Gagrčin, Emilija; Toth, Roland; Schaetz, Nadja; Naab, Teresa; Emmer, Martin

Article

Perceived personal and societal data harms shape users' data control preferences

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Gagrčin, Emilija; Toth, Roland; Schaetz, Nadja; Naab, Teresa; Emmer, Martin (2026) : Perceived personal and societal data harms shape users' data control preferences, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 15, Iss. 1, pp. 1-26, https://doi.org/10.14763/2026.1.2060

This Version is available at:
https://hdl.handle.net/10419/336200

INTERNET POLICY REVIEW

Volume 15 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Perceived personal and societal data harms shape users' data control preferences

Emilija Gagrčin *University of Bergen*
Roland Toth *Weizenbaum Institute for the Networked Society*
Nadja Schaetz *University of Hamburg*
Teresa Naab *University of Mannheim*
Martin Emmer *Freie Universität Berlin*

DOI: https://doi.org/10.14763/2026.1.2060

Published: 9 January 2026
Received: 15 April 2025 **Accepted:** 21 July 2025

Funding: This work was funded by the Federal Ministry of Education and Research of Germany (BMBF), grant number 16DII131 and 16DII135. Data collection was supported with special funds from the Federal Foreign Office for the German EU Council Presidency 2020 granted to the Goethe Institut.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Gagrčin, E., Toth, R., Schaetz, N., Naab, T., & Emmer, M. (2026). Perceived personal and societal data harms shape users' data control preferences . *Internet Policy Review*, *15*(1). https://doi.org/10.14763/2026.1.2060

Keywords: Datafication, Societal harms, Young people, Privacy resignation

Abstract: Platformisation and the growing adoption of AI-driven systems have intensified pervasive data extraction and appropriation that bring distinct harms for both individuals and societies at large. Yet, little is known about how distinct harm perceptions shape citizens' preferences for different control mechanisms. Based on survey data from six EU countries (N=2,889), we examine differences in perceptions of personal vs. societal harm and their implications for individual control preferences and support for regulation. We find a surprising inverse relationship between perceived personal harm and desire for individual control: when citizens' perceive greater personal harm, they become less inclined to seek individual data control, suggesting privacy resignation. Conversely, perceived societal harm positively relates to both individual and regulatory control preferences, underscoring citizens' view of these mechanisms as complementary, particularly when they perceive harms to democracy. For policymakers, the findings suggest that regulators should treat both dimensions as related but distinct inputs when designing interventions and address the conditions that generate both individual and collective harms. Specifically, regulatory frameworks with an overreliance on individual control mechanisms (like consent requirements) may be insufficient or even counterproductive when citizens already perceive data harms.

Introduction

Social media platforms have fundamentally transformed our understanding of privacy through pervasive behavioural data harvesting and commodification that systematically transcends user visibility and identifiability (Matzner, 2014; Zuboff, 2019). Despite growing user awareness, proactive individual measures cannot effectively counter ubiquitous data collection (Dencik & Cable, 2017; Draper & Turow, 2019), creating broader societal challenges that demand regulatory attention (Couldry & Meijas, 2019; Smuha, 2021). When aggregate data enables citizen profiling and manipulation during electoral processes, the potential harm threatens democratic legitimacy itself (Smuha, 2021; Zuiderveen Borgesius et al., 2018). This shift from personal privacy concerns to wider societal harms has sparked calls for comprehensive regulation, particularly within the European Union's developing AI regulation framework.

Although both personal and societal harms from data practices are widely recognised (Muller, 2020; Shelby et al., 2023; Smuha, 2021), we do not know how citizens' perceptions of these harms might shape their regulatory preferences. When perceiving harm to oneself, do citizens primarily seek individual control? When concerned about societal damage, do they turn to government intervention? Or do they want both approaches working together? Our study addresses these questions by examining the relationship between citizens' perceptions of data harms and their preferences for different control mechanisms.

Addressing the relationship between harm perceptions and control preferences matters for several reasons: First, regulations focusing solely on personal harm have created an illusion of control rather than actual protection (e.g., Brandimarte et al., 2013; Bendix & MacKay, 2022). Second, public support for regulatory efforts largely depends on how severe people perceive the harms to be (Slovic, 1987). Third, democratic institutions risk losing trust if citizens feel that powerful entities ignore or fail to address major societal problems.

Drawing on control theory and compensatory control theory, we analyse survey data from six EU countries collected in early 2021. This period constitutes a uniquely informative window, because it captures perceptions roughly one year into the COVID-19 pandemic and the wide deployment of digital methods for the management of the health crisis, that triggered concerns about privacy and intrusion from government (Ioannou & Tussyadiah, 2021) and corporate surveillance (Vitak & Zimmer, 2023). It also is a time in which distinctions and tensions between individual and societal harms have come into sharp relief, as governments have

weighed the protection of public health against the importance of individuals' right to privacy (van Kolfschooten & de Ruitjer, 2020). By examining how citizens perceive data harms, we offer a baseline for understanding the evolving relationship between perceived risks and governance preferences in an era of ubiquitous platformisation and data harvesting (Couldry & Meijas, 2019).

Theoretical background

Privacy concerns have traditionally centered on user disclosure and horizontal privacy risks (Hargittai & Marwick, 2016; Masur, 2020), with focus on individual control over information about oneself and the degree of access others have to this information (Nissenbaum, 2010; Xu et al., 2012). It was generally possible for users to know what they disclosed and to whom, they could reasonably anticipate specific adverse outcomes (i.e. harms) such as reputational damage, discrimination, or harassment, thus fitting the traditional risk frameworks that presume that actors can predict outcomes and assign (at least roughly) probabilities to them (Scoones, 2019). However, the contemporary communication environments of social media platforms have fundamentally transformed the conditions under which people can meaningfully anticipate outcomes of their actions.

Through pervasive backend data collection and commodification (Couldry & Meijas, 2019; Zuboff, 2019), behaviour is reduced to predictive features and cross-contextual inferences (Birch et al., 2021; Matzner, 2014), meaning that relevant "information" does not necessarily stem from deliberate disclosure but from opaque aggregation and inference processes. AI-based predictive analytics amplify this shift by generating new informational categories from data that users neither see nor meaningfully control (Mühlhoff, 2023). Platforms' backend operations make it difficult for users to know how their data are combined, inferred from, or repurposed across contexts, thus creating uncertainty through complexity and opacity (Mackenzie, 2019). As a result, individuals cannot reliably assess what harms might arise, how severe they may be, or whether their own behaviour can meaningfully mitigate them. Thus, since outcomes and their likelihoods cannot be meaningfully anticipated (Knight, 1964), we can say that contemporary platform infrastructures operate under *uncertainty* rather than risk.

In the following, we draw on the ideas of complexity and uncertainty as *background* context for understanding how diffuse, hard-to-attribute harms affect people's perceptions of control. This makes the nature of the harm itself a critical point of differentiation, since some harms are more-or-less perceptible and self-referent while others are rather diffuse, cumulative and collective (e.g., Shelby et

al., 2023). Our study focuses specifically on two key dimensions of possible harm that we review next.

Personal harms

Drawing on Solove's (2006) taxonomy of privacy harms, four practices are critical in potentially inducing harms to individuals: 1) surveillance, in which routine collection of behavioural data erodes the boundary around private life; 2) aggregation and secondary use, where data are repurposed for aims such as political advertising; 3) disclosure, which exposes individuals to unforeseen uses and judgments through third-party sharing; and 4) invasion, as when governmental access to platform data encroaches on informational self-determination. Under Nissenbaum's (2010) theory of contextual integrity, each of these practices constitutes a breach of the norms governing information flows, potentially undermining autonomy, creating reputational risks, and triggering concerns about future misuse.

Empirical work on platform-related harms reinforces this theoretical framing. Boerman et al. (2021) show that users often experience such practices as a threat to their personal interests, prompting protective or compensatory responses. Shelby et al. (2023) extend this view by situating privacy violations within a broader set of sociotechnical harms. In their account, privacy violations extend beyond disclosure to include predictive inference from seemingly innocuous data, cross-context repurposing without consent, and affect-based or ubiquitous surveillance – all of which can heighten feelings of exposure and loss of control even without formal rule-breaking. Specifically related to micro-level harms, Shelby et al. (2023) identify interpersonal harms such as loss of agency, diminished well-being, and technology-facilitated abuse; and quality-of-service harms including alienation, additional user labour, and performance disparities. As they note, harms may be directly or indirectly felt, can accumulate over time, and often overlap with other harm types, meaning individual experiences are better understood as part of a wider harm ecology.

In response, users often experience privacy resignation, defined as a psychological state where individuals believe they cannot meaningfully protect their privacy despite desiring to do so (Draper & Turow, 2019). This resignation stems not from apathy but from recognition that meaningful control is practically impossible under current conditions (Dencik & Cable, 2017; Hargittai & Marwick, 2016). Dencik and Cable (2017) call this state "surveillance realism." Conceptually, the regime of data uncertainty has also given rise to critical theoretical perspectives like "algorithmic alienation," which describes the growing separation between individuals and their

data as it is processed through opaque computational systems (Andrejevic, 2013). Both privacy resignation and algorithmic alienation reflect responses to uncertainty rather than risk, where meaningful prediction of data trajectories becomes impossible (Scoones, 2019). Building on this, we focus on perceived personal harms to denote a self-referent risk appraisal: respondents' judgement of how much platform data practices could negatively affect them personally. Although many data harms are diffuse and hard to pinpoint, people still form self-focused appraisals of that diffuse exposure.

Societal harms

Beyond individual stakes, platforms can imperil collective democratic processes and institutional integrity. Regan (1995) argued early on that a privacy frame limited to individual interests cannot capture the wider risks to social order when information flows escape normative bounds. More recently, Renieris (2023) called to reinterpret the right to privacy, that underpins data protection and security efforts, through a more collective lens. Relatedly, Smuha (2021) defines societal harm as the thwarting of one or more interests of society, including democracy, human rights, and the rule of law (also Muller, 2020). Habermas (2023) underscores that transparent, inclusive discourse is a precondition for legitimate governance, yet opaque platform algorithms and undisclosed data sharing compromise these conditions (Couldry & Mejias, 2019). Empirically, Zuiderveen Borgesius et al. (2018) show how algorithmic micro-targeting and profiling can distort political deliberation through filter bubbles and subliminal persuasion, undermining democratic legitimacy. Finally, high-level incidents, such as the Facebook/Cambridge Analytica scandal (e.g., Nyabola, 2020) and instances of algorithmic censorship in both democratic and authoritarian contexts (Cevallos, 2025), illustrate how aggregated personal data can be weaponised to manipulate electoral outcomes or stifle dissent.

Societal harms differ from personal harms not only in scale but in their often indirect, diffuse, and accumulative character. Shelby et al. (2023) emphasise that such harms may occur downstream from the originating practices, are frequently experienced collectively, and may not be immediately recognized by those affected. Together, this literature positions societal-level platform harms as qualitatively distinct from individual privacy threats, demanding collective – and often regulatory – responses to safeguard democratic processes (Smuha, 2021; Shelby et al., 2023). Against this background, in this study, we define perceived societal harms as users' beliefs – again, potentially diffuse – about the extent to which platform data practices threaten democracy in a broad sense. In doing so, we are interested in distin-

guishing between people's recognition of collective-level risks and the more immediate individual-level harms addressed above.

Compensatory control theory and control preferences

Perceptions of personal and societal harm from datafication can unsettle a sense of order at both the individual and collective level (e.g., Dencik & Cable, 2017; Andrejevic, 2013; Smuha, 2021). Compensatory Control Theory (CCT) explains how people respond to such perceived threats: when primary sources of control appear compromised, individuals seek to restore order either through their own actions or by relying on external systems such as institutions (Kay et al., 2009; Landau et al., 2015). Thus, a key proposition of CCT is the substitution logic: when one source of control falters, people may shift toward another. The substitution mechanism provides the conceptual bridge to two preferred control outcomes: individual control, where the self is the control agent, and proxy control, where powerful others such as regulators act as the agent (Bandura, 2001; Xu et al., 2012). The preferred locus of control expresses normative orientations (i.e., where control should be located) rather than on respondents' beliefs about the current distribution of control.

Individual control in platform environments can be approached from (at least) two perspectives. In the psychological tradition, it refers to an individual's belief in their ability to take meaningful action to manage their digital footprint, in turn producing desired outcomes and preventing undesired ones through available tools (Skinner, 1996; Baruh et al., 2017). In the sociological tradition, such beliefs are understood as socially and structurally situated, reflecting the interplay between user agency and the structural constraints of platform environments (Giddens, 1984; Orlikowski, 2007). Our approach aligns with this latter view: we treat perceived individual control as the belief that ordinary users possess or lack meaningful power over the governance of digital data, recognising that these beliefs are shaped by the broader platform ecosystem in which they are formed (similarly, Pauer et al., 2024). Accordingly, we conceptualise preferred individual control as a belief that ordinary users ought to have greater capacity to govern their own digital data.

When individuals perceive harm but doubt the effectiveness of user control, they may prefer to outsource control to more capable entities (Bandura, 2001). Xu et al. (2012) characterise government legislation as "the most powerful approach for the execution of proxy control" (p. 1350). On a regulatory continuum, this ranges from "hands-off" self-regulation by corporations to full governmental authority over corporate data use (Bendix & MacKay, 2022; Milberg et al., 2000). By extension, we

conceptualise preferred regulatory control as the belief that institutions should have greater authority over platform data practices (Miltgen & Smith, 2015; Okazaki et al., 2009).

From a CCT perspective, harm perceptions can increase support for either or both preferred control outcomes (H1–H4, see below), but the balance between them depends on which control agents are seen as currently effective or trustworthy. We address this in the next section as potential moderators of the harm – control preference relationship.

Key moderators

Perceived individual control

In contrast to preferred individual control as a normative expectation, perceived individual control (PIC) reflects beliefs about the current distribution of control, i.e. the extent to which ordinary users believe to possess or lack meaningful power over the governance of digital data. Meta-analytic evidence indicates that capability proxies such as privacy literacy are positively associated with protective behaviour, and that privacy concerns generally motivate self-protection (Baruh et al., 2017), suggesting that PIC enables harm to translate into self-directed responses. Xu et al. (2012) show that personal control can substitute for proxy control provided by legislation. Cross-domain evidence reinforces this: Pauer et al. (2024) demonstrate that when personal control is low, trust in authorities plays a stronger role in shaping threat evaluation and responses; Fritsche et al. (2022) review multiple studies in which low personal control fosters a turn toward collective or proxy control solutions.

Under CCT, when people feel personally in control of managing a threat, additional triggers have less impact on their desire for further self-directed control. High PIC therefore dampens harm-driven increases in preferred individual control. When PIC is low, harms are more likely to prompt a shift toward external solutions, strengthening harm–regulatory control links (Xu et al., 2012; Fritsche et al., 2022). When PIC is high, perceived harms should have a weaker effect on preferred individual control, as individuals already feel empowered to act. When PIC is low, harms should more strongly increase preference for regulatory control, as individuals turn outward for solutions. This logic underlies H1a–H4a (see Hypotheses).

Perceived regulatory control

Perceived regulatory control (PRC) refers to an individual's belief that external authorities, and most notably governments, already have enough power to oversee

platform data practices effectively. Xu et al. (2012) find that institutional assurances can increase perceived control and reduce privacy concerns, implying that high PRC dampens the perceived need for self-help. Milberg et al. (2000) show that low perceived adequacy of governmental involvement strengthens calls for stronger privacy laws. Jiang and Yang's (2023) study of ride-hailing drivers in China found that perceived government regulation positively influenced drivers' intention to participate in platform governance. Here, the perceived regulatory agency served as a safety signal that negative platform issues are being addressed (Jiang & Yang, 2023; Xu et al., 2012). In contrast, when regulatory bodies are perceived as lacking expertise or enforcement power relative to platforms (Neudert, 2023), their effectiveness as proxy control agents likely diminishes. Evidence from other domains supports the same substitution mechanism: Kay et al. (2010) demonstrate a substitution mechanism between external control systems, with threats to government stability prompting shifts to other external systems (belief in God/divine control), and Pinto et al. (2024) show that low perceived formal control efficacy amplifies support for alternative proxy control forms such as vigilantism (akin to individuals taking back control). Shockley and Fairdosi (2015) report that perceived proxy competence can buffer threat responses in participants with high PRC. Accordingly, we expect PRC to moderate harm–control preference relationships in two main ways. First, high PRC should weaken the association between perceived harm and preferred individual control, as effective oversight reduces the need for personal action. Second, low PRC should strengthen the association between perceived harm and preferred regulatory control, as weak oversight increases pressure for expanded intervention. This logic underlies H1b–H4b (see Hypotheses).

Institutional trust

Institutional trust refers to confidence that public authorities act in the public interest, are competent, and operate with integrity (Adams & Osman, 2023). Classic definitions treat trust as a willingness "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al., 1998, p. 395), and so do "irrespective of the ability to monitor or control that other part" (Mayer et al., 1995, p. 712). According to Mayer, Davis and Schoorman's (1995) seminal model, trust is formed when an entity is perceived as able (i.e., having expertise in a relevant domain), benevolent (i.e., having good intentions) and displays integrity (e.g., by adhering to a set of principles). For the purposes of this paper, we treat institutional trust as a general orientation toward government as a credible and legitimate actor in managing data-related risks. We distinguish it from perceived regulatory control: trust concerns motives and aligns with the public interest, whereas PRC concerns capacity and ef-

fectiveness.

In risk management contexts, institutional trust has been shown to guide whether publics rely on institutional versus individual channels for addressing threats (Ahn & Noh, 2020). Shepherd and Kay (2012) find that high institutional trust attenuates the effect of perceived threat on personal control preferences while amplifying preference for institutional solutions. Pauer et al. (2024) show that when personal control is low, benevolence-based trust in authorities can reduce perceived threat and thereby weaken individual engagement with policy matters, consistent with trust functioning as a delegating heuristic. Lou et al. (2025) and Ahn and Noh (2020) also report that trust in managing authorities can directly promote engagement with institutional channels. Thus, under CCT, high trust in an external system can make it a more attractive target for compensatory control delegation following a threat. Conversely, high trust can also reduce the harm–individual control association, as individuals rely more on trusted institutions and feel less need to act themselves. Specifically, we expect high institutional trust to weaken harm–individual control and strengthen harm–regulatory control relationships. This logic underlies H1c–H4c (see Hypotheses).

Conceptual model and hypotheses

In sum, our hypotheses posit that both personal- and societal-level harm perceptions drive support for greater individual and regulatory control, but that these relationships are contingent on perceptions of control and trust in institutions.

Perceived personal harm will positively predict preferred individual control (**H1**). This effect will be weaker among individuals with (a) high perceived individual control (**H1a**), (b) high perceived regulatory control (**H1b**), and (c) high institutional trust (**H1c**).

Perceived personal harm will positively predict preferred regulatory control (**H2**). This effect will be stronger when perceived individual control is low (**H2a**), but weaker at high perceived regulatory control (**H2b**) and stronger at high institutional trust (**H2c**).

Perceived societal harm will positively predict preferred individual control (**H3**). This effect will be stronger among individuals with (a) high perceived individual control (**H3a**), but weaker at (b) high perceived regulatory control (**H3b**) and (c) high institutional trust (**H3c**).

Perceived societal harm will positively predict preferred regulatory control (**H4**). This effect will be stronger when perceived individual control is low (**H4a**), but weaker at high perceived regulatory control (**H4b**) and stronger at high institutional trust (**H4c**).

TABLE 1: Hypotheses overview

H1	PERCEIVED PERSONAL HARM ++ PREFERRED INDIVIDUAL CONTROL
H1A	WEAKER WHEN PERCEIVED INDIVIDUAL CONTROL IS HIGH
H1B	WEAKER WHEN PERCEIVED REGULATORY CONTROL IS HIGH
H1C	WEAKER WHEN INSTITUTIONAL TRUST IS HIGH
H2	PERCEIVED PERSONAL HARM ++ PREFERRED REGULATORY CONTROL
H2A	STRONGER WHEN PERCEIVED INDIVIDUAL CONTROL IS LOW
H2B	WEAKER WHEN PERCEIVED REGULATORY CONTROL IS HIGH
H2C	STRONGER WHEN INSTITUTIONAL TRUST IS HIGH
H3	PERCEIVED SOCIETAL HARM ++ PREFERRED INDIVIDUAL CONTROL
H3A	STRONGER WHEN PERCEIVED INDIVIDUAL CONTROL IS HIGH
H3B	WEAKER WHEN PERCEIVED REGULATORY CONTROL IS HIGH
H3C	WEAKER WHEN INSTITUTIONAL TRUST IS HIGH
H4	PERCEIVED SOCIETAL HARM ++ PREFERRED REGULATORY CONTROL

H4A	STRONGER WHEN PERCEIVED INDIVIDUAL CONTROL IS LOW
H4B	WEAKER WHEN PERCEIVED REGULATORY CONTROL IS HIGH
H4C	STRONGER WHEN INSTITUTIONAL TRUST IS HIGH

Method

Study context: Young people in the European Union

The data were collected in February and March 2021 via the online panel provider Respondi (N = 2,889) in six European countries: Germany, France, Greece, Italy, Poland, and Sweden. The countries included in the study were chosen following the logic of regional diversity of European Union (EU) countries in terms of geography (North/South/East/West) and size, bearing in mind similarities and differences in education systems and economic standards. We also strived to exemplify diverse media and communication regulations, following the categorization proposed by Humprecht et al. (2022) based on political, economic, media system, and regulatory dimensions. In our study, Germany and Sweden typify the "democratic-corporatist" country type, France and Italy the "hybrid" type, and Poland and Greece the "polarized pluralist" type. As such, our sample provides an opportunity to study a geographically and politically unified entity governed by the General Data Protection Regulation (GDPR). While we sampled these different countries to increase variance and improve the general EU-level estimation of associations, the goal was to test relationships that travel across contexts rather than to explain cross-national differences. Specifically, we were interested in how young Europeans, subjected to the EU's standardised data protection framework, perceive individual and collective privacy threats. Although the EU strives for regulatory harmonisation and economic-social development convergence, variations among European countries persist, as evident in periodic Eurobarometer surveys (EU-wide population surveys on a variety of policy issues).

Young adults are a suitable population to study for several reasons. Firstly, they heavily engage with social media platforms for various purposes, including entertainment, sociability, lifestyle, and politics (Bolin, 2017; Hargittai & Marwick, 2016), thereby continuously generating abundant behavioural data that can be

commodified. As such, the current youth generation constitutes a cohort socialised into wide commodification of user data (Bolin, 2017), often willingly sharing information to optimize services like public transport and healthcare (European Commission, 2020) or news exposure (Schaetz et al., 2023). However, this generation has also grown up in a time of increased public attention towards the risks of data collection and regulations regarding privacy and data processing (European Commission, 2021). Lastly, considering the heightened awareness surrounding societal impacts of climate change, as exemplified by the climate movement led by young people, we anticipate that individuals aged 18 to 30 may demonstrate awareness of both personal and broader societal consequences associated with data commodification, akin to the awareness seen in discussions on climate change. According to the European Qualification Framework (EQF), out of the participants in our sample, 18.8% had a low level (i.e., primary or lower secondary), 53.9% had a medium level (i.e., upper secondary or post-secondary non-tertiary), and 27.3% had a high level (i.e., Bachelor's, Master's, or doctoral degree) of education.

The survey was the same across all countries. The original survey was developed in English and then translated into the national languages of the selected countries with the support of cooperation partners in the respective countries and professional translators at online panel provider company Respondi. For a more detailed overview of the methodological approach, see Gagrčin et al. (2021).

Measures

Independent variables

Personal harm perceptions were measured using four items (ω = .86) adapted from Boerman et al. (2021), asking participants "To what extent do you think that the following may harm you?" regarding social media companies: (1) collecting data about online behaviour, (2) using data for political advertisements, (3) sharing data with other companies, and (4) sharing data with the government (1 = "not at all" to 7 = "to a very large extent"). The items reflected a one-dimensional latent variable according to Confirmatory Factor Analysis (CFA; ω = .86). *Societal harm perceptions* used the same four items but asked about harm to democracy (ω = .86).

Moderators

Perceived individual control[1]was measured with a single item from Pew Research

1. Measuring perceived individual control while using the term "power" is theoretically justified, since the definition of power as the *ability* to control outcomes substantially implies having control or

Center's American Trends Panel (Auxier et al., 2019): "In your view, how much power do individual users have in deciding what happens to our digital data?" (1 = "completely powerless" to 7 = "completely powerful"; M = 3.83, SD = 1.66). The same wording was used to measure *perceived regulatory control*, only asking for government power[2](M = 4.44, SD = 1.56). *Institutional trust* was assessed with a single item from the International Social Survey Programme: Citizenship II (ISSP Research Group, 2016): "Overall, to what extent do you trust the government in your country?" (1 = "completely distrust" to 7 = "completely trust"; M = 3.54, SD = 1.78).

Dependent variables

Preferred individual control and *preferred regulatory control* were measured using single items adapted from Pew (Auxier et al., 2019), asking "How much power should these actors have in deciding what happens to our digital data?" for users (M = 5.36, SD = 1.65) and government (M = 4.53, SD = 1.67), respectively, on the same 7-point scale.

Control variables

We controlled for *age* (M = 24.71, SD = 3.77), *gender* (50% female*), subjective social class* using Kraus et al.'s (2009) ladder measure (M = 5.84, SD = 1.92), *minority status* (9% identified as minority), and *country of residence*. Participants were residents of either Germany (*n* = 481), France (*n* = 487), Greece (*n* = 477), Italy (*n* = 483), Poland (*n* = 463), or Sweden (*n* = 498). In order to distinguish perceptions of personal capacity from structural agency, we use *privacy self-efficacy* (**ω** = .85) adapted from Boerman et al. (2021) – understood as a respondent's perceived *ability* to enact privacy behaviours – as a covariate (since capability typically shifts baseline propensities rather than conditioning the harm, see Baruh et al., 2017; Ahn & Noh, 2020). We asked about the extent to which people agree/disagree with the following statements: "I am able to protect my personal information online," "I feel confident that I can secure my privacy online," and "I can ensure that companies cannot collect my personal information online." By controlling for self-efficacy, we ensure

not (Skinner, 1996; Xu et al., 2012). This allows us to capture the core construct of interest: an individual's perceived influence over what happens to their behavioural data.

2. Based on the principle of subsidiarity, it is actually the EU who has legislative competence in the spheres of information technology, intellectual property, and telecommunications. However, we decided to only include national governments to measure proxy control for two reasons. First, the EU cannot legislate without the national governments' approval. Second, given the complexity of the European legislative system and fairly low levels of knowledge about European institutions (e.g., Pannico, 2017), we could not expect respondents to know which institutional instance has legislative competence.

that our key moderation tests (perceived individual control and perceived regulatory control) capture *structural* beliefs about who holds power over data practices.

Analysis

Since our primary predictors and outcomes were latent variables, we chose Structural Equation Modelling (SEM) to test our hypotheses. Although our data were nested within countries, we decided against a multilevel model for two reasons. First, we did not aim to explain differences between the countries in our sample, and how these differences interact with our variables of interest. Second, with only six countries, there were too few observations at Level 2 for robust modelling (Maas & Hox, 2005). We ultimately created a fixed-effects SEM, using dummy variables to control for the differences between countries (see Measures section).

To avoid inflated estimates, we first checked for possible multicollinearity among all predictors in the model. The only problematic relationship was found between perceptions of individual and societal harm ($\tau = .72$), and this was handled by letting them covary in the model. We then created the SEM, which fit the data sufficiently well (Gibbs et al., 2023; Kay et al., 2009), ?2(257) = 1412.688, $p < .001$, CFI = 0.964, RMSEA = 0.04, 90% CI = [0.042, 0.046], SRMR = 0.03[3]. Figure 1 visualizes the SEM and significant paths, and Table 1 contains all model coefficients.

Results

The results showed that participants from Greece (β = -0.141, 95% CI [-0.198, -0.084], $p < .001$), Poland (β = -0.117, 95% CI [-0.177, -0.056], $p < .001$), and Sweden (β = -0.101, 95% CI [-0.156, -0.046], $p < .001$) wished for less individual data control than participants from Germany. The opposite applied to regulatory data control, with participants from France (β = 0.072, 95% CI [0.019, 0.125], $p = .008$), Greece (β = 0.147, 95% CI [0.092, 0.201], $p < .001$), Italy (β = 0.106, 95% CI [0.053, 0.160], $p < .001$), and Sweden (β = 0.057, 95% CI [0.003, 0.112], $p = .04$) scoring higher than participants from Germany.

Contrary to H1, perceived personal harm was negatively associated with the preferred individual control (β = -0.129, 95% CI [-0.188, -0.07], $p < .001$). This unexpected finding suggests that as individuals perceive greater personal harm, they become *less* inclined to seek individual control. The relationship between personal harm and preferred individual control was negatively moderated by perceived indi-

3. Robust variants were reported for all fit indices but SRMR, as it was not available.

vidual control (β = -0.077, 95% CI [-0.145, -0.009], p = 0.025), supporting H1a and indicating that individuals who already feel some level of control are even less likely to pursue additional individual control mechanisms. Perceived regulatory control (H1b; β = 0.050, 95% CI [-0.018, 0.117], p = 0.149) and institutional trust (H1c; β = 0.002, 95% CI [-0.068, 0.071], p = 0.959) did not significantly affect the relationship between personal harm and preferred individual control.

Further, we found no overall relationship between perceived personal harm and preferred regulatory control (H2; β = 0.055, 95% CI [-0.002, 0.113], p = 0.057). However, this null main effect masks a conditional pattern: the relationship was stronger when perceived regulatory control was high (H2b; β = 0.078, 95% CI [0.025, 0.131], p = 0.004). Perceived individual control (H2a; β = 0.016, 95% CI [-0.039, 0.072], p = 0.562) and institutional trust (H2c; β = -0.048, 95% CI [-0.105, 0.009], p = 0.097) did not significantly affect the (null) relationship between perceived personal harm and preferred regulatory control.

Perceived societal harm was positively associated with preferred individual control (β = 0.384, 95% CI [0.324, 0.443], p < .001), providing support for H3. This association was negatively moderated by perceived regulatory control (β = -0.088, 95% CI [-0.154, -0.021], p = 0.010), corroborating H3b. H3a and H3c were not supported, indicating no significant moderating effects of perceived individual control (β = -0.012, 95% CI [-0.080, 0.055], p = 0.719) and institutional trust (β = -0.055, 95% CI [-0.125, 0.014], p = 0.120) on this relationship.

Finally, H4 was supported: perceived societal harm was also positively associated with the preferred regulatory control (β = 0.119, 95% CI [0.061, 0.178], p < .001). This relationship was positively moderated by institutional trust (β = 0.061, 95% CI [0.004, 0.118], p = 0.037), supporting H4c, but negatively by perceived regulatory control (β = -0.116, 95% CI [-0.170, -0.062], p < .001), supporting H4b. We find no evidence for a moderation by perceived individual control (H4a; β = 0.005, 95% CI [-0.051, 0.061], p = 0.870).

TABLE 2: Full model results

VARIABLE	*β*	CI (lower)	CI (upper)	*se*	*p*
PREFERRED INDIVIDUAL CONTROL					
PERCEIVED PERSONAL HARM	-0.129	-0.188	-0.070	0.030	0.000
PERCEIVED SOCIETAL HARM	0.384	0.324	0.443	0.030	0.000
PRIVACY SELF-EFFICACY	-0.060	-0.103	-0.017	0.022	0.006

INSTITUTIONAL TRUST	-0.011	-0.058	0.037	0.024	0.659
*PERS. HARM * INST. TRUST*	*0.002*	*-0.068*	*0.071*	*0.036*	*0.959*
*SOC. HARM * INST. TRUST*	*-0.055*	*-0.125*	*0.014*	*0.036*	*0.120*
PERCEIVED INDIVIDUAL CONTROL	0.079	0.035	0.124	0.023	0.000
*PERS. HARM * PERCEIVED IND. CONTROL*	*-0.077*	*-0.145*	*-0.009*	*0.034*	*0.025*
*SOC. HARM * PERCEIVED IND. CONTROL*	*-0.012*	*-0.080*	*0.055*	*0.035*	*0.719*
PERCEIVED REGULATORY CONTROL	-0.005	-0.046	0.036	0.021	0.802
*PERS. HARM * PERCEIVED REG. CONTROL*	*0.050*	*-0.018*	*0.117*	*0.034*	*0.149*
*SOC. HARM * PERCEIVED REG. CONTROL*	*-0.088*	*-0.154*	*-0.021*	*0.034*	*0.010*
AGE	0.010	-0.033	0.053	0.022	0.652
GENDER (FEMALE)	0.085	0.042	0.127	0.022	0.000
SOCIAL CLASS	-0.014	-0.057	0.028	0.021	0.500
ETHNIC MINORITY	-0.041	-0.086	0.004	0.023	0.072
FRANCE	-0.026	-0.081	0.030	0.028	0.363
GREECE	-0.141	-0.198	-0.084	0.029	0.000
ITALY	-0.043	-0.100	0.013	0.029	0.134
POLAND	-0.117	-0.177	-0.056	0.031	0.000
SWEDEN	-0.101	-0.156	-0.046	0.028	0.000
PREFERRED REGULATORY CONTROL					
PERCEIVED PERSONAL HARM	0.055	-0.002	0.113	0.029	0.057
PERCEIVED SOCIETAL HARM	0.119	0.061	0.178	0.030	0.000
PRIVACY SELF-EFFICACY	0.013	-0.026	0.051	0.020	0.522
INSTITUTIONAL TRUST	0.251	0.210	0.291	0.021	0.000
*PERS. HARM * INST. TRUST*	*-0.048*	*-0.105*	*0.009*	*0.029*	*0.097*
*SOC. HARM * INST. TRUST*	*0.061*	*0.004*	*0.118*	*0.029*	*0.037*
PERCEIVED INDIVIDUAL CONTROL	-0.048	-0.087	-0.009	0.020	0.017
*PERS. HARM * PERCEIVED IND. CONTROL*	*0.016*	*-0.039*	*0.072*	*0.028*	*0.562*
*SOC. HARM * PERCEIVED IND. CONTROL*	*0.005*	*-0.051*	*0.061*	*0.029*	*0.870*
PERCEIVED REGULATORY CONTROL	0.218	0.183	0.252	0.018	0.000
*PERS. HARM * PERCEIVED REG. CONTROL*	*0.078*	*0.025*	*0.131*	*0.027*	*0.004*

*SOC. HARM * PERCEIVED REG. CONTROL*	*-0.116*	*-0.170*	*-0.062*	*0.027*	*0.000*
AGE	0.048	0.009	0.088	0.020	0.017
GENDER (FEMALE)	-0.014	-0.054	0.026	0.020	0.497
SOCIAL CLASS	0.015	-0.022	0.052	0.019	0.426
ETHNIC MINORITY	-0.008	-0.049	0.033	0.021	0.697
FRANCE	0.072	0.019	0.125	0.027	0.008
GREECE	0.147	0.092	0.201	0.028	0.000
ITALY	0.106	0.053	0.160	0.027	0.000
POLAND	-0.018	-0.073	0.037	0.028	0.522
SWEDEN	0.057	0.003	0.112	0.028	0.040

Note. Interactions are printed in italics; control variables are printed in grey.

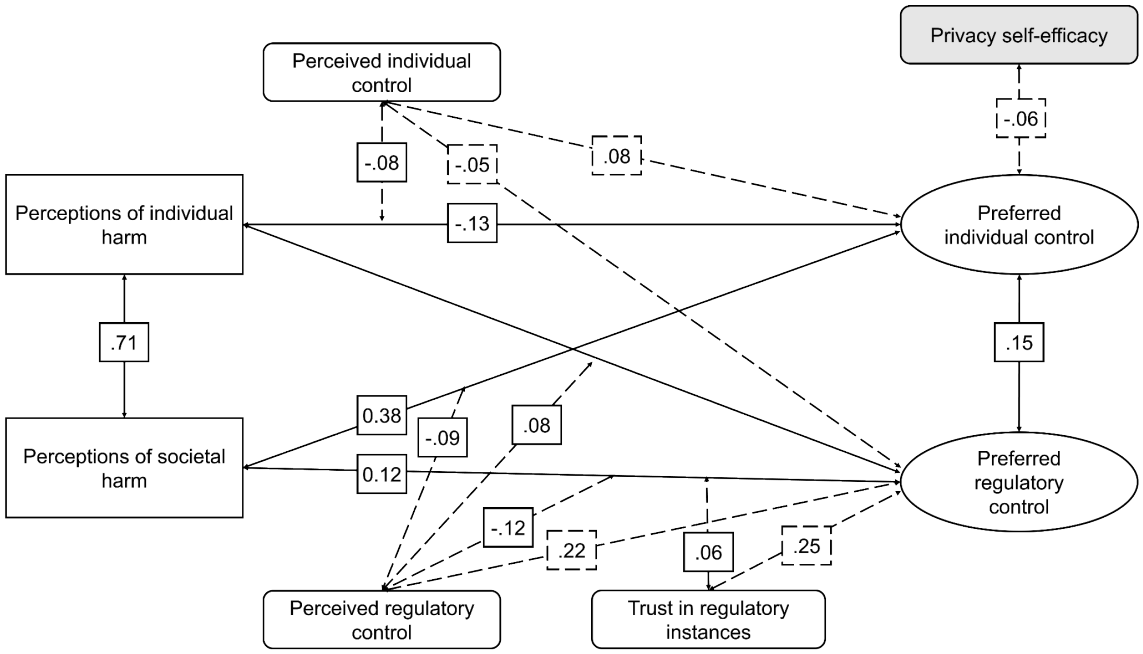

FIGURE 1: Model visualisation and results

Note. All displayed effects are significant at $p < .05$.

Discussion

This paper set out to explain how perceptions of data harms map onto preferences for who should exercise control over platform data practices. Drawing on control theory and compensatory control theory, we argued that both personal and soci-

etal harm perceptions could trigger demands for control, but that the balance between individual and regulatory loci would depend on beliefs about existing control and trust in institutions.

A first, integrative takeaway is that personal and societal harm perceptions are not only conceptually but also empirically close. Sitting under conditions of complexity and data uncertainty where outcomes and probabilities are hard to specify and harms can be diffuse and cumulative (Stirling, 2019; Shelby et al., 2023), personal and societal harm are strongly correlated, which likely reflects a common risk appraisal about the digital environment. Still, they feed into different control preferences, meaning that while related, they are not isomorphic, and shouldn't be treated as a proxy for the other but rather kept analytically distinct.

Against H1, we find that perceived personal harm is negatively associated with preferred individual control. Self-focused harm appears to erode perceived efficacy at the individual locus, thus making "more settings, more consent" less attractive when harm is salient. This reading is reinforced by the negative moderation effect of perceived individual control (H1a), as well as the negative correlation between privacy self-efficacy (controlled for) and preferred individual control. Although we did not directly measure resignation, surveillance realism, or algorithmic alienation (perceived individual control serves as a proxy for these dynamics, albeit an oversimplified one), they can help interpret this finding. Privacy resignation might explain why citizens may abandon individual control efforts when they perceive the task as overwhelming (Draper & Turow, 2019); surveillance realism reflects the recognition that datafication is inescapable (Dencik & Cable, 2017), while algorithmic alienation -where individuals become separated from their data as data becomes "a power on its own" (Marx, 1974, p. 325, as cited in Andrejevic, 2013) - how users lose connection to their data through opaque aggregation and analysis processes. Put simply: once people feel they already do what can be done, additional levers seem futile in the face of fundamental limitations of personal measures against massive data harvesting and appropriation (Couldry & Meijas, 2019; Zuboff, 2019). In this sense, the result does not overturn the CCT but rather signals a boundary condition, suggesting that individual control preferences may decline when harm salience coexists with a sense of already "doing all one can." Future work could operationalize these concepts as distinct but related dimensions the erosion of individual efficacy in the face of datafication: alienation as an expression of the structural relationship between users and their data, realism reflecting the cognitive assessment, and resignation the affective response (see also Gagrčin et al., 2024 for a similar dimensionalisation).

Further, we found no significant relationship between personal harm perception and preferred regulatory control (H2). At the same time, and in contrast to H2b, this relationship was stronger when perceived regulatory control was high. Since our measure of perceived regulatory control indexes perceived *capacity*, this moderation can be read as a boundary condition. CCT predicts shifts toward external agents when those agents are seen as efficacious, so when citizens experience resignation, develop realism about structural limitations, and feel alienated from their data, they may perceive data governance as beyond both individual *and* governmental control, particularly under conditions where even regulators face significant information asymmetries compared to platforms (Neudert, 2023). In other words, endorsement of regulation is contingent on perceived regulatory capacity and trust, not merely on perceived harm.

By contrast, societal harm predicts higher preference for both individual *and* regulatory control, in line with H3–H4. The positive link between societal harm and individual control is a classic CCT effect: when external order looks shaky, people upweight personal agency to reassert predictability. In addition, since research shows that privacy concerns predict protective behaviour (Baruh et al., 2017), so too can a rise in broad, system-related concern plausibly increase desire for individual safeguards. The supported H4 aligns with previous findings that perceptions of harm extending beyond the individual relate to support for restrictive policies (Snider et al., 2021) and governmental regulation (Huang & Cao, 2023; Riedl et al., 2022). Together, H3–H4 suggest that collective threats do not necessarily crowd out personal agency but prompt people to hedge at multiple control instances (e.g., Goode & Keefer, 2016; Rodríguez-López et al., 2022). This is also in line with Shelby et al. (2023) who show that harms are experienced across micro–meso–macro levels and can travel between them, so simultaneous responses at multiple control loci are theoretically plausible.

Both H3 and H4 relationships were weaker when respondents perceived regulators as already effective (H3b, H4b), consistent with a substitution–safety signal account: when authorities are seen as already effective, the marginal need for extra control (whether individual or regulatory) diminishes (Ahn & Noh, 2020; Xu et al., 2012). In contrast, institutional trust strengthened the relationship between societal-harm and preferred regulatory control (H4c), consistent with delegating control to credible institutions (Auxier et al., 2019). However, institutional trust shows no moderating effect on societal harm-individual control relationship. This pattern is also consistent with work showing that when domains feel complex and people feel dependent, trust in government rises and functions as a cue for delegation

rather than self-help, thus orienting citizens toward institutional solutions and, potentially, avoidance of the threatening topic altogether (Ahn & Noh, 2020; Shepherd & Kay, 2012). In our setting, that helps explain why trust strengthens the move to regulation but does not alter the impulse to demand for individual control. Together, these patterns suggest that responses to system-level threats are layered: people hedge with personal control mechanisms *and* back collective solutions, but the strength of each route depends on whether regulators are seen as powerful and trustworthy enough.

The strong relationship between harm perceptions and regulatory oversight might also reflect our research context across six EU countries that may have "a strong reputation for enforcing government legislation" (like Singapore in Xu et al., 2012, p. 1358). However, we find some notable cross-country differences: France, Greece and Italy demonstrated stronger preferences for regulatory data control compared to Germany, while respondents from Greece, Poland, and Sweden showed comparably lower preferences for individual data control mechanisms. These cross-national differences underscore that specific national contexts matter for citizens' perspectives on data governance (Arner et al., 2022; Dammann & Glasze, 2023), suggesting that while European citizens broadly recognize the relationship between societal harm and regulatory needs, their approaches to proxy control vary significantly (Xu et al., 2012). Future research should consider multilevel analyses that account for country-specific regulatory traditions, cultural attitudes toward privacy, or other institutional factors explaining these differences. That said, it should be noted that while our theoretical lens applies to adults generally, results here should be interpreted within the scope of a young-adult sample. The patterns we observe may differ among older cohorts with distinct digital socialisation histories (Bolin, 2017), so a replication with more age-diverse samples is warranted.

Taken together, individual and regulatory control read as complementary rather than competing approaches, whose relative weight depends on perceived control and trust. The negative relationship between personal harm and preferred individual control signals that at the level of the self, young Europeans see diminishing returns to user-centric levers when harms feel diffuse and structurally produced; at the same time, societal-harm salience moves along with support for both personal and policy levers, with perceived regulatory control and institutional trust governing how much extra control people want to layer on.

In terms of policy, our study suggests that because individual and societal harm perceptions are closely related but not interchangeable, regulators should treat them as distinct inputs when designing interventions. Measures that only address

individual protection may fail to mitigate perceived harms at the collective level, while interventions aimed to protect society at large may not address individual-level dynamics. Specifically, an overreliance on individual control mechanisms (such as consent requirements and transparency tools) in regulatory approaches are not only insufficient but might even be counterproductive. For people who already perceive privacy related harms, individual control mechanisms may feel like band-aid solutions that fail to address deeper structural issues. That is, individual control mechanisms inadvertently shift the burden of data governance onto citizens, asking them to navigate opaque algorithmic processes, rather than addressing the conditions that give rise to data appropriation in the first place. Worse, they may legitimize data harms by framing them as acceptable so long as a formal consent process has been followed. Our results further indicate that societal harms are drivers of both individual and collective preferences for stronger governance. This underscores the importance of addressing societal dimensions of data harms in regulatory frameworks. Risk-based regulatory frameworks, such as the EU AI and Digital Services Act, represent an important step in this direction, as they rightfully recognize the need for societal-level protection and attempt to confront the conditions that generate both individual and collective harms.

Limitations

Let us start with obvious shortcomings: our cross-sectional design limits our ability to establish causality or track evolving perceptions and our data are from 2021 and thus may not fully reflect more recent shifts in public discourse, policy developments, and technological adoption, especially in regards to AI. While we acknowledge these limitations, we argue that this period captures a uniquely informative snapshot: the widespread use of digital health management tools heightened concerns about government intrusion and corporate surveillance, while making tensions between individual and societal data harms (particularly the trade-off between public health protection and privacy rights) especially visible. Secondly, the fundamental relationships we identify between perceived harms and regulatory preferences likely remain relevant to current policy discussions given the stable nature of such attitudes. Nevertheless, as the EU continues to implement and refine its approach to AI regulation and platform governance, *longitudinal* studies are needed to track shifts in citizens' perceptions of harm and control preferences over time, while accounting for additional variables like ideology and algorithm literacy (Gagrčin et al., 2024; Huang & Cao, 2022).

Further, several measurement limitations warrant acknowledgment. First, unlike

individual control (where people have tangible experiences with privacy settings), assessing regulatory effectiveness involves complex institutional factors most individuals presumably do not engage with deeply. Second, several key constructs are measured using single items. While we have taken steps to ensure statistical validity regardless, we recognize that multi-item scales would better capture these constructs' full dimensionality. Third, our focus on national governments overlooks the multilevel governance reality in Europe, where the EU plays a crucial regulatory role. Though we provided, in our opinion, compelling reasons for this approach, especially given our young sample, excluding EU institutions may misrepresent how young Europeans conceptualise regulatory control. Further, our predictors use an abstract frame ("ordinary users"), while personal harm is self-referent. Here, we acknowledge that difference in item framing can induce third-person perceptions and shift absolute levels. Future work should compare self vs abstract wording within respondents. While we distinguish between individual and societal harm, our measures do not capture the full spectrum of potential harms (e.g., Shelby et al., 2023) that might influence control preferences differently. This calls for more contextual, domain-specific, and potentially platform-specific approaches to harm perceptions and control preferences (Gagrčin et al., 2024).

Finally, while we discuss complexity and uncertainty as structural features of platforms that theoretically shape how harms are perceived, we did not directly measure uncertainty or complexity perceptions. Because these factors served as contextual framing rather than testable mechanisms, we believe that this limitation does not affect our main results. Still, future research should assess perceived uncertainty as a potential antecedent or moderator of harm appraisal and control preferences. We also do not measure dispositional *need for control*, which is relevant for understanding individual experiences under uncertainty; PIC, PRC, and institutional trust capture beliefs about who can act effectively, not the underlying control motive. Incorporating direct measures of perceived uncertainty and control dispositions would allow future work to clarify the psychological pathways through which data harms translate into control preferences.

References

Adams, Z., & Osman, M. (2023). Institutional trust, risk and product safety: A consumer survey. *Journal of Risk Research*, *26*(6), 648–674. https://doi.org/10.1080/13669877.2023.2204875

Ahn, J., & Noh, G.-Y. (2020). Determinants of environmental risk information seeking: An emphasis on institutional trust and personal control. *Health, Risk & Society*, *22*(3–4), 214–230. https://doi.org/10.1080/13698575.2020.1813261

Andrejevic, M. (2013). *Alienation's returns* (C. Fuchs & M. Sandoval, Eds; 1st edn). Taylor & Francis.

Arner, Douglas W.; Castellano, Giuliano G.; Selga, Eriks K.; (2022). *The transnational data governance problem*. https://doi.org/10.15779/Z38GF0MX5G

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, *52*(1), 1–26. https://doi.org/10.1146/annurev.psych.52.1.1

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

Bendix, W., & MacKay, J. (2022). Fox in the henhouse: The delegation of regulatory and privacy enforcement to big tech. *International Journal of Law and Information Technology*, *30*(2), 115–134. https://doi.org/10.1093/ijlit/eaac011

Birch, K., Cochrane, D., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society*, *8*(1), 20539517211017308. https://doi.org/10.1177/20539517211017308

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

Bolin, G. (2017). *Media generations: Experience, identity and mediatised social change*. Routledge.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Cevallos, A. (2025). How autocrats weaponize AI - and how to fight back. *Journal of Democracy*. https://www.journalofdemocracy.org/online-exclusive/how-autocrats-weaponize-ai-and-how-to-fight-back

Couldry, N., & Meijas, U. (2019). *The cost of connection. How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Dammann, F., & Glasze, G. (2023). Governing digital circulation: The quest for data control and sovereignty in Germany. *Territory, Politics, Governance*, *11*(6), 1100–1120. https://doi.org/10.1080/21622671.2022.2141850

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, *11*, 763–781.

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

European Commission. (2020). *Special Eurobarometer 503: Attitudes towards the impact of digitalisation on daily lives*. https://europa.eu/eurobarometer/surveys/detail/2237

European Commission. (2021). *Special Eurobarometer 518: Digital rights and principles*. https://europ

a.eu/eurobarometer/surveys/detail/2270

Fritsche, I. (2022). Agency through the We: Group-based control theory. *Current Directions in Psychological Science*, *31*(2), 194–201. https://doi.org/10.1177/09637214211068838

Gagrčin, E., Naab, T. K., & Grub, M. F. (2024). Algorithmic media use and algorithm literacy: An integrative literature review. *New Media & Society*, 14614448241291137. https://doi.org/10.1177/14614448241291137

Gagrčin, E., Schaetz, N., Rakowski, N., Toth, R., Renz, A., Vladova, G., & Emmer, M. (2021). *We and AI - Living in a datafied world: Experiences & attitudes of young Europeans*. Weizenbaum Institute. https://doi.org/10.34669/WI/1

Gibbs, W. C., Kim, H. S., Kay, A. C., & Sherman, D. K. (2023). Who needs control? A cultural perspective on the process of compensatory control. *Social and Personality Psychology Compass*, *17*(2), e12722. https://doi.org/10.1111/spc3.12722

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. University of California Press.

Goode, C., & Keefer, L. A. (2016). Grabbing your bootstraps: Threats to economic order boost beliefs in personal control. *Current Psychology*, *35*(1), 142–148. https://doi.org/10.1007/s12144-015-9376-0

Goudsmit, S. A. (1972). An *ad hoc* committee. *Physical Review Letters*, *29*(3), 143–143. https://doi.org/10.1103/PhysRevLett.29.143

Habermas, J. (2023). *A new structural transformation of the public sphere and deliberative politics*. Polity.

Hargittai, E., & Marwick, A. (2016). *'What can I really do?': Explaining the privacy paradox with online apathy*. https://doi.org/10.5167/UZH-148157

Huang, Y., & Cao, X. (2023). Calling on the third-party privacy control into algorithmic governance framework: Linking users' presumed influence with control agency theory. *International Journal of Public Opinion Research*, *35*(4), edad036. https://doi.org/10.1093/ijpor/edad036

Humprecht, E., Castro Herrero, L., Blassnig, S., Brüggemann, M., & Engesser, S. (2022). Media systems in the digital age: An empirical comparison of 30 countries. *Journal of Communication*, *72*(2), 145–164. https://doi.org/10.1093/joc/jqab054

ISSP Research Group. (2016). *International social survey programme: Citizenship II - ISSP 2014* (Version 2.0.0) [Data set]. GESIS Data Archive. https://doi.org/10.4232/1.12590

Jiang, G., & Yang, W. (2023). Signal effect of government regulations on ride-hailing drivers' intention to mobile-based transportation platform governance: Evidence from China. *Transport Policy*, *139*, 63–78. https://doi.org/10.1016/j.tranpol.2023.05.009

Kay, A. C., Gaucher, D., Napier, J. L., Callan, M. J., & Laurin, K. (2008). God and the government: Testing a compensatory control mechanism for the support of external systems. *Journal of Personality and Social Psychology*, *95*(1), 18–35. https://doi.org/10.1037/0022-3514.95.1.18

Kay, A. C., Whitson, J. A., Gaucher, D., & Galinsky, A. D. (2009). Compensatory control: Achieving order through the mind, our institutions, and the heavens. *Current Directions in Psychological Science*, *18*(5), 264–268. https://doi.org/10.1111/j.1467-8721.2009.01649.x

Knight, F. H. (1964). *Risk, uncertainty and profit*. Sentry Press.

Kraus, M. W., Piff, P. K., & Keltner, D. (2009). Social class, sense of control, and social explanation. *Journal of Personality and Social Psychology*, *97*(6), 992–1004. https://doi.org/10.1037/a0016357

Landau, M. J., Kay, A. C., & Whitson, J. A. (2015). Compensatory control and the appeal of a structured world. *Psychological Bulletin*, *141*(3), 694–722. https://doi.org/10.1037/a0038703

Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology*, *32*(2), 311–328. https://doi.org/10.1037/0022-3514.32.2.311

Lou, X., Li, L. M. W., & Ito, K. (2025). Compensating personal climate response inefficacy with political conservatism? *Political Psychology*, pops.70045. https://doi.org/10.1111/pops.70045

Maas, C. J. M., & Hox, J. J. (2005). Sufficient sample sizes for multilevel modeling. *Methodology*, *1*(3), 86–92. https://doi.org/10.1027/1614-2241.1.3.86

Mackenzie, A. (2019). From API to AI: Platforms and their opacities. *Information, Communication & Society*, *22*(13), 1989–2006. https://doi.org/10.1080/1369118X.2018.1476569

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society*, *12*(2), 93–106. https://doi.org/10.1108/JICES-08-2013-0030

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57. https://doi.org/10.1287/orsc.11.1.35.12567

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006

Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data & Society*, *10*(1), 20539517231166886. https://doi.org/10.1177/20539517231166886

Neudert, L.-M. (2023). Regulatory capacity capture: The United Kingdom's online safety regime. *Internet Policy Review*, *12*(4). https://doi.org/10.14763/2023.4.1730

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

Nyabola, N. (2020, January 18). *Cambridge Analytica and the end of elections*. Al Jazeera. https://www.aljazeera.com/opinions/2020/1/18/cambridge-analytica-and-the-end-of-elections

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising*, *38*(4), 63–77. https://doi.org/10.2753/JOA0091-3367380405

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization Studies*, *28*(9), 1435–1448. https://doi.org/10.1177/0170840607081138

Pannico, R. (2017). Is the European Union too complicated? Citizens' lack of information and party cue effectiveness. *European Union Politics*, *18*(3), 424–446. https://doi.org/10.1177/1465116517699892

Pauer, S., Rutjens, B. T., & Van Harreveld, F. (2024). Trust is good, control is better: The role of trust and personal control in response to threat. *Journal of Applied Social Psychology*, *54*(9), 552–571. https://doi.org/10.1111/jasp.13058

Pinto, I. R., Frings, D., & Marques, J. M. (2024). Social exclusion and vigilantism toward criminal offenders as compensatory reactions to the perceived inefficacy of social control. *Peace and Conflict: Journal of Peace Psychology*, *30*(3), 308–316. https://doi.org/10.1037/pac0000742

Regan, M. P. (1995). *Legislating privacy: Technology, social values, and public policy*. The University of North Carolina Press.

Renieris, E. M. (2023). *Beyond data: Reclaiming human rights at the dawn of the metaverse*. The MIT Press.

Riedl, M. J., Naab, T. K., Masullo, G. M., Jost, P., & Ziegele, M. (2021). Who is responsible for interventions against problematic comments? Comparing user attitudes in Germany and the United States. *Policy & Internet*, *13*(3), 433–451. https://doi.org/10.1002/poi3.257

Rodríguez-López, Á., De Lemus, S., Bukowski, M., Potoczek, A., & Fritsche, I. (2022). Political change as group-based control: Threat to personal control reduces the support for traditional political parties. *PLOS ONE*, *17*(12), e0278743. https://doi.org/10.1371/journal.pone.0278743

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Schaetz, N., Gagrčin, E., Toth, R., & Emmer, M. (2025). Algorithm dependency in platformized news use. *New Media & Society*, *27*(3), 1360–1377. https://doi.org/10.1177/14614448231193093

Scoones, I. (2019). *What is uncertainty and why does it matter?* Institute of Development Studies. https://opendocs.ids.ac.uk/articles/report/What_is_Uncertainty_and_Why_Does_it_Matter_/26432353

Shelby, R., Rismani, S., Henne, K., Moon, Aj., Rostamzadeh, N., Nicholas, P., Yilla-Akbari, N., Gallegos, J., Smart, A., Garcia, E., & Virk, G. (2023). Sociotechnical harms of algorithmic systems: Scoping a taxonomy for harm reduction. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*, 723–741. https://doi.org/10.1145/3600211.3604673

Shepherd, S., & Kay, A. C. (2012). On the perpetuation of ignorance: System dependence, system justification, and the motivated avoidance of sociopolitical information. *Journal of Personality and Social Psychology*, *102*(2), 264–280. https://doi.org/10.1037/a0026272

Shockley, E., & Fairdosi, A. S. (2015). Power to the people? Psychological mechanisms of disengagement from direct democracy. *Social Psychological and Personality Science*, *6*(5), 579–586. https://doi.org/10.1177/1948550614568159

Skinner, E. A. (1996). A guide to constructs of control. *Journal of Personality and Social Psychology*, *71*(3), 549–570. https://doi.org/10.1037/0022-3514.71.3.549

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/science.3563507

Smuha, N. A. (2021). Beyond the individual: Governing AI's societal harm. *Internet Policy Review*,

10(3). https://doi.org/10.14763/2021.3.1574

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Stirling, A. (2019). *Politics in the language of uncertainty*. STEPS Centre, University of Sussex. https://steps-centre.org/blog/politics-in-the-language-of-uncertainty/

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). **Research note**—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, *23*(4), 1342–1363. https://doi.org/10.1287/isre.1120.0416

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile books.

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & De Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82. https://doi.org/10.18352/ulr.420

Published by

Alexander von Humboldt Institute for Internet and Society

CAIS Research for the Digital Age

in cooperation with

CREATe

cnrs centre internet et societe

UOC R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies