cyberstalkers was enabled through the mining of social networking data, triggering tensions in social relationships and threatening personal data security (Trottier, 2012; Zhang et al., 2017). Issues of digital surveillance reflect the privacy-surveillance tensions between individuals and institutions as well as between different individuals (Trottier, 2012). It is thus critical to examine how users assent to or oppose surveillance activities and execute personal power to self-protect against those practices.

There has been rich research on digital surveillance and user privacy experience in a wide range of contexts. For example, researchers applied privacy calculus and asymmetric information theory to understand internet users' privacy concerns and attitudes toward government surveillance (Dinev et al., 2006, 2008); surveillance on consumers was discussed in online marketing and advertising (Kim & Huh, 2017); intimate partner surveillance has been explored from interpersonal and legal perspectives (Fox & Tokunaga, 2015; Levy, 2014). These investigations are usually in-depth and siloed in separate domains, calling for systematic examinations of contextual factors, such as cultural and national backgrounds (e.g., Shin, 2021a; Shin et al., 2022a), participating institutions (e.g., Trottier, 2016), topics of information disclosure (e.g., Bol et al., 2018), as well as affordances and contextual cues on the interface (e.g., Gu et al., 2017; Trepte et al., 2020). Using the contextual integrity framework, Martin and Shilton (2016) employed a factorial vignette survey to measure the impact of various real-world contexts (e.g., medical, navigation, music), data types, and data uses on user privacy expectations. Naeini et al. (2017) used a similar vignette approach to focus on privacy expectations and preferences in IoT data collection and use scenarios. These investigations provide rich evidence of the nuanced and context-dependent nature of privacy, paving the way for more integration and specificity within the diverse yet fragmented body of literature. In this study, we aim to understand users' privacy management under digital surveillance in collapsed contexts, first by establishing a coherent view that connects different surveillance scenarios, and then by comparing contextual nuances.

Our research draws from the theory of planned behavior (TPB) and the theory of contextual integrity (CI). While TPB offers a framework for investigating behavioral mechanisms related to digital surveillance, CI expands our scope to examine these mechanisms across various surveillance contexts. Our primary goal was to examine user acceptance and self-protection in response to digital surveillance across contexts involving various surveillance parties. We sought to delineate disparities in attitudes and behaviors related to digital surveillance and to analyze how the influence of certain contributing factors varies across these contexts. Drawing from existing privacy research, we identified privacy attitudes, knowledge, and control as the main precursors of surveillance acceptance and self-protection. These were further specified as privacy concerns, algorithm awareness, and perceived privacy control.

In our main analyses, we compared acceptance, self-protection, and the effects of these antecedent factors in three contexts: government, commercial, and interpersonal surveillance, given that e-government, e-commerce, and social networking are major online information collectors (Kokolakis, 2017). Additionally, we conducted a series of exploratory analyses examining political beliefs as a significant moderator, particularly relevant to privacy and surveillance in the U.S. We also explored the relationship between surveillance acceptance and self-protection. Our findings enhance the understanding of users' experiences and mindsets concerning privacy and surveillance by various parties. We advocate for further theoretical integration, given the rising but fragmented investigations of contextual issues in the privacy literature. Furthermore, we emphasize the necessity for increased transparency and clearer explanations to improve user comprehension and control over digital platform surveillance activities. This is in line with the crucial role of explainability in promoting user trust and technology acceptance (Shin, 2021b).

Theory of Planned Behavior (TPB) and Surveillance Acceptance and Self-Protection

The TPB specifies three major contributing factors to an individual's behavioral intention and subsequent actions: attitude toward the behavior, beliefs about the surrounding social norms, and perceived control over the performance of the behavior (Ajzen, 1991). In this study, we mainly focus on examining two behavioral tendencies: acceptance of digital surveillance and adoption of self-protection against digital surveillance, using the TPB framework.

Acceptance is an important manifestation of behavioral intentions in privacy literature (Beke et al., 2018; Distler et al., 2020). We may draw the importance of studying acceptance from the "privacy paradox," which refers to the inconsistency between users' privacy-related behaviors and their pervasive privacy concerns (Dienlin & Trepte, 2015). It indicates a mismatch between the actual privacy protection measures and the public sentiment regarding privacy issues that are influenced by major events (e.g., 9/11 and the Snowden revelation; LaRose & Rifon, 2006; Park, 2013). The reasons for the privacy paradox are multifaceted, and existing literature offers a range of interpretations, including privacy calculus, social theories, cognitive biases and illusions, quantum theory, methodological limitations, etc. (Gerber et al., 2018; Kokolaki, 2017). A particularly intriguing perspective we observed suggests that users may adopt a passive mindset in the face of surveillance power, an attitude that might vary based on the surveillance context (Park, 2021). This aligns with the concept of "privacy cynicism" (Lutz et al., 2020), which describes an attitude of uncertainty, powerlessness, skepticism, and resignation toward data management by online services, leading to inaction. Our goal is to explore how individuals, under varying circumstances of digital surveillance, perceive reality, maintain their sense of agency, and exercise control.

Resistance is another central theme in studies on surveillance (Martin et al., 2009). On an individual level, the act of resistance is manifested by users' efforts to protect their personal information against digital monitoring activities. These self-protecting efforts may include changing privacy settings, clearing browsing history, avoiding certain websites, providing fake personal information, deleting social media accounts, and self-censorship, etc. (Park, 2013). By studying acceptance and self-protection in different contexts of digital surveillance, we can further unpack users' privacy processes in a complex set of individual social-psychological behaviors and institutional behaviors. We intend to generate important implications for policymaking and technology designs to build a more context-aware and transparent digital environment.

When applying the TPB to online privacy behaviors, studies have shown that internet users' privacy concerns, knowledge, and self-efficacy are primary antecedents of self-protective actions against privacy threats (Dienlin & Trepte, 2015; Saeri et al., 2014; Yao & Linz, 2008). In this study, given our emphasis on the attitudinal aspect, we specifically concentrate on privacy concerns. Additional privacy literature also highlights awareness and control as two pivotal determinants of privacy-related attitudes and behaviors (Acquisti & Gross, 2006; Park, 2013; Trepte et al., 2015).

Privacy Concerns

Privacy concerns, defined as the general concerns and inherent worries of loss of information privacy (Malhotra et al., 2004; Xu et al., 2011), have been identified as a reliable proxy to measure internet users' attitudes towards online privacy threats in literature (Baruh et al., 2017; Yao & Linz, 2008). Despite the "privacy paradox", privacy concerns remain an effective and parsimonious measure of an individual's general attitude toward privacy threats. In this study, we include privacy concerns in our baseline model as an antecedent to digital surveillance acceptance and self-protection.

Algorithm Awareness

Previous research has demonstrated that people's online privacy-related attitudes and behaviors are influenced by their understanding of the internet and related technologies (S. Barth et al., 2019; Park, 2013; Trepte et al., 2015). As data technologies and algorithmic operations on digital platforms become more prevalent, we focus on user literacy regarding digital surveillance as another key factor in their acceptance and self-protection. Digital surveillance typically involves intricate algorithms to collect, process, and analyze users' behaviors, preferences, and interactions (Bazarova & Masur, 2020; van Dijck et al., 2018). Yet, the extent to which users are aware of these algorithms and their role in surveillance can differ. Lay users, lacking the necessary technical backgrounds, often form specific mental models about privacy and security (Camp, 2009; Oates et al., 2018). These models are conceptual frameworks or cognitive representations that users have regarding how a system or interface functions. However, However, these mental constructs may lack critical technical nuances and could diverge from the system's actual operational mechanisms (Kang et al., 2015; Lin et al., 2012). In this context, the way users perceive and understand algorithms would play a crucial role in their attitudes and interaction with digital systems (Shin, 2020; Shin, 2021a). Therefore, we highlight "algorithm awareness"—an accurate understanding of algorithmic functions and impacts (Gran et al., 2021; Shin et al., 2022b; Zarouali et al., 2021)—as a potential determinant of surveillance acceptance and self-protection. The degree of algorithm awareness among internet users may shape their affective and cognitive evaluations of digital surveillance. Enhanced awareness might induce heightened apprehension regarding surveillance-related activities, potentially resulting in users' resistance and disengagement (Baruh et al., 2017; Kosinski et al., 2013).

Perceived Privacy Control

According to the TPB, behavioral control, the degree to which an individual believes that the desired behavior is under their control, is a strong predictor of behavioral intention and a critical factor leading to the performance of this behavior (Ajzen, 1991; Pavlou, 2002; Yao & Linz, 2008). Perceived privacy control is defined as an individual's perceptions and beliefs in their ability to manage the exposure and dissemination of personal information (Xu et al., 2011). Not only does perceived privacy control determine users' privacy decision-making behaviors (e.g., Baruh et al., 2017; Taddei & Contena, 2013), but also it reflects users' dispositions and expectations in their thought processes. High perceived privacy control may indicate users' high confidence in their own ability to protect themselves, therefore, they may have a rather relaxed and optimistic attitude toward digital monitoring and may actively engage in self-protection measures (Boerman et al., 2021; Dienlin & Metzger, 2016). As for digital surveillance, perceived privacy control is indicative of users' overall assessment of their agency and autonomy against external factors, such as advanced technology and the power of the surveyors.

Contextual Integrity (CI) and Surveillance Acceptance and Self-Protection in Varying Social Contexts

It is difficult to assess digital surveillance and privacy violations without context. Context refers to "the type of institution and organization in question and to the goals, rules, and expectations they are associated with" (Marx, 2015, p. 734). Expanding beyond a singular scenario, the theory of contextual integrity (CI) introduced by Nissenbaum (2004) addresses the appropriateness of specific information exchanges based on privacy norms, questioning whether a unified behavioral mechanism can be applicable across diverse privacy contexts. This theory suggests that people possess expectations about which information should be shared in various social contexts. These expectations are molded by the norms and values of the social groups they are affiliated with. CI serves as a conceptual framework to elucidate privacy expectations and their ramifications on law, public policy, and political philosophy (A. Barth et al., 2006). While TPB enables us to explore behavioral mechanisms in a specific context, CI introduces another dimension for comparison across diverse contexts. This complements our understanding by emphasizing the type of information collected, its recipient, and its usage as the transmission principles. For instance, by applying CI, Martin and Nissenbaum (2017) uncovered how context and the purpose of information collection influenced confounding variables (i.e., privacy categories and users' judgment of information sensitivity) to explain the disconnections between people's privacy actions and their serious concerns.

To study contextual factors, Xu et al. (2008) advocated an integrated view of individual privacy concerns by testing a privacy model with users from e-commerce, social networking, financial, and healthcare sites; Bol et al. (2018) emphasized the context-dependency of privacy and examined the difference in self-disclosure towards personalization across health, news, and commerce contexts; Trottier (2016) presented ethnographic research on surveillance in social media by separating individual, institutional, market-based, security, and intelligence forms of surveillance that happen on the same site; furthermore, Bazarova and Masur (2020) systematically reviewed individualistic, networked, and institutional approaches to disclosure and privacy research. They contended that while the three distinct approaches exist in the literature, the collapse of context and the blurred boundaries between the public and private spheres in the digital space necessitate the integration of these approaches with a multifaceted perspective.

Research Questions

In this study, we investigate users' differing levels of acceptance and self-protection against digital surveillance activities across government, commercial, and interpersonal contexts. Informed by TPB, we focus on users' privacy concerns, algorithm awareness, and perceived control to construct a general framework for the comparison across contexts. Considering the robustness of the TPB in predicting a wide range of social behaviors (Saeri et al., 2014), including online privacy-related beliefs and actions, our goal is not to re-evaluate and retest the theory itself but to utilize it as a baseline model of surveillance acceptance and self-protection. Subsequently, drawing inspiration from CI, we examine how this baseline model manifests varying privacy norms in the governmental, commercial, and interpersonal surveillance contexts. Later, we further tested the role of political orientation and the link between acceptance and self-protection exploratorily. Our main exploration begins with:

RQ1: Do internet users exhibit varying levels of (a) acceptance and (b) self-protection in the government, commercial, and interpersonal surveillance contexts?

RQ2: How do users' privacy concerns, algorithm awareness, and perceived privacy control influence (a) acceptance and (b) self-protection across government, commercial, and interpersonal surveillance contexts?

Much privacy research based on TPB has examined the effects of behavioral beliefs (e.g., Baruh et al., 2017; Dinev & Hart, 2004; Joinson et al., 2010) and control beliefs (e.g., Chen et al., 2008; Taddei & Contena, 2013; Xu et al., 2011) on privacy-related attitudes and behaviors. However, normative beliefs have received less attention in this discourse. Normative beliefs pertain to "the likelihood that important referent individuals or groups approve or disapprove of performing a given behavior" (Ajzen, 2002, p. 195). This perspective prompts us to consider not only unified behavioral mechanisms but also population segmentations. Typically, privacy-related attitudes and behaviors are delineated by socio-demographics and political views as distinct grouping factors (Bergström, 2015). Notably, in the US context, a survey revealed that Americans' views on surveillance are primarily influenced by party affiliation and political ideology, outweighing factors like income, age, gender, and race/ethnicity (Turow et al., 2018). The results indicate that conservative Republicans are generally more receptive to surveillance than liberal Democrats.

It is crucial to recognize that the relationship between political orientation and privacy concerns is intricate and can shift depending on the context. When discussing government-based or corporate-based large-scale surveillance, individuals' political attitudes can further polarize their views on government regulation and corporate freedom (Rosenberg, 2005). While liberals and conservatives may find common ground on many overarching privacy issues, they can differ significantly in their support for government regulations and market interventions (Westin, 2003). Such socio-political dimensions of privacy-related attitudes are predominantly addressed at the societal level in political science literature (Margulis, 2003). Adopting a behavioral perspective, we integrate political orientation as a normative factor through the TPB lens. We aim to discern the role of political orientation in surveillance acceptance and self-protection mechanisms across contexts and ask the following research question:

RQ3: What is the role of political orientation in predicting surveillance acceptance and protection in different surveillance contexts?

While it is intuitive and logical to expect a negative association between the acceptance of surveillance and the adoption of self-protection measures, existing research is insufficient, and evidence of such negative correlations has been inconsistent. Some researchers did not find significant associations between attitudes toward acceptance and protection behavior (Thompson et al., 2020), while others identified a significant positive correlation (Ioannou & Tussyadiah, 2021). These findings point to a need to explore the nuances. Therefore, we raise another research question:

RQ4: What is the relationship between surveillance acceptance and self-protection in government, commercial, and interpersonal surveillance contexts?

Methods

Sample and Procedure

With approval from the IRB in September 2021, we administered an online survey via Amazon Mechanical Turk. Three hundred seventy-nine English-speaking adult respondents, currently residing in the US, completed the survey questionnaire. After excluding 23 participants who failed the attention checks, our final sample comprised 356 participants (44.4% females). Participants indicated their age in numeric values, which ranged from 23 to 78 (*M* = 42.10, *SD* = 11.89). Among the sample, 79.8% of the participants were white, 9% were Black or African American, 6.7% were Asian, 1.1% were American Indian or Alaska Native, and 1.1% were mixed races. Informed consent was obtained from all participants.

In the survey, participants answered questions about their general experience of internet use, privacy concerns, perceived privacy control, and algorithm awareness; then they reported their acceptance of and self-protection behavior against the government, commercial, and interpersonal surveillance in random order; political orientation and demographics were measured in later sections.

Measures

Acceptance of Surveillance

We included 7 items based on the common information collection practices (e.g., IP address, phone number, location, etc.) discussed in previous studies (e.g., Thompson et al., 2020). To assess the acceptance of digital surveillance, participants were asked to indicate the extent to which they accept digital monitoring activities in the three contexts individually in different blocks (e.g., please indicate your acceptance of the following digital monitoring activities by *government agencies*, *business corporations,* and *individuals*) on a 5-point Likert scale (1 = *Completely do not accept to* 5 = *Completely accept*). These 7 items were measured repeatedly in each block and demonstrated good reliability in each context (government: α = .95; commercial: α = .89; interpersonal: α = .94). We averaged the 7 items to create the acceptance score for the government, commercial, and interpersonal contexts (M_{gov} = 2.41, SD_{gov} = 1.18; M_{com} = 2.49, SD_{com} = 1.06; M_{inter} = 2, SD_{inter} = 1.13).

Self-Protection Against Surveillance

Mirroring the acceptance measure, we measured self-protection against digital surveillance with the same 7 items. Participants were asked to indicate how often they take action to protect their information against the following digital monitoring activities from government agencies, business corporations, and individuals separately on a 5-point Likert scale (1 = *Never* to 5 = *Always*). Cronbach's alphas (government: α = .93; commercial: α = .88; interpersonal: α = .92) demonstrated good reliability, we averaged the 7 items to gauge the self-protection of surveillance in government, commercial, and interpersonal contexts (M_{gov} = 3, SD_{gov} = 1.21; M_{com} = 3.12, SD_{com} = 1.02; M_{inter} = 3.48, SD_{inter} = 1.16).

Privacy Concerns

We used a 4-item scale adapted from Thomson et al. (2015), which included statements such as *I'm concerned that the information about myself will be used in a way I did not foresee*. Participants were asked to indicate to what extent they agree or disagree with the statements on a 5-point Likert scale (1 = *Strongly disagree* to 5 = *Strongly agree*). As Cronbach's alpha (.84) demonstrated good reliability of the scales, we averaged the 4 items to generate the overall privacy concerns (*M* = 3.78, *SD* = 0.90).

Perceived Privacy Control

A 4-item scale adapted from Xu et al. (2011) was used to measure perceived privacy control. The scale included statements such as *I believe I have control over who can get access to my personal information collected online*. Participants were asked to indicate to what extent they agree or disagree with the statements on a 5-point Likert scale (1 = *Strongly disagree* to 5 = *Strongly agree*). As Cronbach's alpha (.93) demonstrated good reliability of the scales, we averaged the 4 items to generate the overall perceived privacy control (*M* = 2.77, *SD* = 1.18).

Algorithm Awareness

We adopted the 14-item scale from Zarouali et al. (2021), which included descriptions related to algorithmic activities such as *The fact that algorithms use my personal data to recommend certain media content has consequences for my online privacy*. Participants were asked to indicate their awareness of these situations on a 5-point Likert scale (1 = *Not at all aware* to 5 = *Completely aware*). As Cronbach's alpha (.91) demonstrated good reliability of the scales, we averaged the 14 items to generate the overall algorithm awareness (*M* = 4.06, *SD* = 0.64).

Political Orientation

People's political orientation was measured on a 7-point Likert scale (1 = *Strongly conservative* to 7 = *Strongly liberal*).

Results

Testing the Baseline Model of Surveillance Acceptance and Self-Protection

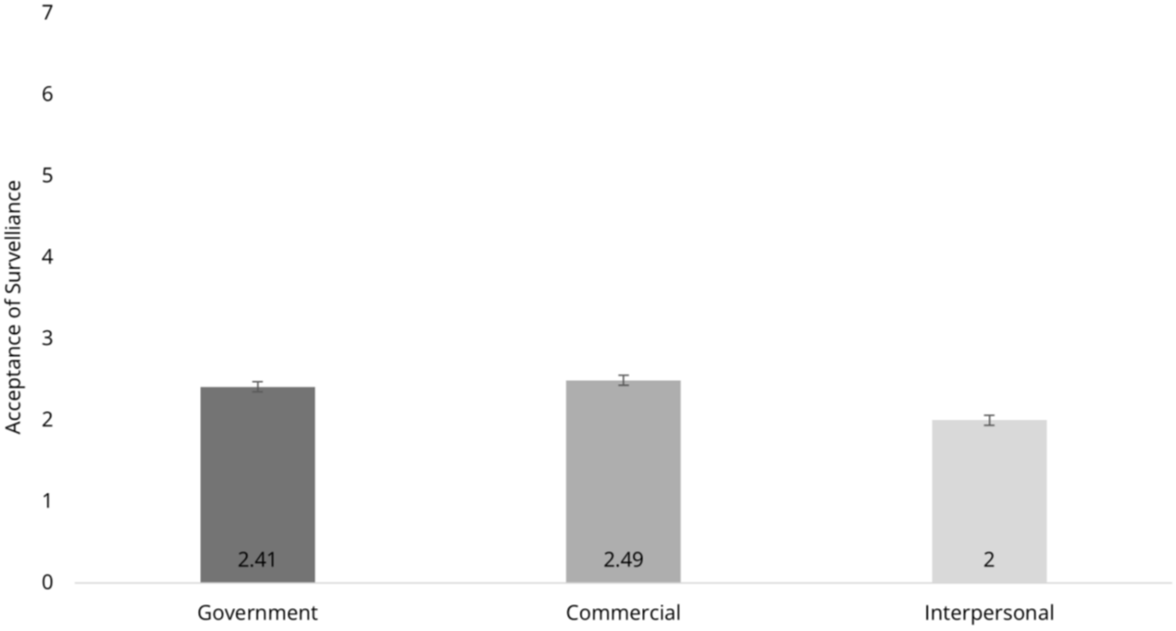
Before answering the research questions, we first tested the baseline assumptions with privacy concerns, algorithm awareness, and perceived privacy control as three key predictors of surveillance acceptance and self-protection. We created a composite index of general surveillance acceptance and self-protection by aggregating the scores across government, commercial and interpersonal surveillance contexts. Age and gender were set as control variables throughout the analyses. Gender was dummy coded (1= *female*, 0 = *male*) and entered into the first step of analyses.

Regression analysis revealed that regarding acceptance, only perceived privacy control was a significant factor that influences acceptance (β = .44, *p* < .001). Privacy concerns (β = −.05, *p* = .268) and algorithm awareness (β = −.08, *p* = .072) were not significant. However, for general self-protection, privacy control (β = .20, *p* < .001), privacy concerns (β = .31, *p* < .001), and algorithm awareness (β = .13, *p* = .017) were all significantly associated with self-protection against surveillance.

Contextual Differences in Surveillance Acceptance and Self-Protection

To answer RQ1(a), we conducted a one-way repeated measures ANCOVA to test the contextual differences in surveillance acceptances. The results showed that contexts significantly influence the level of acceptance of surveillance; *F*(2, 706) = 3.72, *p* = .027, η^2 = .10. While observing a floor effect, a planned contrast revealed that participants' acceptance of interpersonal surveillance (*M* = 2.00, *SE* = .06) was significantly lower than that of government surveillance (*M* = 2.41, *SE* = .06, *p* < .001) and commercial surveillance (*M* = 2.49, *SE* = .06, *p* < .001); no significant difference in acceptance was found between the government and the commercial contexts (see Figure 1). To answer RQ1(b), a similar ANCOVA with self-protection as the dependent variable indicated that people's protection against surveillance from government, commercial and individual contexts did not differ; *F*(2, 706) = 1.02, *p* = .357, η^2 = .00.

Figure 1. *Acceptance of Surveillance in Government, Commercial, and Interpersonal Contexts.*



To answer RQ2(a), we ran a series of hierarchical linear regressions, setting privacy concerns, algorithm awareness, and perceived privacy control as predictors, demographic variables as control variables, and acceptance of surveillance as the dependent variable in the three contexts (see Table 1). In the government context, perceived privacy control was the only significant predictor of surveillance acceptance (β = .39, *p* < .001). The same pattern was found in the commercial context. These results suggest that individuals with greater perceived control over their online privacy would be more likely to accept surveillance from both the government and corporations (β = .35, *p* < .001). In the interpersonal context, both perceived privacy control (β = .44, *p* < .001) and algorithm awareness (β = −.15, *p* = .002) were significantly related to surveillance acceptance. Still, privacy concerns were not significant. People who perceive greater control are more likely to accept interpersonal surveillance; those who are less knowledgeable about how algorithms work are more likely to accept interpersonal surveillance.

Table 1. *Standardized Regression Results of the Association Between Antecedents (Privacy Concerns, Algorithm Awareness, Perceived Privacy Control) Acceptance of Surveillance.*

		Acceptance of surveillance											
		Government				Commercial				Interpersonal			
		β	*B*	*SE*	*p*	β	*B*	*SE*	*p*	β	*B*	*SE*	*p*
Step 1	Age	−.16	−.02	.01	.002	−.15	−.01	.01	.004	−.18	−.02	.01	.001
	Gender	.02	.04	.13	.730	−.09	−.18	.11	.109	−.01	−.03	.12	.796
	R^2	.03				.04				.03			
Step 2	Age	−.07	−.01	.01	.173	−.07	−.01	.01	.182	−.06	−.01	.01	.250
	Gender	.04	.10	.12	.387	−.06	−.14	.11	.200	.00	.01	.11	.940
	PC	−.06	−.08	.07	.249	−.07	.09	.06	.148	−.01	−.02	.06	.797
	PPC	.39	.39	.05	< .001	.35	.31	.05	< .001	.44	.42	.05	< .001
	AA	−.04	−.07	.09	.477	−.03	−.05	.09	.542	−.15	−.27	.09	.002
	R^2	.19				.17				.27			

Note. *N* = 356. The abbreviation PC denotes privacy concerns, PPC denotes perceived privacy control, and AA denotes algorithm awareness.

In summary, privacy concerns were not a significant predictor of acceptance in any of the three surveillance contexts; algorithm awareness negatively affected acceptance but only in the interpersonal context; perceived privacy control was positively associated with acceptance in all three contexts.

To answer RQ2(b), the same regression model was tested but with self-protection as the dependent variable (see Table 2). In the government context, privacy concern (β = .16, *p* = .002) and perceived privacy control (β = .30, *p* < .001) were significantly associated with protection. People who are more concerned about their privacy and perceive greater control are more likely to protect themselves from government surveillance. In the commercial context, all three predictors were positively associated with protection against surveillance (privacy concern β =

.29, $p < .001$; perceived privacy control $\beta = .27$, $p < .001$; algorithm awareness $\beta = .19$, $p = .020$). A similar result was found in the interpersonal context. People who scored high on privacy concern ($\beta = .12$, $p = .023$), perceived privacy control ($\beta = .21$, $p < .001$), and algorithm awareness ($\beta = .20$, $p < .001$) are more likely to take self-protective actions against commercial and interpersonal surveillance.

Table 2. *Standardized Regression Results of the Association Between Antecedents (Privacy Concerns, Algorithm Awareness, Perceived Privacy Control) Protection Against Surveillance.*

		Protection against surveillance											
		Government				Commercial				Interpersonal			
		β	*B*	*SE*	*p*	β	*B*	*SE*	*p*	β	*B*	*SE*	*p*
Step 1	Age	−.11	−.01	.01	.046	−.08	−.01	.01	.130	−.05	−.01	.01	.352
	Gender	−.15	−.35	.13	.006	.13	−.27	.11	.012	−.11	−.25	.12	.041
	R^2		.04				.04				.03		
Step 2	Age	−.06	−.01	.01	.281	−.05	−.00	.00	.344	−.04	−.00	.01	.408
	Gender	−.12	−.30	.12	.017	−.10	−.21	.10	.045	.08	-.17	.11	.139
	PC	.16	.22	.07	.002	.25	.29	.06	< .001	.12	.15	.06	.023
	PPC	.30	.31	.06	< .001	.32	.27	.05	< .001	.21	.20	.05	< .001
	AA	.02	.04	.10	.662	.12	.19	.08	.020	.20	.34	.09	< .001
	R^2		.13				.17				.27		

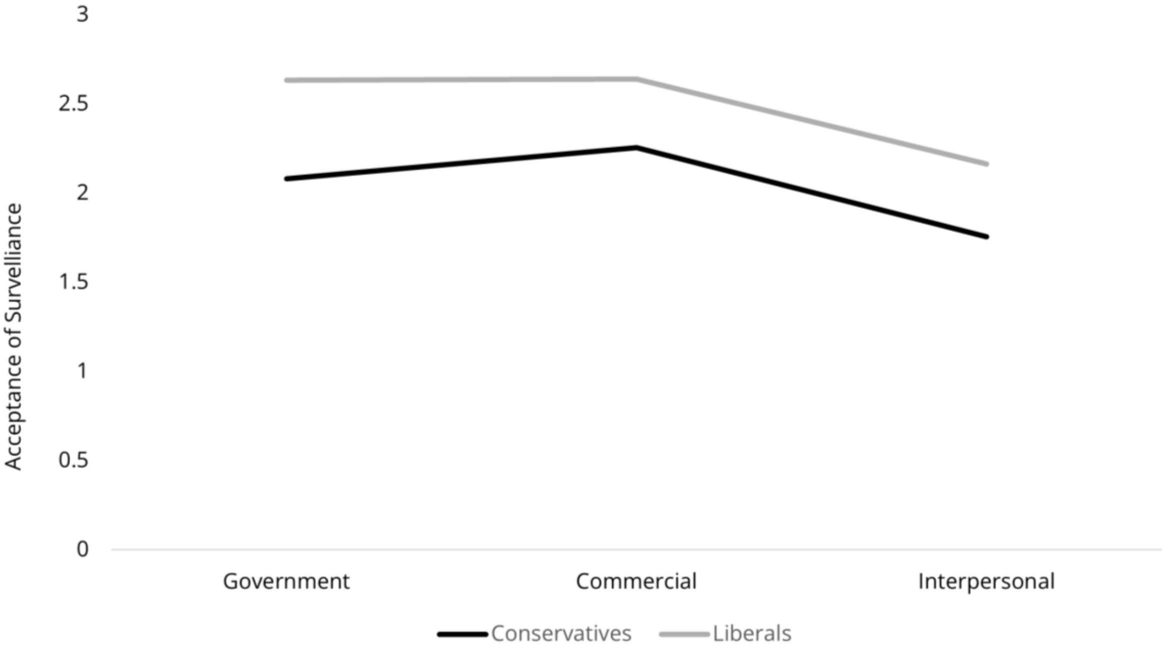
Note. $N = 356$. The abbreviation PC denotes privacy concerns, PPC denotes perceived privacy control, and AA denotes algorithm awareness.

In summary, privacy concerns and perceived privacy control positively affected self-protection in all surveillance contexts; algorithm awareness positively affected self-protection in commercial and interpersonal contexts while was not significant in the government context.

The Role of Political Orientation

To answer RQ3, we first explored the role of political orientation by conducting repeated measures ANCOVAs with political orientation as a moderator of a) the relationship between context and surveillance acceptance and b) the relationship between context and self-protection against surveillance. In analysis a), Mauchly's test suggested a violation of sphericity, $\chi^2(2) = .94$, $p < .001$, so we corrected the degrees of freedom by using the Huhnh-Feldt estimate of sphericity ($\varepsilon = .96$). There was a significant interaction effect of political orientation and contexts on acceptance of surveillance while setting gender and age as covariates, $F(1.92, 677.13) = 3.78$, $p = .025$. As shown in Figure 2, after median split, participants who leaned towards conservative ($n = 143$) were less likely to accept the surveillance from all three parties. The gap between the conservatives and liberals ($n = 211$) was the largest in the government context. A similar analysis was conducted for b). No significant interaction effect of political orientation and contexts was detected on self-protection, $F(1.89, 668.60) = 0.61$, $p = .536$. Political orientation only moderated the contextual effects on surveillance acceptance.

Figure 2. *The Moderating Effect of Political Orientation on the Association Between Contexts and Acceptance of Surveillance.*



We further explored if political orientation moderated the relationships between the antecedents and acceptance of surveillance in the three contexts. A set of hierarchical regressions were conducted. Stepwise, we entered control variables (age and gender), the three antecedents, and the interaction terms for each antecedent and political orientation (see Table 3). The variables were centered to avoid multicollinearity.

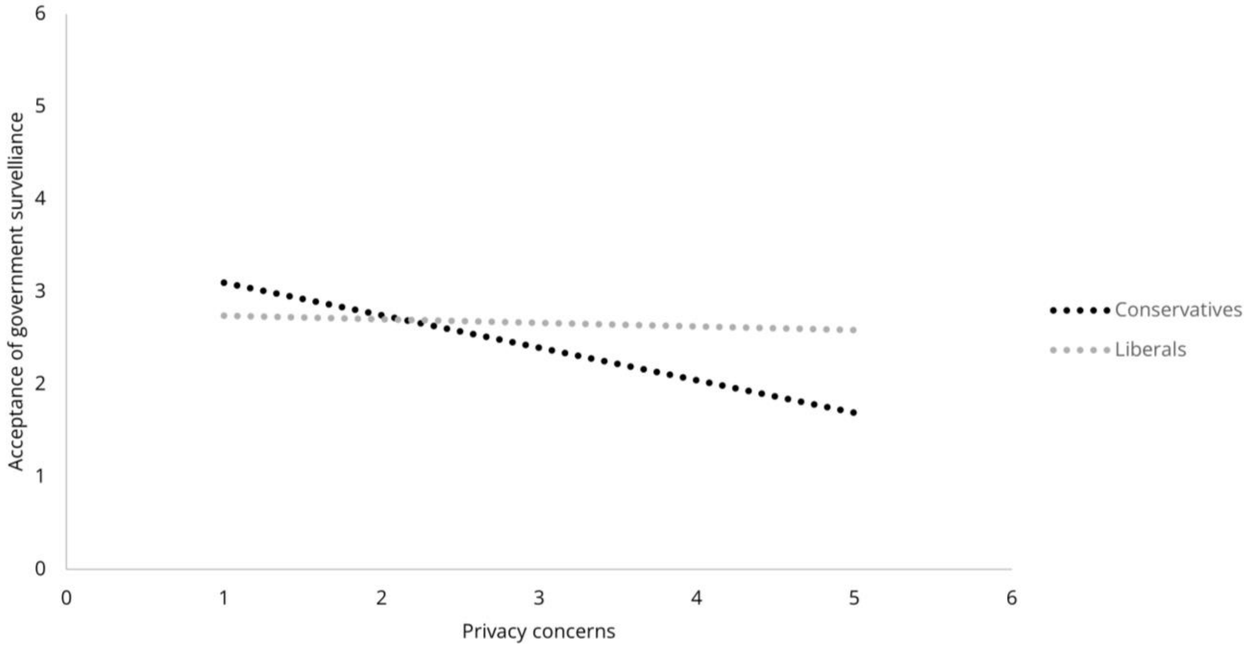
Table 3. *The Regression Results About the Moderating Role of Political Orientation on the Association Between Antecedents (Privacy Concerns, Algorithm Awareness, Perceived Privacy Control) and Acceptance of Surveillance.*

		Acceptance of surveillance											
		Government				Commercial				Interpersonal			
		β	*B*	*SE*	*p*	β	*B*	*SE*	*p*	β	*B*	*SE*	*p*
Step 1	Age	−.16	−.02	.01	.002	−.15	−.01	.01	.004	−.18	−.02	.01	.001
	Gender	.02	.04	.13	.730	−.09	−.18	.11	.109	−.01	−.03	.12	.796
	R^2	.03				.04				.03			
Step 2	Age	−.07	−.01	.01	.173	−.07	−.01	.01	.182	−.06	−.01	.01	.250
	Gender	.04	.10	.12	.387	−.06	−.14	.11	.200	.00	.01	.11	.940
	PC	−.06	−.08	.07	.249	−.07	−.09	.06	.148	−.01	−.02	.06	.797
	PPC	.39	−.07	.05	< .001	.35	.31	.05	< .001	.44	.42	.05	< .001
	AA	−.04	.39	.09	.477	−.03	−.05	.09	.542	−.15	−.27	.09	.002
	R^2	.19				.17				.27			
Step 3	Age	−.06	−.01	.01	.266	−.06	−.01	.00	.215	−.05	−.01	.01	.293
	Gender	.03	.08	.11	.476	−.07	−.16	.10	.137	.00	.00	.11	.980
	PC	−.05	−.07	.06	.270	−.08	−.09	.06	.111	−.01	−.01	.06	.811
	PPC	.40	.40	.05	< .001	.35	.31	.05	< .001	.45	.43	.05	< .001
	AA	−.05	−.09	.09	.331	.04	−.07	.03	.394	−.15	−.27	.09	.002
	PO	.13	.09	.03	.009	.04	.02	.03	.437	.05	.03	.03	.291
	PC*PO	.14	.10	.04	.006	.18	.12	.03	< .001	.01	.01	.03	.780
	PPC*PO	.05	.03	.03	.347	.04	.02	.03	.399	.07	.04	.03	.142
	AA * PO	.07	.08	.06	.164	.06	.06	.05	.272	.08	.09	.05	.100
	R^2	.24				.21				.28			

Note. The abbreviation PC denotes privacy concerns, PPC denotes perceived privacy control, AA denotes algorithm awareness, and PO denotes political orientation (lower scores indicate higher level of conservatism and higher scores indicate higher level of liberalism).

We found that political orientation significantly moderated the associations between privacy concerns and surveillance acceptance in government (β = .14, *p* = .006) and commercial (β = .18, *p* = .001) contexts. As in Figure 3 and Figure 4, conservatives were less likely to accept surveillance from the government and corporations if they had greater privacy concerns. However, for liberals, the slopes were relatively flat, indicating that acceptance of government and commercial surveillance may not drastically change with privacy concerns. In the interpersonal context, we detected no significant moderation effects of political orientation on the associations between the three antecedents and acceptance of interpersonal surveillance.

Figure 3. *The Moderating Role of Political Orientation on the Association Between Privacy Concerns and Acceptance of Government Surveillance.*



As for self-protection, political orientation only significantly moderated the association between algorithm awareness and self-protection in the commercial context (β = .11, *p* = .040, see Table 4). As shown in Figure 5, overall, participants who scored high on algorithm awareness were more likely to protect themselves from commercial surveillance while the relationship is subtly stronger for the liberals than the conservatives. However, the difference is rather marginal and may need further confirmation.

Figure 4. *The Moderating Role of Political Orientation on the Association Between Privacy Concerns and Acceptance of Commercial Surveillance.*

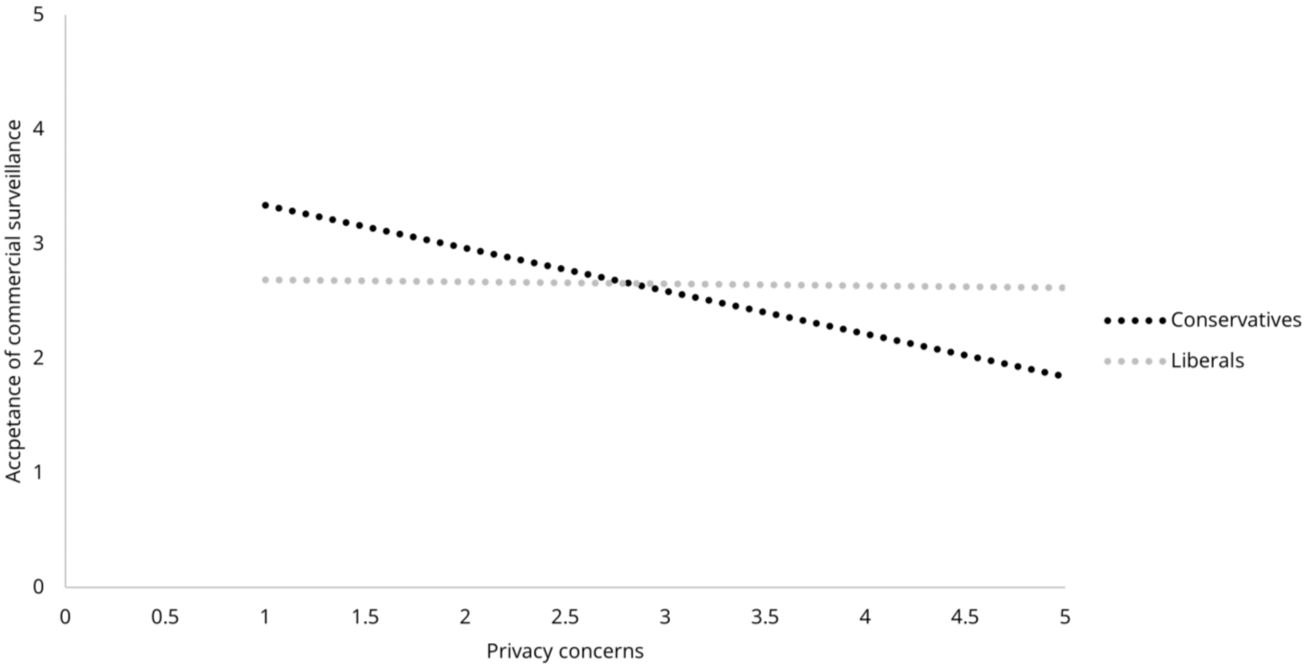
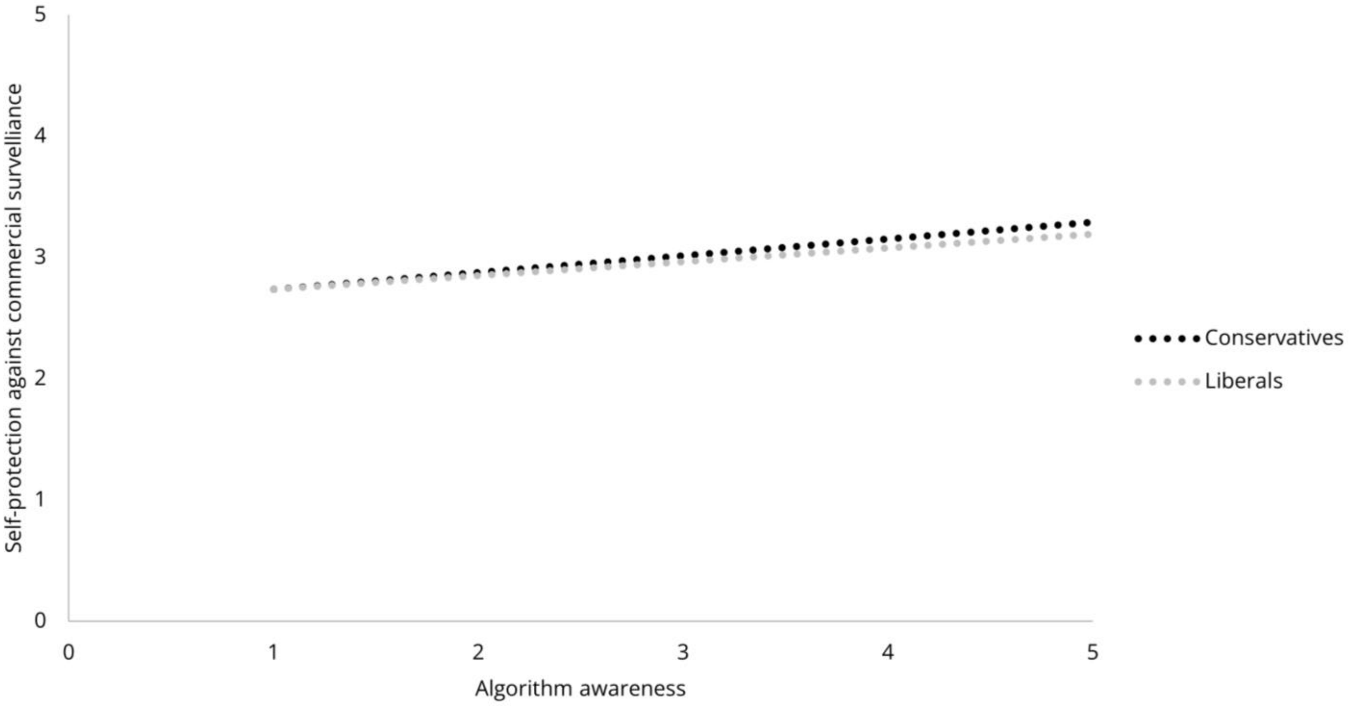


Table 4. *The Regression Results About the Moderating Role of Political Orientation on the Association Between Antecedents (Privacy Concerns, Algorithm Awareness, Perceived Privacy Control and Protection Against Surveillance.*

		Protection against surveillance											
		Government				Commercial				Interpersonal			
		β	*B*	*SE*	*p*	β	*B*	*SE*	*p*	β	*B*	*SE*	*p*
Step 1	Age	−.11	−.01	.01	.046	−.08	−.01	.01	.130	−.05	−.01	.01	.352
	Gender	−.15	−.35	.13	.006	−.13	−.27	.11	.012	−.11	−.25	.12	.041
	R^2	.04				.03				.02			
Step 2	Age	−.06	−.01	.01	.281	−.05	−.00	.00	.344	−.04	−.00	.01	.408
	Gender	−.12	−.30	.12	.017	−.10*	−.21	.10	.045	−.08	−.17	.12	.139
	PC	.16	.22	.07	.002	.25	.29	.06	< .001	.12	.15	.07	.023
	PPC	.30	.31	.06	< .001	.32	.27	.05	< .001	.21	.20	.05	< .001
	AA	.02	.04	.10	.662	.12	.19	.08	.020	.20	.34	.09	< .001
	R^2	.13				.16				.09			
Step 3	Age	−.06	−.01	.01	.228	−.06	−.01	.00	.284	−.05	−.01	.01	.367
	Gender	−.12	−.30	.13	.018	−.10*	−.21	.10	.038	−.08	−.18	.12	.131
	PC	.16	.21	.07	.003	.24	.27	.06	< .001	.11	.14	.07	.035
	PPC	.30	.31	.06	< .001	.32	.27	.05	< .001	.21	.20	.05	< .001
	AA	.02	.04	.10	.661	.12	.18	.08	.025	.19	.34	.09	< .001
	PO	−.07	−.05	.04	.179	−.07	−.04	.03	.186	−.04	−.03	.03	.405
	PC*PO	−.02	−.01	.04	.744	.03	.02	.03	.569	.02	.01	.04	.759
	PPC*PO	.05	.03	.03	.331	.09	.05	.03	.067	.07	.04	.03	.181
	AA*PO	.05	.06	.06	.310	.11	.10	.05	.040	.07	.08	.06	.172
	R^2	.14				.18				.10			

Note. The abbreviation PC denotes privacy concerns, PPC denotes perceived privacy control, AA denotes algorithm awareness, and PO denotes political orientation (lower scores indicate higher level of conservatism and higher scores indicate higher level of liberalism).

Figure 5. *The Moderating Role of Political Orientation on the Association Between Algorithm Awareness and Protection From Commercial Surveillance.*



Linking Surveillance Acceptance and Self-Protection

To answer RQ4, we ran a set of simple linear regressions. No significant relationships between acceptance of surveillance and self-protection against surveillance were detected in the three contexts (see Table 5).

Table 5. *Standardized Regression Results of the Association Between Acceptance of Surveillance and Protection Against Surveillance.*

		Protection against surveillance											
		Government				Commercial				Interpersonal			
		β	*B*	*SE*	*p*	β	*B*	*SE*	*p*	β	*B*	*SE*	p
Step 1	Age	−.11	−.01	.01	.046	−.08	−.01	.01	.130	−.05	−.01	.01	.130
	Gender	−.15	−.35	.13	.006	−.13	−.27	.11	.012	−.11	−.25	.12	.012
	R^2	.03				.02				.04			
Step 2	Age	−.11	−.01	.01	.044	−.09	−.01	.01	.082	−.06	−.01	.01	.082
	Gender	−.15	−.35	.13	.007	−.14	−.29	.11	.008	−.11	−.25	.12	.008
	Acceptance	−.02	−.02	.05	.773	−.09	−.08	.05	.113	−.05	−.05	.05	.113
	R^2	.04				.02				.07			

To further explore the reason for the insignificant results, we conducted post-hoc analyses. As perceived privacy control has been a strong factor in both previous studies and our analyses, we examined whether privacy control played a role in the relationships between acceptance and self-protection. The results showed that the interaction of surveillance acceptance and perceived privacy control were significantly and positively associated with self-protection in all three contexts (government: β = .17, *B* = .15, *p* < .001; commercial: β = .26, *B* = .20, *p* < .001; interpersonal: β = .17, *B* = .14, *p* = .031). The relationships between surveillance acceptance and self-protection are opposite in the low and high perceived privacy control groups: for participants with a lower level of perceived privacy control, the less they accept surveillance, the more they engage in self-protection; for participants with a higher level of perceived privacy control, more acceptance leads to greater self-protection (See Figure 6, 7, and 8). To be cautious about over-interpretation, we could say that the post-hoc analyses provided unexpectedly inspiring implications: the insignificant relationships between surveillance acceptance and protection could be explained by potential opposite mechanisms canceling out each other.

Figure 6. *The Moderating Effect of Perceived Privacy Control Between Surveillance Acceptance and Self-Protection in the Government Context.*

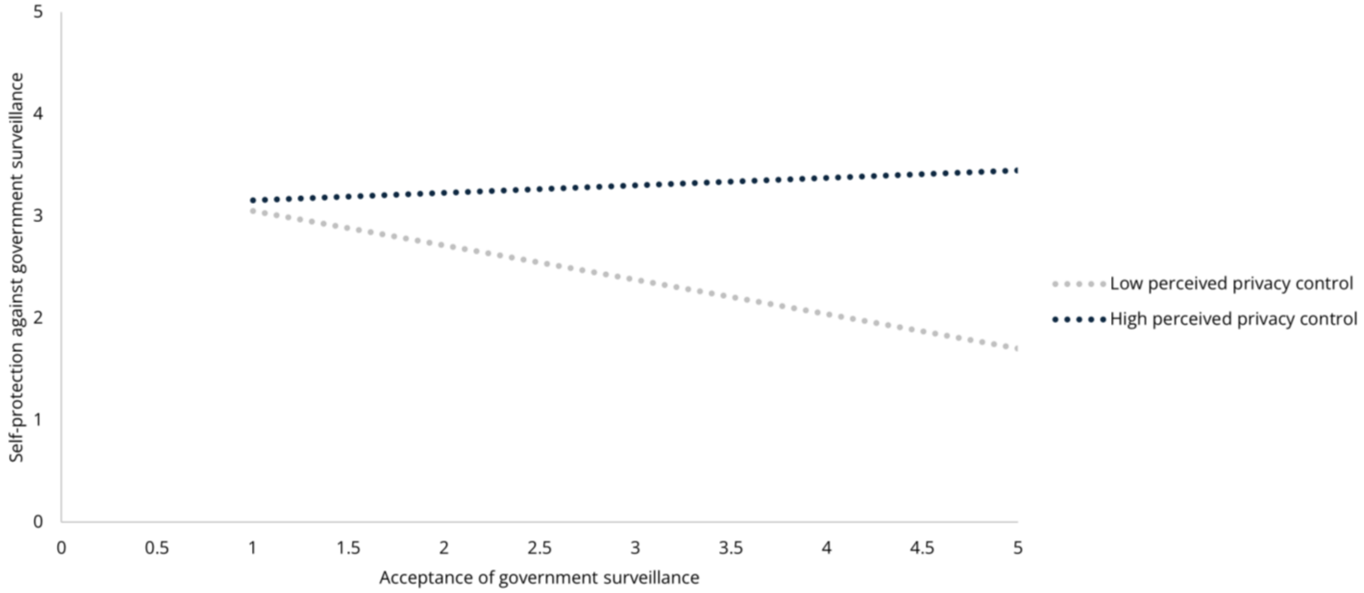


Figure 7. *The Moderating Effect of Perceived Privacy Control Between Surveillance Acceptance and Self-Protection in the Commercial Context.*

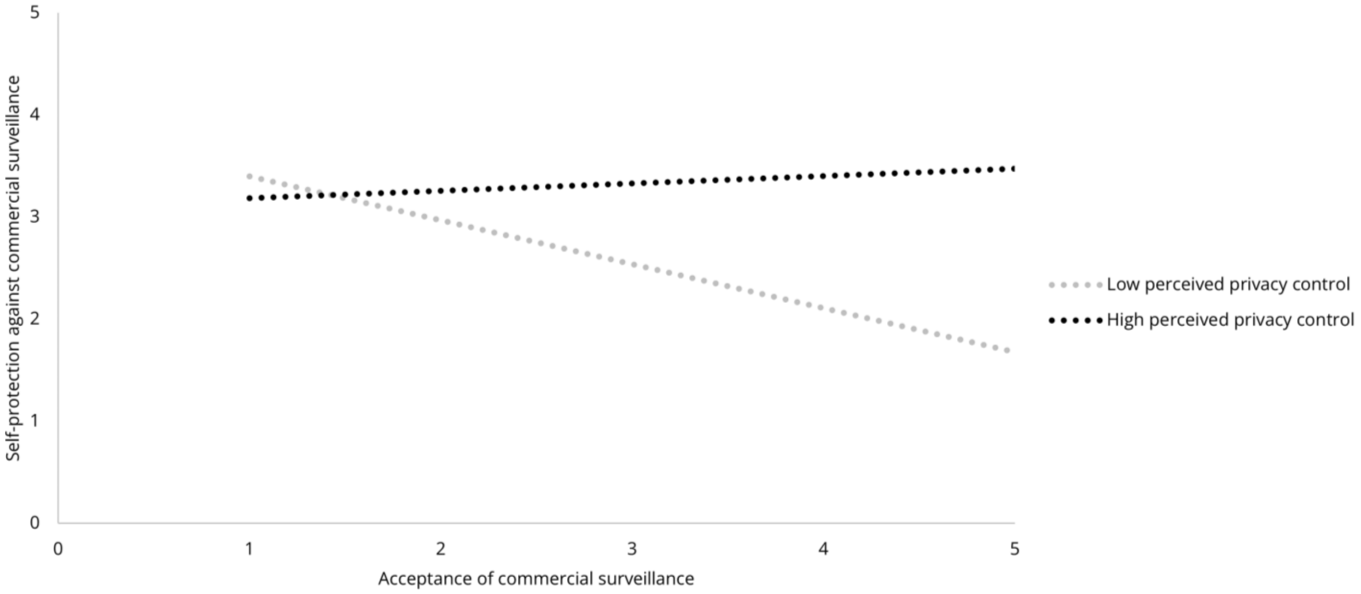
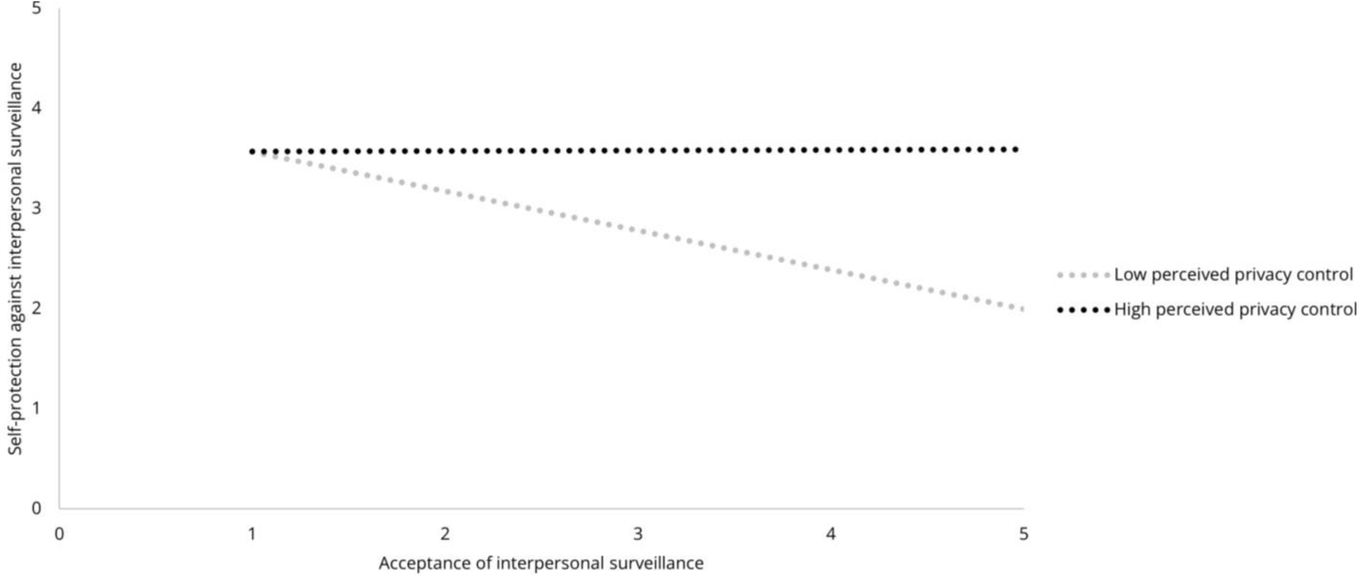


Figure 8. *The Moderating Effect of Perceived Privacy Control Between Surveillance Acceptance and Self-Protection in the Interpersonal Context.*



Discussion

In this study, we explored the contextual differences in US internet users' perceptions and behaviors relating to digital surveillance. Initially, we established a baseline model, using privacy concerns, algorithm awareness, and privacy control as antecedents to explain surveillance acceptance and self-protection. Subsequently, we a) compared surveillance acceptance and self-protection across government, commercial, and interpersonal contexts, b) assessed the influence of the antecedents within each context, c) probed the moderating role of political orientation, and d) evaluated the relationship between surveillance acceptance and self-protection in each context.

Our results led to three overarching conclusions, which will be elaborated in later sections:

Context is crucial: Prior research on internet privacy and digital surveillance has largely emphasized attitude, beliefs, knowledge, and risk-benefit calibration. Our findings underscore that these individual-level processes must be contextualized. Different variables influenced acceptance and self-protection across various surveillance contexts.

Nuances in political beliefs: Our investigation into the role of political beliefs unveiled nuanced but critical differences in users' interpretations of their rights and normative beliefs. While no significant disparities were observed in the acceptance of government vs. commercial surveillance, further segmentation by political leaning revealed subtle distinctions.

Absence of association between attitudes and behaviors: Our study reaffirms a disconnection between privacy-related attitudes and behaviors. However, our perspective is unique: a user's rejection of digital surveillance is not directly tied to their intent to self-protect. Our finding suggests that acceptance and protection can be distinct constructs while providing further explorations regarding different mindsets based on perceived privacy control.

Collectively, our findings enrich our understanding of user experiences under digital surveillance, advocating for a more holistic theoretical framework that encapsulates privacy and surveillance in context. Moreover, we emphasize the urgent need for transparency in surveillance practices to bolster public trust and protect individual rights.

Contextual Differences

Differences in surveillance acceptance reveal that users draw a clear line between interpersonal and institutional surveillance. Observing the patterns across contexts, people are unwilling to accept surveillance in general and are particularly more resistant in the interpersonal context. However, the line blurs when differentiating between government and commercial surveillance. One general reason could be that government and commercial surveillance are ubiquitous and unavoidable, indicating a passive and powerless position of individual users in face of the institutional power. Meanwhile, insights from the poll data presented us with an alternative explanation. According to the data, Americans generally exhibit greater trust in businesses over the government, a sentiment expected to translate into greater acceptance of commercial surveillance compared to government surveillance. However, social media companies are not perceived as trustworthy as other businesses (Tures, 2020). In the digital context of our study, questions about commercial surveillance might have prompted participants to make a direct association with major tech companies. As such, the anticipated higher acceptance of commercial over government surveillance could have been counterbalanced by the specific distrust in tech firms. Additionally, the moderating effects of political orientation also contributed to the non-significant difference between acceptance of government and commercial surveillance because the difference (if any) could be hard to detect when the liberals and the conservatives were analyzed altogether.

Users' self-protection in the three surveillance contexts was not significantly different from each other, which connects to one of the two contrasting perspectives from Dienlin and Breuer (2022), that people may think privacy is "dead" and there is nothing they can do. Another possibility is that although people may have different levels of acceptance of surveillance in different contexts, they would strive to protect their information regardless of contexts. Furthermore, in practical terms, it may be difficult for users to acquire enough information and training to effectively distinguish between different surveillance parties in real-world scenarios. This underscores the necessity for enhanced transparency in surveillance activities, empowering users to make more informed self-protection decisions. Specifically, when digital platforms engage in user data collection, it is imperative that their privacy policies meticulously detail what parties will have access to this data and how it will be utilized. Such precise contextual factors significantly influence users' privacy decisions, further emphasizing the need for careful policy articulation.

Along with increasing empirical research efforts on contextualizing privacy and surveillance (e.g., Martin & Shilton, 2016; Trepte et al., 2020), our findings further indicate the need to disentangle the common grounds as well as the uniqueness of different privacy/surveillance contexts in theory-building. We foresee the need for the existing research endeavors to be linked systematically, with both commonalities and disparities duly identified. Particularly when utilizing specific theories and models (e.g., communication privacy management, privacy calculus, etc.), researchers should continue to pinpoint factors with universal implications, as well as those that are more contingent upon contexts.

Political Beliefs as a Nuanced Factor

While the effects of general privacy concerns on surveillance acceptance were not pronounced, the interaction between political orientation and privacy concerns revealed the key role that political orientation plays: liberal-leaning participants did not differentiate acceptance of government and commercial surveillance while conservative-leaning participants demonstrated significantly lower acceptance of government surveillance (M = 2.08, SE = 0.1) than commercial surveillance (M = 2.25, SE = 0.09, p = .007). In general, conservative-leaning participants' acceptance of surveillance was sensitive to privacy concerns, leading to less acceptance and more self-protection with greater concerns. Liberal-leaning participants, on the other hand, maintained a stable stance toward surveillance, less impacted by privacy concerns. Possible reasons, such as that conservatives may resist surveillance under a democratic-led government, merit further investigation. More interestingly, future studies could explore how liberals react to surveillance when Republicans are leading the administration to help further comprehend such a phenomenon. The intersection of digital surveillance, privacy, and political ideologies sheds light on more nuanced aspects that demand further exploration.

Potential Underlying Processes

We found that acceptance of and protection against digital surveillance are not associated. Being two distinct constructs, users' dispositions may not transfer to their protection behavior due to perceived control. The post hoc analysis with perceived control as a moderator may hint at distinct user mindsets: users might feel personally responsible for their privacy in interpersonal contexts, which echoes a long-time argument that individuals are groomed to believe that privacy is their personal responsibility (e.g., Marwick et al., 2017). However, facing institutional surveillance, they might perceive an external locus of control, doubting their ability to effect change or feeling that protection is the institution's duty. The analysis highlights a potential divide in acceptance, with perceived privacy control as key: a) forced acceptance, marked by low expectations and helplessness, leading to passive self-protection; b) voluntary acceptance, characterized by approval and a belief in personal ability to protect, leading to active self-protection. However, we observed such patterns based on our conceptual framework for this particular study, which could not rule out other possible explanations and contributing factors for related concepts such as privacy paradox (Dienlin & Trepte, 2015), privacy cynicism (Hoffman et al., 2016), and privacy fatalism (Xie et al., 2019). Therefore, our interpretations should be further explored and corroborated by more studies.

Limitations and Future Research

Our sample is from MTurk, which has been a controversial platform regarding its data generalizability and data quality (e.g., Chmielewski et al., 2020). We are aware of the choice of this population may limit the interpretation of the findings. Future research can seek a more diverse sample and better data quality to replicate the results. We also advise future researchers to employ larger sample sizes to yield greater power and boost the robustness of the findings.

Furthermore, without a prior power analysis to decide the number of participants in the planning phase, there is some uncertainty about the true power of our results. Therefore, caution is needed when interpreting the observed effects in our study. For instance, some weak relationships, like privacy concerns and protection against individual surveillance (β = .12, p = .019), may have appeared significant due to Type I error. Conversely, the relationship between the interaction term of perceived privacy control and political orientation and protection against commercial surveillance (β = .10, p = .067) may have been insignificant due to Type II error. Moreover, we calculated the smallest acceptable correlation coefficient based on our power (.8), significance level (0.05), and sample size (356) and yielded a cutoff value of r = .15. There is a possibility that a true effect around r = .1 or r = .12 can be missed. We remind our readers to interpret our correlations that are smaller than .15 with caution[1].

We measured self-protection by asking "frequency of taking actions to self-protect," which could be opaque and unspecific to certain participants. Through this measure, we essentially obtained participants' subjective evaluations, which could have confounded various individual understandings of self-protective actions and thus made the self-report deviate from actual behavior. Besides the vague and general self-report questions, we may seek behavioral observations to reflect participants' protection more accurately in the future. Moreover, the statements in the algorithm awareness measure largely focused on media manipulation, which can be more typically linked with commercial contexts instead of the government and interpersonal contexts. Therefore, the results can be limited considering the applicability of the measures employed in this study. Future research should find more appropriate measures that match the contexts more universally. Last but not least, in a recent paper (Colnago et al., 2022), the authors investigated different privacy scales and discovered a significant misalignment between the intended constructs and participant understanding: many statements in a particular scale with the intention to assess constructs like privacy concern, were perceived by survey participants as characterizing different constructs (e.g., privacy preferences); no statement uniquely measured a single construct. Therefore, it is important to be aware that such epistemological and practical problems may exist in the scales that we employed, threatening the validity of our findings. In future investigations, we should seek replication of the findings in this study and be extra careful with the selected measures.

In empirical research regarding privacy and surveillance, our exploration of political beliefs remains preliminary as a starting point to integrate political and social factors. Besides self-identified political orientation included in this study, political beliefs, values, and ideologies are far more than the liberal-conservative dichotomy (e.g., Feldman, 1988; Treier & Hillygus, 2009). Future studies can test more dimensions of political beliefs with different spectrums and categorizations.

It is important to be mindful that surveillance is a global issue yet with many cultural variations (Lyon, 2007). The findings from this study may only apply to the context of the United States, a country that highly values individualism and personal freedom. We believe that culture plays an important role in how people understand privacy, surveillance, and power. We suppose there could be drastically different patterns in different cultural backgrounds than we found. Follow-up studies could focus on cross-cultural comparisons between countries like China, which has contrasting regimes, political ideologies, and social norms compared to the U.S.

Footnotes

[1] We did this additional analysis per our reviewer's request.

Conflict of Interest

This manuscript has not been published and is not under consideration for publication elsewhere. We have no conflicts of interest to disclose. All authors have approved the manuscript and agree with its submission to *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Authors' Contribution

Weizi Liu: conceptualization, methodology, investigation, validation, writing—original draft, writing—review & editing, project administration. **Seo Yoon Lee:** data analysis, data curation, software, validation, visualization, writing—original draft, writing—review & editing. **Mike Yao:** conceptualization, methodology, writing—review & editing.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy enhancing technologies* (pp. 36–58). Springer. https://doi.org/10.1007/11957454_3

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of Applied Social Psychology*, *32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In *2006 IEEE symposium on security and privacy* (pp. 183–198). IEEE. https://doi.org/10.1109/SP.2006.32

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118–123. https://doi.org/10.1016/j.copsyc.2020.05.004

Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends® in Marketing*, *11*(1), 1–71. https://doi.org/10.1561/1700000057

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419–426. https://doi.org/10.1016/j.chb.2015.07.025

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society, 9*(1), 1–14. https://doi.org/10.1177/20539517211065368

Camp, L. J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine*, *28*(3), 37–46. https://doi.org/10.1109/MTS.2009.934142

Chen, H.-G., Chen, C. C., Lo, L., & Yang, S. C. (2008). Online privacy control via anonymity and pseudonym: Cross-cultural implications. *Behaviour & Information Technology*, *27*(3), 229–242. https://doi.org/10.1080/01449290601156817

Chmielewski, M., & Kucker, S. C. (2020). An MTurk crisis? Shifts in data quality and the impact on study results. *Social Psychological and Personality Science*, *11*(4), 464–473. https://doi.org/10.1177/1948550619875149

Christl, W. (2017, June). Corporate surveillance in everyday life. How companies collect, combine, analyze, trade, and use personal data on billions. *Cracked Labs*. http://crackedlabs.org/en/corporate-surveillance

Colnago, J., Cranor, L. F., Acquisti, A., & Stanton, K. H. (2022). Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth symposium on usable privacy and security (SOUPS 2022)* (pp. 331–346). USENIX. https://www.usenix.org/conference/soups2022/presentation/colnago

Degli-Esposti, S. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society*, *12*(2), 209–225. https://doi.org/10.24908/ss.v12i2.5113

Dienlin, T., & Breuer, J. (2022). Privacy is dead, long live privacy! *Journal of Media Psychology, 35*(3), 159–168. https://doi.org/10.1027/1864-1105/a000357

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management, 14(*4), 57–93*.* https://doi.org/10.4018/jgim.2006100103

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

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

Distler, V., Lallemand, C., & Koenig, V. (2020). How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs. *Computers in Human Behavior*, *106*, Article 106227. https://doi.org/10.1016/j.chb.2019.106227

Feldman, S. (1988). Structure and consistency in public opinion: The role of core beliefs and values. *American Journal of Political Science*, *32*(2), 416–440. https://doi.org/10.2307/2111130

Fox, J., & Tokunaga, R. S. (2015). Romantic partner monitoring after breakups: Attachment, dependence, distress, and post-dissolution online surveillance via social networking sites. *Cyberpsychology, Behavior and Social Networking*, *18*(9), 491–498. https://doi.org/10.1089/cyber.2015.0123

Gangadharan, S. P. (2017). The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal internet users. *New Media & Society*, *19*(4), 597–615. https://doi.org/10.1177/1461444815614053

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security,* 77, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gran, A.-B., Booth, P., & Bucher, T. (2021). To be or not to be algorithm aware: A question of a new digital divide? *Information, Communication & Society*, *24*(12), 1779–1796. https://doi.org/10.1080/1369118X.2020.1736124

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), Article 7. https://doi.org/10.5817/CP2016-4-7

Ioannou, A., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society*, *67*, Article 101774. https://doi.org/10.1016/j.techsoc.2021.101774

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/07370020903586662

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My data just goes everywhere": User mental models of the internet and implications for privacy and security. In L. F. Cranor, R. Biddle & S. Consolvo (Eds.), *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 39–52). USENIX. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. *Journal of Current Issues & Research in Advertising*, *38*(1), 92–105. https://doi.org/10.1080/10641734.2016.1233157

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

LaRose, R., & Rifon, N. (2006). Your privacy is assured - of being disturbed: Websites with and without privacy seals. *New Media & Society*, *8*(6), 1009–1029. https://doi.org/10.1177/1461444806069652

Levy, K. E. C. (2014). Intimate surveillance. *Idaho Law Review*, *51*(3), 679–694. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834354

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing* (pp. 501–510). https://doi.org/10.1145/2370216.2370290

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22(7),* 1168–1187. https://doi.org/10.1177/1461444820912544

Lyon, D. (2007). *Surveillance studies: An overview*. Polity.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, *59*(2), 243–261. https://doi.org/10.1111/1540-4560.00063

Martin, A. K., Brakel, R. E. van, & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*, *6*(3), 213–232. https://doi.org/10.24908/ss.v6i3.3282

Martin, K., & Nissenbaum, H. (2017). Measuring privacy: An empirical test using context to expose confounding variables. *Science and Technology Law Review*, *18*(1), 176–218. https://doi.org/10.7916/stlr.v18i1.4015

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*, *32*(3), 200–216. https://doi.org/10.1080/01972243.2016.1153012

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Marwick, A. E., Fontaine, C., & boyd, d. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media + Society*, *3*(2), 1–14. https://doi.org/10.1177/2056305117710455

Marx, G. T. (2015). Surveillance studies. In J. D. Wright (Ed.), *International encyclopedia of the social & behavioral sciences* (2nd ed., pp. 733–741). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy expectations and preferences in an IoT world. In *Thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 399–412). USENIX. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

Nissenbaum, H. (2004). Privacy as contextual integrity symposium—Technology, values, and the justice system. *Washington Law Review*, *79*(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Balebako, R., & Cranor, L. F. (2018). Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies*, *2018*(4), 5–32. https://doi.org/10.1515/popets-2018-0029

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. J. (2021). *The future of digital surveillance: Why digital monitoring will never lose its appeal in a world of algorithm-driven AI*. University of Michigan Press. https://doi.org/10.3998/mpub.10211441

Pavlou, P. A. (2002). What drives electronic commerce? A theory of planned behavior perspective. *Academy of Management Proceedings*, *2002*(1), A1–A6. https://doi.org/10.5465/apbpp.2002.7517579

Rosenberg, S. (2005, May 10). Profiles of the typology groups. *Pew Research Center - U.S. Politics & Policy*. https://www.pewresearch.org/politics/2005/05/10/profiles-of-the-typology-groups/

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, *154*(4), 352–369. https://doi.org/10.1080/00224545.2014.914881

Segijn, C. M., Opree, S. J., & van Ooijen, I. (2022). The validation of the Perceived Surveillance Scale. *Cyberpsychology*: *Journal of Psychosocial Research on Cyberspace, 16(3)*, Article 9. https://doi.org/10.5817/CP2022-3-9

Shin, D. (2020). User perceptions of algorithmic decisions in the personalized AI system: Perceptual evaluation of fairness, accountability, transparency, and explainability. *Journal of Broadcasting & Electronic Media, 64*(4), 541–565. https://doi.org/10.1080/08838151.2020.1843357

Shin, D. (2021a). A cross-national study on the perception of algorithm news in the East and the West. *Journal of Global Information Management*, *29*(2), 77–101. http://doi.org/10.4018/JGIM.2021030105

Shin, D. (2021b). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies*, *146*, Article 102551. https://doi.org/10.1016/j.ijhcs.2020.102551

Shin, D., Chotiyaputta, V., & Zaid, B. (2022a). The effects of cultural dimensions on algorithmic news: How do cultural value orientations affect how people perceive algorithms? *Computers in Human Behavior*, *126*, Article 107007. https://doi.org/10.1016/j.chb.2021.107007

Shin, D., Rasul, A., & Fotiadis, A. (2022b). Why am I seeing this? Deconstructing algorithm literacy through the lens of users. *Internet Research, 32*(4), 1214–1234. https://doi.org/10.1108/INTR-02-2021-0087

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

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

Thomson, R., Yuki, M., & Ito, N. (2015). A socio-ecological approach to national differences in online privacy concern: The role of relational mobility and trust. *Computers in Human Behavior*, *51*(Part A), 285–292. https://doi.org/10.1016/j.chb.2015.04.068

Treier, S., & Hillygus, D. S. (2009). The nature of political ideology in the contemporary electorate. *Public Opinion Quarterly*, *73*(4), 679–703. https://doi.org/10.1093/poq/nfp067

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, Article 106115. https://doi.org/10.1016/j.chb.2019.08.022

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14

Trottier, D. (2012). Interpersonal surveillance on social media. *Canadian Journal of Communication*, *37*(2), 319–332. https://doi.org/10.22230/cjc.2012v37n2a2536

Trottier, D. (2016). *Social media as surveillance: Rethinking visibility in a converging world*. Routledge. https://doi.org/10.4324/9781315609508

Tures, J. (2020, August 12). *Americans trust businesses more than government—except social media, which they hate*. https://observer.com/2020/08/polls-americans-trust-businesses-more-than-government-except-social-media/

Turow, J., Hennessy, M., Akanbi, O., Virgilio, D., & Draper, N. (2018). *Divided we feel: Partisan politics American’s emotions regarding surveillance of low-income populations*. Annenberg School for Communication University of Pennsylvania. https://repository.upenn.edu/handle/20.500.14332/2209

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society*. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

Xie, W., Fowler-Dawson, A., & Tvauri, A. (2019). Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*, *38*(7), 742–759. https://doi.org/10.1080/0144929X.2018.1552717

Xu, H., Dinev, T., Smith, H., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings,* Article 6. https://aisel.aisnet.org/icis2008/6

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association of Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior*, *11*(5), 615–617. https://doi.org/10.1089/cpb.2007.0208

Zarouali, B., Boerman, S. C., & de Vreese, C. H. (2021). Is this recommended by an algorithm? The development and validation of the Algorithmic Media Content Awareness Scale (AMCA-scale). *Telematics and Informatics*, *62*, Article 101607. https://doi.org/10.1016/j.tele.2021.101607

Zhang, Z., Liu, J., Wei, Z., Tao, Y., & Bai, Q. (2017). From secrete admirer to cyberstalker: A measure of online interpersonal surveillance. In J. Diesner, E. Ferrari, & G. Xu (Eds.), *Proceedings of the 2017 IEEE/ACM international conference on advances in social networks analysis and mining 2017* (pp. 613–614). https://doi.org/10.1145/3110025.3110065

Appendix

Table A1. *Bivariate Correlations Among Key Variables*.

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
1. Acceptance of government surveillance	1									
2. Acceptance of commercial surveillance	.76**	1								
3. Acceptance from interpersonal surveillance	.67**	.71**	1							
4. Protection against government surveillance	.00	.02	.22**	1						
5. Protection against commercial surveillance	−.04	−.05	.11*	.72**	1					
6. Protection against interpersonal surveillance	.03	.04	−.04	.61**	.67**	1				
7. Privacy concerns	−.15**	−.15**	−.13*	.10	.20**	.11*	1			
8. Perceived privacy control	.43**	.39**	.49**	.28**	.26**	.15**	−.21**	1		
9. Algorithm awareness	−.16**	−.14**	−.27**	−.03	.08	.16**	.16**	−.26**	1	
10. political orientation	.15**	.07	.06	−.08	−.07	−.04	−.09	−.02	.00	1

Note. *N* = 356, $^{**}p$ < .01.

Measures

Privacy concerns (1 = *strongly disagree*, 5 = *strongly agree*)

- I'm concerned that the information about myself will be used in a way I did not foresee.
- I'm concerned that the information about myself will become available to someone without my knowledge.
- I'm concerned that the information about myself will be continuously spied on.
- I'm concerned that the information about myself will be misinterpreted.

Perceived privacy control (1 = *strongly disagree*, 5 = *strongly agree*)

- I believe I can control my personal information provided online.
- I believe I have control over who can get access to my personal information collected online.
- I think I have control over what personal information is released online.
- I believe I have control over how personal information is used online.

Algorithm awareness (1 = *not at all aware*, 5 = *completely aware*)

- Algorithms are used to show someone else different media content from what I get to see on online platforms.
- Algorithms are used to recommend media content to me on online platforms.
- Algorithms are used to show me media content on online platforms based on automated decisions.
- Algorithms make automated decision on what I get to see online.
- Algorithms are used to tailor certain media content to me on online platforms.
- Algorithms do not require direct human judgments in deciding which media content to show me on online platforms.
- Algorithms are used to prioritize certain media content above others.
- The media content that algorithms recommend to me on online platforms can be subjected to human biases such as prejudices and stereotypes.

- It is not always transparent why algorithms decide to show me certain media content on online platforms.
- The media content that algorithms recommend to me on online platforms depend on my online behavior on those platforms.
- The media content that algorithms recommend to me on online platforms depend on my online behavioral data.
- Algorithms use my personal data to recommend certain media content on online platforms.
- The fact that algorithms use my personal data to recommend certain media content has consequences for my online privacy.
- The media content that algorithms recommend to me on online platform depends on the data that I make available online.

Surveillance acceptance (1 = *completely not accept*, 5 = *completely accept*)/protection (1 = *never*, 5 = *always*)

- Accessing my phone number
- Accessing my physical location
- Recording my IP addresses
- Accessing my social contacts (family, friends, colleagues, etc.)
- Tracking my online purchases
- Keeping my name in a database
- Tracking my browsing history

About Authors

Weizi Liu is an Assistant Professor at the Bob Schieffer College of Communication at Texas Christian University. Her research lies at the intersection of communication, human-computer interaction, and social psychology. She studies how users communicate with emerging media tools and platforms (e.g., smart speakers, chatbots, and recommendation systems), focusing on social dynamics, user trust and acceptance, as well as privacy and data security.

https://orcid.org/0000-0003-2071-1603

Seo Yoon Lee is an Assistant Professor in the Digital Media Program, Department of Information Science Technology, Technology Division at the Cullen College of Engineering at the University of Houston. Her research focuses on revealing the factors that motivate individuals to engage in toxic online communication and the nuanced impacts of emerging media technologies on strategic communication, particularly in addressing health and environmental concerns.

https://orcid.org/0000-0002-3302-3220

Mike Yao is a Professor of Digital Media and Director of the Institute of Communications Research (ICR) at the University of Illinois Urbana-Champaign. His research delves into the interplay between media, technology, society, and human communication. He examines how people engage with emerging technologies like AI and immersive multimedia across diverse social settings and how these interactions influence social behavior and human communication in digitally mediated spaces.

✉ **Correspondence to**
Weizi Liu, Bob Schieffer College of Communication, Texas Christian University, 2800 South University Drive
Fort Worth, Texas, 76109, weizi.liu@tcu.edu