Brandimarte, Laura; Gutmann, Jerg; Muehlheusser, Gerd; Weber, Franziska

Working Paper

Privacy Concerns and Willingness to Adopt AI Products: A Cross-Country Randomized Survey Experiment

CESifo Working Paper, No. 11774

Provided in Cooperation with:
Ifo Institute – Leibniz Institute for Economic Research at the University of Munich

Suggested Citation: Brandimarte, Laura; Gutmann, Jerg; Muehlheusser, Gerd; Weber, Franziska (2025) : Privacy Concerns and Willingness to Adopt AI Products: A Cross-Country Randomized Survey Experiment, CESifo Working Paper, No. 11774, CESifo GmbH, Munich

This Version is available at:
https://hdl.handle.net/10419/316888

CESifo WORKING PAPERS

11774
2025

March 2025

Privacy Concerns and Willingness to Adopt AI Products: A Cross-Country Randomized Survey Experiment

Laura Brandimarte, Jerg Gutmann, Gerd Muehlheusser, Franziska Weber

CESifo

Impressum:

CESifo Working Papers
ISSN 2364-1428 (electronic version)
Publisher and distributor: Munich Society for the Promotion of Economic Research - CESifo GmbH
The international platform of Ludwigs-Maximilians University's Center for Economic Studies and the ifo Institute
Poschingerstr. 5, 81679 Munich, Germany
Telephone +49 (0)89 2180-2740, Telefax +49 (0)89 2180-17845, email office@cesifo.de
Editor: Clemens Fuest
https://www.cesifo.org/en/wp
An electronic version of the paper may be downloaded
· from the SSRN website: www.SSRN.com
· from the RePEc website: www.RePEc.org
· from the CESifo website: https://www.cesifo.org/en/wp

CESifo *Working Paper No. 11774*

Privacy Concerns and Willingness to Adopt AI Products: A Cross-Country Randomized Survey Experiment

Abstract

We examine the trade-off between functionality and data privacy inherent in many AI products by conducting a randomized survey experiment with 1,734 participants from the US and several European countries. Participants' willingness to adopt a hypothetical, AI-enhanced app is measured under three sets of treatments: (i) installation defaults (opt-in vs. opt-out), (ii) salience of data privacy risks, and (iii) regulatory regimes with different levels of data protection. In addition, we study how the willingness to adopt depends on individual attitudes and preferences. We find no effect of defaults or salience, while a regulatory regime with stricter privacy protection increases the likelihood that the app is adopted. Finally, greater data privacy concerns, greater risk aversion, lower levels of trust, and greater skepticism toward AI are associated with a significantly lower willingness to adopt the app.

JEL-Codes: D800, D900, K240, L860, Z100.

Keywords: artificial intelligence, privacy concerns, randomized survey experiment, smart products, technology adoption.

Laura Brandimarte
Eller College of Management
University of Arizona, Tucson / AZ / USA
lbrandimarte@arizona.edu

Jerg Gutmann
Institute of Law and Economics
University of Hamburg / Germany
jerg.gutmann@uni-hamburg.de

Gerd Muehlheusser
Department of Economics
University of Hamburg / Germany
gerd.muehlheusser@uni-hamburg.de

Franziska Weber
School of Law, Erasmus University
Rotterdam / The Netherlands
weber@law.eur.nl

March 21, 2025
This study was pre-registered with the Open Science Foundation (osf.io/xahej). We thank Saharsh Agarwal and Nishargo Nigar as well as participants at the 2024 WISE Conference in Bangkok, the 2025 EMLE Midterm Meeting Workshop, and the 2025Workshop in Microeconomics at the University of Hamburg for their helpful comments and suggestions. We gratefully acknowledge financial support by the Center of Interdisciplinary Research (ZiF) at Bielefeld University (Research Group "Economic and Legal Challenges in the Advent of Smart Products"). IRB approval was obtained from the University of Hamburg's Faculty of Economic and Social Sciences.

1 Introduction

Recent technological developments have made artificial intelligence (AI) a crucial feature of many commercial products—from autonomous vehicles to health and smart home devices, from apps for real-time language translation and editing to software for financial transactions, such as wire transfers and stock market analysis. AI enables functionalities that were previously inconceivable. So, it is no surprise that products like ChatGPT have been welcomed with great enthusiasm, since their launch to the public, and attracted the attention of users at an unprecedented speed.[1] However, official estimates suggest that there still is reluctance to use AI for productive activities in Western economies, both in Europe[2] and North America.[3] AI-enhanced products and services may attract excited early adopters, but there seems to be a considerable share of the population –in fact, the majority on both continents on either side of the Atlantic– that is not yet convinced. In this paper, we explore the factors that may hinder the adoption of an AI-enhanced product or service. We focus on individual consumers' privacy concerns regarding such products, which are notoriously data-intensive (Whang et al., 2023), as well as other personal characteristics, and derive important managerial implications. To the best of our knowledge, this study is the first attempt to systematically explore and compare such factors, specifically in the United States and continental Europe.

For this exploration, we conducted a cross-country randomized experiment. It focuses on a specific hypothetical product, an AI-enhanced email app, in order to provide participants with a scenario as close as possible to a real-world choice whether to adopt an AI-enhancement.[4] Consistent with existing literature on the adoption of AI products, such as in health management services (Hong and Cho, 2023) or autonomous vehicles (Kyriakidis, Happee, and de Winter, 2015), we introduce a hypothetical AI-based app called "Smart-Scan". In our experiment, participants are offered the possibility to adopt this app which learns from email correspondence to simplify the writing and enhance the quality of personalized emails in various languages. This scenario is timely, as such text generators are currently one of the fastest-growing AI-based technologies. In several treatments, we explore the relevance of defaults, salience, and regulatory regimes for participants' willingness to use Smart-Scan. We study default settings because the behavioral economics literature suggests that they generally have strong behavioral effects (Jachimowicz et al., 2019) and, at the same time, the defaults set by providers—of technology in general and AI products in particular—can have important privacy implications (Acquisti et al., 2017). Regulating default settings is also a low-cost policy intervention. Furthermore, we evaluate whether increasing the salience of data privacy risks makes a difference, since previous research has demonstrated

[1] ChatGPT, e.g., reached 100 million users within one year from its release in the Fall of 2022 (`https://www.theverge.com/2023/11/6/23948386/chatgpt-active-user-count-openai-developer-conference`, last accessed on January 15, 2025), making it the fastest growing technology in the field until Threads arrived.

[2] `https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240529-2`, last accessed on January 15, 2025.

[3] `https://www.census.gov/library/stories/2023/11/businesses-use-ai.html`, last accessed on January 15, 2025.

[4] We do not consider cases where the consumer must adopt the AI-enhancement, or where full privacy preservation is guaranteed.

a significant asymmetry between providers and users of a product or service regarding their awareness of privacy trade-offs (Acquisti, Brandimarte, and Loewenstein, 2020). Does the remarkably fast and widespread adoption of technologies like large language models result from a true lack of privacy concerns or rather from a lack of transparency regarding the relevant privacy trade-offs, as previous literature may suggest (Tsai et al., 2011)? Moreover, we test for effects of various regulatory regimes because the level of protection they entail for AI-related technology impacts consumers and firms differently, as the introduction of the European General Data Protection Regulation (GDPR; Godinho de Matos and Adjerid 2022; Johnson, Shriver, and Goldberg 2023) illustrates. However, it is crucial to not only compare regulatory regimes, but also to study respondents from countries governed by different regulatory frameworks to test for heterogeneous preferences across these populations. Finally, we study how participants' adoption of Smart-Scan is influenced by personal characteristics, such as risk preferences, trust, privacy concerns, and views on algorithmic decision-making. The experiment was conducted online with participants from the United States and several continental European countries. Interestingly, our main finding is that while defaults and salience are not decisive factors, the applicable privacy regime and individuals' privacy concerns and economic attitudes significantly affect their willingness to adopt an AI-enhancement.

Our work has important managerial and policy implications. First, understanding whether users have concerns regarding data sharing with providers of AI technologies offers crucial insights to investors in and developers of such technologies, potentially shaping the design of products and services (Alkhatib et al., 2020) as well as innovation and industry competitiveness (Voss and Houser, 2019). Second, understanding user preferences regarding existing privacy regimes can guide the design of privacy policies in general and business decisions regarding the choice of business and server locations more specifically. Finally, user preferences over regulatory regimes can inform policy decisions regarding the design of regulatory frameworks that govern cross-country data sharing, such as the EU-US Data Privacy Framework.

The remainder of the paper is structured as follows. Section 2 lays the theoretical foundations for the adoption decision of AI technology in light of privacy concerns, and it derives a set of hypotheses for empirical testing. Section 3 explains the experimental design and its practical implementation. The empirical analysis is presented in Section 4. Section 5 discusses key managerial and policy implications of our findings. Section 6 points to limitations of the study and outlines directions for future research, before Section 7 concludes. The Online Appendix contains experimental instructions as well as supplementary empirical results.

2 Theoretical background

Technology acceptance has a long history in the information systems literature, dating back to the late 1980s and the seminal Technology Acceptance Model (Davis, Bagozzi, and Warshaw, 1989), which identified ease of use and especially perceived short-term usefulness (Chau, 1996) as the main determinants of individuals' intention to use a technology. Venkatesh et al. (2003) expanded

the model by integrating other major theories of technology acceptance and established a unified theory of acceptance and use of technology, identifying four direct determinants: performance and effort expectancy (analogous to usefulness and ease of use), social influence (especially relevant social norms), and facilitating conditions (i.e., external constraints). However, even the expanded version of the model does not account for potential consumers' attitudes and preferences that could be relevant to technology adoption. More recent work by Dhagarra, Goswami, and Kumar (2020) has incorporated individuals' privacy concerns into the Technology Acceptance Model in the context of healthcare. Their results confirm that, in addition to perceived usefulness and ease of use, trust and privacy concerns are significant predictors of patients' technology acceptance. Similarly, earlier work found that the strongest drivers of the acceptance of biometric identification systems are trust in technology and perceived privacy risk (Miltgen, Popovič, and Oliveira, 2013). We build on this literature by examining whether privacy concerns and other economic attitudes, specifically risk attitudes and trust, play a role in individuals' willingness to adopt AI-enhanced products.

A large body of research in behavioral economics has shown that human behavior can be affected by the architecture of choice sets (Thaler and Sunstein, 2008). In particular, default effects strongly affect choices and behaviors in a variety of contexts, from retirement plans (Madrian and Shea, 2001; Beshears et al., 2009) to organ donations (Johnson and Goldstein, 2003), but also, specifically, privacy decision-making (Anaraky et al., 2018; Graßl et al., 2021). Because of the uncertainties surrounding privacy trade-offs, privacy default settings for services and products may be especially effective (Acquisti et al., 2017), at times encouraging errors in judgment (e.g., since an option is offered as default, one may assume that it is sufficiently protective of one's privacy; see Leon et al. 2012). Therefore, we expect the following:

Hypothesis 1 (Default)**.** *Individuals are more willing to adopt Smart-Scan if the app is activated by default.*

Privacy risks associated with sharing personal information are uncertain and difficult to grasp, resulting in many people discounting or ignoring them altogether (Acquisti and Grossklags, 2007). A more salient presentation of privacy risks, however, has been shown to significantly affect privacy-related choices (Tsai et al., 2011). Thus, we expect that explaining what personal information would be shared with a system will decrease individuals' willingness to use it. In other words, we expect that:

Hypothesis 2 (Salience)**.** *Individuals are less willing to adopt Smart-Scan if data privacy risks are described in more detail.*

Public policies can significantly impact the perceived trustworthiness and acceptance of an information system (e.g., in public health, see Meredith et al., 2007), as they can reassure citizens of their legally protected privacy rights. The European Union's GDPR, for instance, was shown to have positive effects on European citizens' willingness to share data with service providers, who are now forced to be transparent in their privacy policies and request informed consent for data

collection and use (Godinho de Matos and Adjerid, 2022), and led to some privacy improvements for consumers (Johnson, 2024). Therefore, we compare the effects of applicable data protection laws based on data stored in jurisdictions with different levels of de facto protection of privacy, and hypothesize that the willingness to use a system that requires sharing personal information is higher if laws strictly regulate the market for personal information, especially policies restricting government access to stored personal data:

Hypothesis 3 (Regulatory regime)**.** *Individuals are more willing to adopt Smart-Scan if shared personal information is more strictly protected by local data protection law.*

Besides the strictness of the regulatory framework, there are also other reasons why users may prefer data storage in a particular jurisdiction—typically in their country of residence. This home bias effect can be observed, for example, in finance when investors deviate from an optimally diversified portfolio and prefer to over-invest in domestic assets (Gaar, Scherer, and Schiereck, 2020). A home bias could exist due to greater familiarity with the legal system, the expectation of judiciaries being biased towards protecting the interests of local citizens, or behavioral factors, such as patriotism (Enke, 2020). In our context, these considerations imply that:

Hypothesis 4 (Home bias)**.** *Individuals are more willing to adopt Smart-Scan if their data is stored in their home jurisdiction.*

Furthermore, not only properties of the AI technology in question, but also individual attitudes and preferences of potential consumers play a key role in the decision to adopt it. We consider three types of attitudes; (i) general concerns about privacy, (ii) attitudes towards the risks and trust entailed in sharing data with others, and (iii) specific concerns about AI technology. First of all, individuals who are generally more concerned about privacy are expected to be less willing to use technologies that require users to share personal information:

Hypothesis 5 (Privacy concerns)**.** *Individuals with higher levels of privacy concern are less willing to adopt Smart-Scan.*

Attitudes that are generally important for economic decision-making (Falk et al., 2018), such as risk-aversion and generalized trust, may also be relevant to the adoption of AI-based products. Here, risk can be defined as the potential of incurring a loss while in pursuit of a desired outcome from using a technology (Featherman and Pavlou, 2003). Given the significant uncertainty associated with sharing personal data, more risk-averse individuals should be less inclined to expose themselves to the possible consequences. It is difficult to anticipate who gains access to one's personal data once it is shared, what it will be used for, and what harm it could cause (Pew Research Center, 2019).

Hypothesis 6 (Risk aversion)**.** *More risk-averse individuals are less willing to adopt Smart-Scan.*

Trust is a fundamental building block of relationships, not only among humans but also between humans and non-human entities (Dinev, McConnell, and Smith, 2015). Trust can be defined

as "… the extent to which one feels secure and psychologically comfortable about depending on the trustee" (Komiak and Benbasat, 2006). An individual who is generally more trusting should be more willing to adopt technologies that entrust others with their personal data:

Hypothesis 7 (Trust)**.** *More trusting individuals are more willing to adopt Smart-Scan.*

Finally, artificial intelligence may, just like other significant technological innovations (e.g., GMOs or mRNA vaccines), be met with serious skepticism by many. AI may be rejected not only because of its feared consequences for one's privacy, but also because of how it is expected to affect society more broadly, for example, in terms of creating, changing, and displacing jobs or by compromising the verifiability of information in the public sphere (Acemoglu, 2024). If motivated by these general concerns, the decision not to adopt AI technology may be considered expressive behavior (Hillman, 2010).

Hypothesis 8 (AI skepticism)**.** *Individuals who are generally concerned about the use of AI-based algorithms are less willing to adopt Smart-Scan.*

3 Survey experiment

3.1 Design

In our pre-registered randomized survey experiment, participants are told about a hypothetical new AI-based app called Smart-Scan that would become available free of charge with the next update of their email app. Its functionalities, privacy-related costs, and important aspects of its operation are explained. Participants learn that Smart-Scan enhances email communication and offers various features, such as personalized grammar and spell check, automated full-text translation, a high-quality dictionary, and thesaurus functions. However, it needs access to the user's email correspondence to learn about their writing style. Users only need to write a prompt for Smart-Scan to quickly and conveniently formulate error-free, professional, yet authentic text in any language (the complete experiment is documented in Appendix A).

Embedded in the survey instructions are experimental manipulations following a 2 (opt-in vs. opt-out of usage) x 2 (more vs. less salient privacy costs) x 3 (jurisdiction in which user data is stored) between-subject factorial design. *Default* varies whether Smart-Scan needs to be activated by the user by explicitly opting in, or whether it is automatically activated. In either case, Smart-Scan can be deactivated anytime. *Salience* varies whether subjects are given more detailed information on the privacy risk entailed in using Smart-Scan. Specifically, such risk is described as deriving from sharing personal data as well as data of contacts with whom participants exchange emails. Finally, *regulatory regime* varies the location of the servers on which the data is stored (EU, US, or Hong Kong) and thus the level of de facto legal privacy protection. The EU and the US are chosen because of their influential and yet very different data protection frameworks. The EU's GDPR offers a higher standard of data protection (Frankenreiter, 2022), whereas the US provides legal protection only via state and local regulation. Therefore, the US regulatory framework provides law enforcement agencies with easier access to private data, and firms are less burdened with

costly mandatory data protection measures. The EU and the US still represent cases from different poles of the Western democratic spectrum of data regulation. Outside of Western democracies, many regimes are characterized by political control over data that far exceeds that in the EU or the US (Guriev and Treisman, 2022). Hong Kong is selected here as the third server location because it is a jurisdiction that digital services providers may have realistically chosen, as it historically enjoyed a high degree of political autonomy, allowing it to provide a relatively generous data protection regime. At the same time, Hong Kong's government retains extensive powers to access citizens' and organizations' data.[5] Therefore, Hong Kong offers the weakest protection of data privacy among the three server locations in our experiment.

After having presented the survey instructions, we ask participants a series of questions that are identical across treatment conditions. One of these questions asks whether they would adopt Smart-Scan, and the answer to this question (yes/no) serves as our main dependent variable. Further questions concern participants' attitudes, preferences, and demographic characteristics. First, we use two survey items from the preference survey module developed and validated by Falk et al. (2018, 2023) to elicit participants' risk preferences and generalized trust. Second, we measure their concerns regarding the use of algorithms in general based on two questions introduced by Horowitz and Kahn (2021). Specifically, we ask how participants judge the relative importance of data collection versus the protection of privacy in governments' use of algorithms, as well as how concerned participants are about bias in algorithms. Third, we elicit privacy concerns using the questions from the well-established Internet Privacy Concerns (IPC) scale (Hong and Thong, 2013), which consists of six sub-scales, each calculated from three questions: Collection, Secondary usage, Errors, Improper access, Control, and Awareness. Finally, participants are asked to provide their age, gender, ethnic background, country of residence, and level of education.

3.2 Implementation

The survey experiment was run in April 2024. It was programmed in *Qualtrics* and participants were recruited via *Prolific*.[6] To ensure the participation of experienced Prolific users, we required that participants had previously completed at least ten tasks on the platform. Participants were paid a flat fee of £1.5 (approximately $1.9). On average, they earned a wage equivalent to £9.5 per hour (plus a possible bonus payment), which exceeds the hourly wage of £9 recommended by Prolific for high-quality data.

To test whether respondents carefully read the basic instructions, participants were only allowed to continue with the study after passing a comprehension check, which was shown just before the instruction screens including the treatments. Out of a list of four statements, participants had to select those that were consistent with the instructions. If their answers were not

[5] Since Hong Kong has introduced a new national security law, law enforcement agencies can search electronic devices and online speech without a warrant. National security authorities can compel the deletion of data. Public authorities can legally access corporate information without the firms' knowledge (see Wright, 2023, for an assessment of data protection in Hong Kong).

[6] Subjects recruited via Prolific have been repeatedly shown to provide better quality data than, e.g., MTurk workers (Albert and Smilek, 2023; Douglas, Ewell, and Brauer, 2023; Peer et al., 2017, 2021).

correct, participants had to re-read the instructions and answer the comprehension check again until they passed.[7] Finally, to ensure that participants answered the questions carefully, we included three attention checks. In line with Prolific's regulations, the 16 participants who failed more than one attention check were excluded from the survey, and all other participants were paid.

4 Empirical analysis

This section contains the empirical analysis. Section 4.1 explains the key variables, while the main results are presented in Section 4.2. Finally, Section 4.3 reports robustness tests and additional results.

4.1 Variables

Our treatment indicators are based on the version of the instructions survey participants were randomly exposed to. The treatment indicator for Default indicates whether respondents were asked to opt-in (1) or opt-out (0) of using Smart-Scan. Salience is represented by a binary indicator that takes the value 1 if additional information was provided on the potential privacy costs of using Smart-Scan, and 0 otherwise. The Regulatory regime is captured by two binary variables indicating whether the personal data collected by Smart-Scan is stored on servers in the United States or the European Union, with Hong Kong being the reference category. Building on this information, we create an additional indicator to capture heterogeneous treatment effects. This binary indicator takes the value 1 either if the participant lives in the US and the data is stored on servers in the US or if the participant lives in continental Europe (including Switzerland) and the data is stored on servers in the EU. We call this indicator Home bias, as it captures whether European and US residents have a systematically different evaluation than others of the desirability of data storage in their home jurisdiction.

To determine the latent factors underlying respondents' answers to the 18 questions that make up Hong and Thong's (2013) IPC scale, we conduct an exploratory factor analysis, as detailed in Appendix B. The resulting scree plot in Figure B.1 identifies only three factors, rather than six as in the IPC scale. The first factor represents concerns regarding the protection of personal data, and subsumes four IPC-sub-scales (Collection, Improper access, Control, and Awareness). The second factor corresponds to the sub-scale Secondary usage and describes respondents' trust in the good privacy practices of organizations entrusted with personal data. The third factor corresponds to the sub-scale Errors, which reflects an expectation that organizations should invest in the quality of the personal data in their databases. We expect that the privacy concerns captured in factor 1 discourage the adoption of Smart-Scan, whereas the trust in organizations holding personal data and the concern about the quality of that data expressed in factors 2 and 3 seem to favor

[7] 69% of participants passed at the first attempt, 92% cumulatively by the second, 97% by the third, and 99% had passed by the fourth attempt.

the adoption of an AI-based app. In the empirical analysis, we use all three factors to represent privacy attitudes, although only the first factor is suitable for testing Hypothesis 5.

Table 1: Descriptive statistics

	Full sample				Europe	US	Non-users	Users
	Mean	SD	Min	Max	Mean	Mean	Mean	Mean
Would you use the app?	0.35	0.48	0	1	0.35	0.34	0.00	1.00
Opt-in needed (treat)	0.50	0.50	0	1	0.49	0.50	0.50	0.48
Privacy risk salient (treat)	0.50	0.50	0	1	0.49	0.51	0.52	0.48
US server location (treat)	0.33	0.47	0	1	0.34	0.32	0.32	0.34
EU server location (treat)	0.32	0.47	0	1	0.32	0.33	0.30	0.37
Home bias	0.32	0.47	0	1	0.32	0.32	0.29	0.38
IPC: Collection	5.73	1.07	1	7	5.69	5.76	5.96	5.29
IPC: Secondary usage	2.67	1.66	1	7	2.54	2.79	2.41	3.14
IPC: Control	4.84	1.35	1	7	4.51	5.15	4.70	5.10
IPC: Errors	6.47	0.81	1	7	6.46	6.48	6.61	6.22
IPC: Improper access	5.80	0.92	2.3	7	5.71	5.88	5.93	5.55
IPC: Awareness	6.25	0.80	2.7	7	6.17	6.32	6.38	6.00
Willingness to take risks	4.81	2.39	0	10	5.04	4.60	4.47	5.47
Generalized trust level	4.91	2.49	0	10	4.85	4.96	4.68	5.32
Gov use of AI	3.87	1.02	1	5	3.81	3.93	4.08	3.48
Concern about AI	3.23	1.03	1	5	3.19	3.27	3.41	2.89
Gender: Female	0.40	0.49	0	1	0.36	0.45	0.42	0.38
Gender: Other or n/a	0.03	0.17	0	1	0.03	0.03	0.04	0.01
25-34 years old	0.39	0.49	0	1	0.47	0.31	0.39	0.38
35-44 years old	0.22	0.41	0	1	0.18	0.25	0.23	0.19
45-54 years old	0.12	0.32	0	1	0.06	0.18	0.12	0.11
55-64 years old	0.06	0.25	0	1	0.02	0.11	0.07	0.05
65+ years old	0.04	0.20	0	1	0.01	0.07	0.04	0.03
US sample	0.51	0.50	0	1	0.00	1.00	0.52	0.51

Number of observations in…Full sample: $N = 1,734$, Europe: $N = 844$, US: $N = 890$, Non-users: $N = 1,129$, Users: $N = 605$. The table shows mean values of the six IPC dimensions instead of the factor scores (which by construction have a mean of 0 and a standard deviation of 1 and are thus not suitable for comparison between our sample and other subjects).

4.2 Results

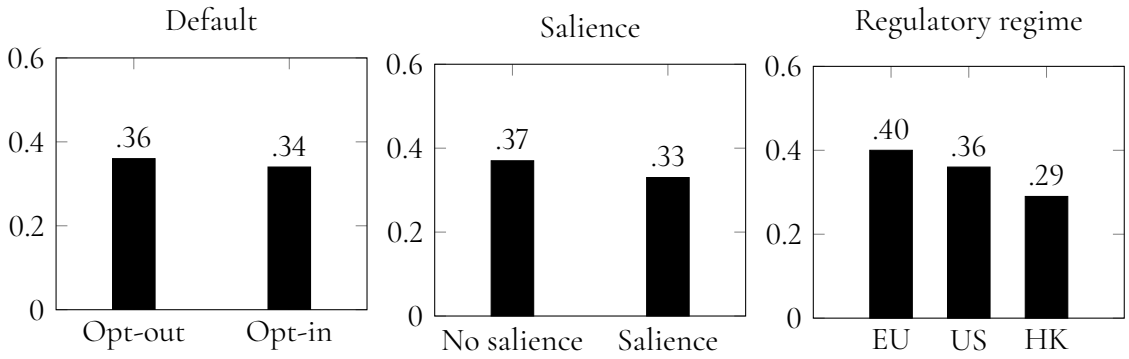
Our analysis relies on data from those 1,734 participants who passed all attention checks.[8] Table 1 shows the descriptive statistics for this sample. About 35% of participants, both in the US and Europe, indicate that they would use Smart-Scan. The distribution of treatments is consistent with a random assignment of conditions with equal probabilities. 51% of the participants are US residents and the other 49% come from seven continental European countries.[9] 32% of participants have the possibility to exhibit a home bias, because they are US (European) residents and they are informed that the servers would be located in the US (the EU). 40% of participants are female (45% in the US) and 56% of participants are between 18 and 34 years old. This age distribution is typical for online experiments and still closer to the age distribution in the general population than that of typical university labs' subject pools.

[8] In total, we collected 2,068 participants' responses in the experiment (1,035 from the US and 1,033 from Europe).

[9] Germany (32%), France (5%), Netherlands (5%), Austria (3%), Switzerland (2%), Belgium (1%), and Luxembourg (0.1%).

Figure 1 presents first descriptive evidence for treatment effects. In line with our predictions, participants who have to opt-in to use the app (Hypothesis 1) or who are provided with more information about its privacy risks (Hypothesis 2) are less willing to adopt the app. Also the regulatory regime regarding data privacy (Hypothesis 3) shows the expected association with technology adoption: A server location in the US or the EU, respectively, is associated with a 7 or 11 percentage points higher willingness to adopt than if the server was in Hong Kong.

Figure 1: Share of participants willing to adopt the app by treatment conditions



In a next step, we use regression analysis to formally test our hypotheses. Table 2 shows our main results. The average marginal effects are calculated based on Probit estimates with robust standard errors in parentheses. The binary dependent variable indicates whether a participant is willing to use Smart-Scan. The model underlying Column 1 includes the four experimental treatments and a dummy variable for whether a participant is a US resident. In Column 2, we account for a possible home bias by allowing the server-location treatment effect to vary depending on whether it coincides with the participant's home jurisdiction (which we assume is the EU for continental Europeans). In Column 3, we add controls for participants' age and gender. Column 4 includes the three factor variables introduced above (f1, f2, and f3), as well as the other attitudes and preferences expected to be relevant for participants' willingness to use the app.

Consistent with the descriptive results depicted in Figure 1, we find negative estimates for the opt-in treatment (Hypothesis 1) and the salient privacy cost treatment (Hypothesis 2), but neither effect is statistically significant. We do find support for Hypothesis 3, as a server location in Hong Kong is associated with a reduced willingness to use the app. However, the difference between servers in Hong Kong and the US is no longer statistically significant once we account for a potential home bias. The probability that a participant wants to use Smart-Scan is 8 to 11 percentage points higher if the data is stored in the EU rather than in Hong Kong. The home bias effect itself is statistically significant at the 5% or 10% level, depending on the model specification, and indicates that a server being located in one's home jurisdiction increases the willingness to use the app by 4 to 6 percentage points. This effect is estimated under the assumption that there is one homogeneous home bias.

In a more detailed analysis, we allow the home biases of US residents and Europeans to differ. The results, based on a sample split between European and US residents, are visualized in the

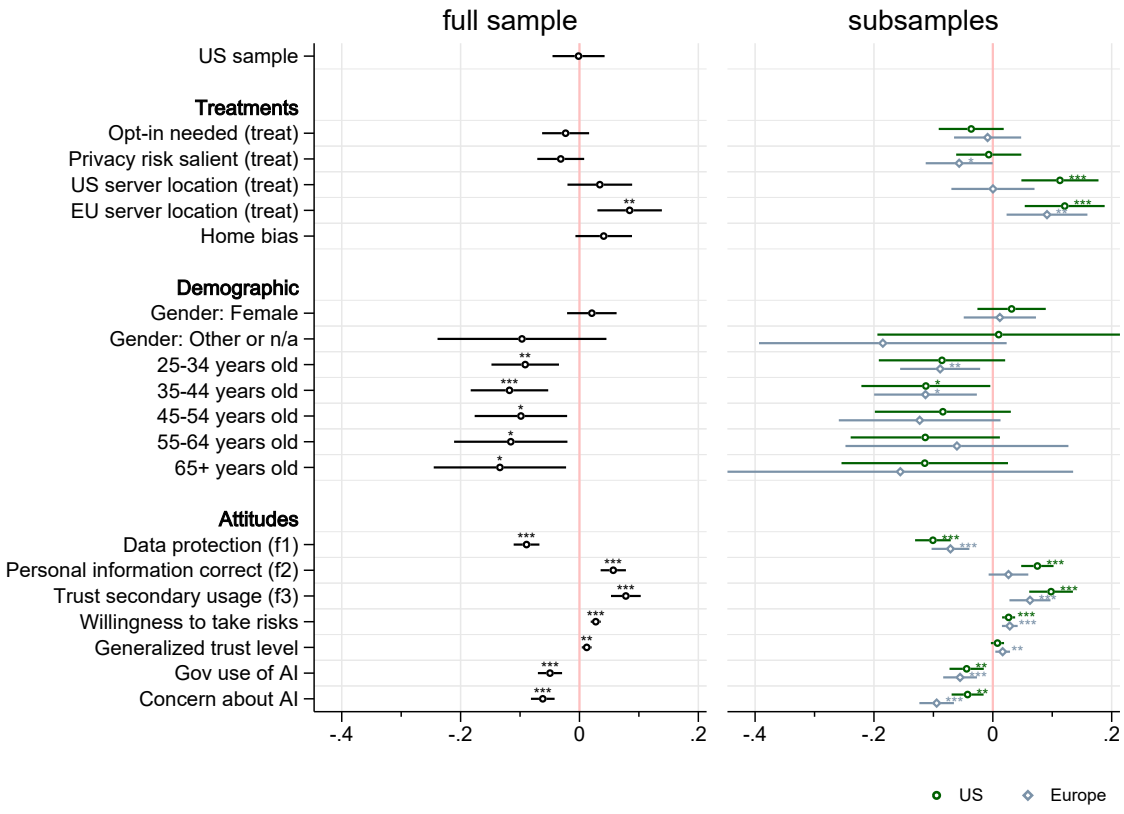
Table 2: Willingness to use the app

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	-0.018	-0.018	-0.019	-0.023
	(0.023)	(0.023)	(0.022)	(0.020)
Privacy risk salient (treat)	-0.033	-0.035	-0.031	-0.032
	(0.023)	(0.023)	(0.022)	(0.020)
US server location (treat)	0.073**	0.041	0.039	0.034
	(0.028)	(0.031)	(0.031)	(0.028)
EU server location (treat)	0.113***	0.082**	0.083**	0.084**
	(0.028)	(0.031)	(0.030)	(0.028)
Home bias		0.063*	0.063*	$0.041^{(+)}$
		(0.028)	(0.027)	(0.024)
Data protection (f1)				-0.089***
				(0.011)
Personal information correct (f2)				0.057***
				(0.011)
Trust secondary usage (f3)				0.078***
				(0.013)
Willingness to take risks				0.027***
				(0.004)
Generalized trust level				0.012**
				(0.004)
Gov use of AI				-0.050***
				(0.010)
Concern about AI				-0.062***
				(0.010)
Age and gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,734	1,734	1,734
Nagelkerke R-sq.	0.016	0.020	0.055	0.300

Notes: Average marginal effects based on Probit models with robust SE in parentheses. Binary dependent variable: Would you use the app? (yes/no). $^{(+)}$: $p < 0.10$, * : $p < 0.05$, ** : $p < 0.01$, *** : $p < 0.001$.

right panel of Figure 2.[10] While we find no home bias of European participants, as European and US participants agree on how to rate EU servers relative to Hong Kong servers, US residents do exhibit a home bias in the sense that Europeans do not share Americans' preference for US servers over Hong Kong servers. Hence, our results partially support Hypothesis 4 (i.e., for participants from the US, but not for European residents).

Figure 2: Willingness to use the app



Notes: Plots display coefficient estimates with corresponding 95%-confidence intervals. Left panel: results are based on the full sample and correspond to those shown in Column 4 of Table 2. The US sample dummy identifies differences between European and US participants after accounting for treatments and participant characteristics. Right panel: results are produced separately for the subsamples of US and European participants. They correspond to the regressions shown in Columns 2 and 3 of Table D.7. $^{(+)}: p < 0.10, ^{*}: p < 0.05, ^{**}: p < 0.01, ^{***}: p < 0.001$.

Column 4 of Table 2 shows that participants' attitudes and preferences are powerful predictors of their propensity to use Smart-Scan, as theoretically expected (see also the left panel of Figure 2). The three factors derived from the IPC scale indicate that participants who prefer strong data protection, who do not trust websites regarding the secondary use of data, or who do not prefer websites to maintain correct personal data are less willing to use the app. Subjects who want governments to prioritize privacy concerns over generating more information when using algorithms are also less likely to use Smart-Scan. These results are consistent with Hypothesis 5. Participants' willingness to use the app is also affected by general economic attitudes. A higher

[10] The corresponding regression results are shown in Columns 2 and 3 of Table D.7 in the Online Appendix. The interaction model in Columns 4 tests whether effects differ between the two subsamples.

willingness to take risks (Hypothesis 6) and a higher level of trust (Hypothesis 7) are both positively related to the adoption of Smart-Scan. Finally, participants who are generally concerned about AI are less interested in using Smart-Scan (Hypothesis 8). Table 3 summarizes our results for all eight Hypotheses.

Table 3: Summary of hypothesis tests

Hypothesis	**Willingness to adopt Smart-Scan is higher, when …**	**Finding**
H1 (Default)	it is activated by default	✗
H2 (Salience)	more information about data privacy risks is provided	✗
H3 (Regulatory regime)	data is better protected by law	✓
H4 (Home bias)	data is stored in individuals' home jurisdiction	✓
H5 (Privacy concerns)	individuals are less concerned about data privacy	✓
H6 (Risk aversion)	individuals exhibit low risk aversion	✓
H7 (Trust)	individuals exhibit high trust	✓
H8 (AI skepticism)	individuals are less concerned about AI-based algorithms	✓

Notes: For each hypothesis (row), the last column indicates whether the hypothesis is empirically supported ("✓") or not supported ("✗").

4.3 Robustness tests and extensions

In this section, we report our findings from various robustness tests and extended analyses (see Appendix D for details).

In a first robustness test, we repeat the main regression analysis in Table 2 using two alternative dependent variables measuring (i) how convinced participants are of Smart-Scan (5-point Likert scale) and (ii) how many other participants they expect to adopt it (five intervals: <20%, 20%–39%, …). The latter question is incentivized, as five randomly selected participants who chose the correct interval received a bonus payment of £40 (about US$50). As can be seen from Tables D.1 and D.2, the results are very similar to the main analysis. The only difference is that participants expect others to have a strong preference for servers being located in the US or the EU. Respondents have no significant preference for an EU server location over servers located in the US, and they exhibit no home bias regarding others' expected willingness to use Smart-Scan. This difference in results may be due to the fact that we have not informed participants where the other participants (whose decision they are asked to anticipate) are from. The fact that the results from the incentivized question are otherwise comparable to our non-incentivized questions lends additional support to our research design.

In a second set of robustness tests, we estimate linear probability models (OLS) instead of probit models for our main model specification as well as the two models using alternative dependent variables. We find virtually identical results (see Tables D.3 to D.5).

As a third robustness test, we repeat the main regression analysis as in Column (4) of Table 2, while varying how well participants had to have performed in the comprehension check for them to be included in the regression sample. Recall that participants were not excluded for failing the comprehension check even repeatedly, but they had to reread the instructions and answer the same comprehension check question again until they passed it. As shown in Column 4 of Table D.6,

there are two differences compared to our findings in the main analysis: First, the salience of the privacy costs of using Smart-Scan now reduces participants' willingness to use the app. Second, participants now also prefer US server location over data storage in Hong Kong. All other results remain qualitatively unchanged.

As an extension, we investigate whether the results presented in Table 2 differ between participants from Europe and the US. The results are shown in Column 5 of Table D.7. Apart from the difference in home bias already discussed in Section 4.2, we find only two other differences. US participants who are concerned about the quality of personal information stored by businesses are more likely to use Smart-Scan than other participants from the US, but the same does not apply to Europeans. Moreover, the negative effect of concerns about AI on the willingness to use Smart-Scan is twice as pronounced among participants from Europe as compared to those from the US.

Finally, we have implemented a second salience treatment in which randomly selected participants receive (together with their randomly assigned server location) additional information about what characterizes data protection in the respective jurisdiction.[11] For EU servers, high data protection standards are emphasized by the information treatment, for servers in the US and Hong Kong, it is pointed out that data can under certain circumstances be accessed by third parties in the interest of public safety. The results of this extension are shown in Table D.8. The regressions include a binary variable for whether the participant was treated, and this dummy variable is also interacted with the variables for US and EU sever location. As can be seen, the coefficients for location salience and the two interaction terms between location salience and location are not significantly different from zero, indicating that participants do not react to the additional information (irrespective of the server location and the dependent variable). This may indicate that they were already well aware of the levels of data protection in the three jurisdictions. That would be in line with our interpretation of the location treatments as reflecting to a large extent differences in perceived data protection, as opposed to any other relevant differences between storing data in these jurisdictions.

5 Discussion

The results of our experiment have several implications and can inform both policymakers and companies in the area of (international) data privacy regulation.

First, default settings and salience were not significant factors in our experiment. This is in line with some previous findings in the literature on data privacy risks. For example, Hermstrüwer and Dickert (2017) found no effect of the default design in the context of the right to be forgotten, specifically regarding deletion requests for personal data. Moreover, Buckman, Bockstedt, and Hashim (2019) found that privacy valuation is not significantly affected by a more salient explanation of privacy risks. The difficulty of communicating privacy risks when AI is concerned makes manipulation of salience a less effective strategy. However, we cannot rule out that our

[11] This treatment has been pre-registered, but it is omitted from the main models for the sake of conciseness.

experimental manipulations were too subtle. Hence, it would be premature to conclude that defaults and salience do not matter for consumer choices in our context. Of course, they do matter from a regulatory compliance perspective. For example, existing regulation in Europe already has requirements regarding privacy by design and by default (e.g., Art. 25 GDPR). More recent European legislation continues this trend, for instance with the Data Act pursuing a strategy of 'accessibility (of data) by design.' The European AI Act also stipulates that individuals affected by the decision of certain high risk AI systems have a right to 'clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken' (Art. 86). Therefore, the EU-US Data Privacy Framework, which regulates data exchanges across the Atlantic, effectively requires US providers of commercial AI-based services who wish to maintain their customer base in the EU to prioritize transparency.

Second, from a managerial perspective, server location matters. While participants in general see no difference between locations in the US and Hong Kong, they prefer server locations in the EU over the other two countries. This seems to indicate that the stronger data protection afforded by the GDPR and related legislation assuages concerns about sharing data with a data-intensive application like Smart-Scan. Therefore, there may be good reasons for locating servers in the EU, and maintaining data centers there might be a profitable enterprise in spite of higher costs. Alternatively, organizations that decide to keep their servers in their home location may have to implement data protection solutions that are similar to those required by GDPR if they want to convince privacy-concerned customers to adopt their AI-based products. Company strategies like that of Microsoft to announce[12] that they would increase the data protection requirements to all customers worldwide may indeed make economic sense (Voss and Houser, 2019). They call this business strategy one of "advantage," reducing regulatory compliance costs by having a harmonized strategy for all customers, based on the expectation that other countries would eventually follow suit to the standards of the GDPR anyway. Indeed, Davis and Marotta-Wurgler (2024) provide empirical support for such a regulatory spillover from the EU to the US. As another strategy, namely "transformation," US companies can leverage their compliance with the GDPR to change and improve their corporate culture and reputation, leading to greater trust among consumers—something that has recently been eroded by incidents such as the Cambridge Analytica scandal (Brown, 2020).

Third, our study shows the impact of personal characteristics on adoption decisions. Smart or AI-enhanced products have some inherent data privacy risks, and consumers' willingness to adopt such products depends, among other factors, on privacy concerns, risk preferences, trust, and general attitudes towards AI algorithms. We find that such factors indeed play an important role in the adoption decision. This suggests that superior functionality of a new product alone may not be enough to penetrate a market, if consumers can choose between novel and incumbent products. For example, in the context of autonomous vehicles (AVs), there is robust survey evidence that data privacy, the fear of data misuse, and trust in the product are important factors for consumers'

[12] https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/

willingness to pay for such products (Kyriakidis, Happee, and de Winter, 2015; Shabanpour et al., 2018; Cunningham et al., 2019).[13] Importantly, the willingness to adopt a new AI technology is affected by individual attitudes, which cannot easily be changed through policy. This might make it even more important to create clear and transparent data governance structures, clarifying user rights and provider responsibilities to users, since these factors appear to be crucial for adoption. It remains to be seen if EU legislation on data protection around AI will successfully counter citizens' concerns about AI products without stifling companies' innovativeness and competitiveness.

6 Limitations and directions for future work

This study investigates the willingness to adopt AI-based products by introducing survey participants to a hypothetical enhancement of their preferred email-app. Such vignette studies are commonly used for testing theories of technology adoption, but they cannot measure actual adoption. Future research may attempt to measure actual adoption by implementing a field experiment, perhaps in collaboration with a provider of an AI-enhanced product or service.

Furthermore, it is possible that the findings of this study generalize to any kind of data-intensive technology, not necessarily AI-based. However, the focus of this work is specifically on AI-enhanced products. The motivation for this choice is twofold. First, AI products constitute one of the most rapidly evolving types of technology, with high potential for – yet limited evidence of – widespread adoption. Secondly, privacy-functionality trade-offs are particularly interesting in the context of AI products. Fair information management, which can be beneficial for both consumers and companies (Lee, Ahn, and Bang, 2011), and privacy-enhancing technologies (Acquisti, Taylor, and Wagman, 2016) can partially resolve the trade-off between privacy and functionality when it comes to most technological products. For instance, if one wants to use social media but is concerned about platforms exploiting one's data, one can choose a decentralized privacy-preserving competitor; if one wants to search, browse, and shop online but does not want one's search, browse, or purchase history to feed targeted advertising, privacy-preserving search engines and browsers may offer a solution. For many transactions involving information technology, there are solutions for the privacy-concerned customer to enjoy the technology's benefits without giving up too much of their privacy. In contrast, resolving the convenience-privacy trade-off becomes more difficult when it comes to AI, as typical AI commercial applications can only function if they are fed vast amounts of data. To understand how individuals deal with this trade-off, it is crucial to identify the factors that determine user acceptance. Existing work has analyzed the impact of privacy concerns on adoption of other types of data-intensive technology, such as product or service personalization (Chellappa and Sin, 2005), but more work is needed in order to extend the present results to all new and emerging technologies.

Finally, we acknowledge the possibility that our experimental manipulation of the server location may effectively constitute a manipulation of more than just the data protection regime.

[13] Dawid and Muehlheusser (2022), Dawid et al. (2024), and Feess and Muehlheusser (2024) use game-theoretic models to study how the safety of a novel smart product (AV) and the regulatory framework affect consumers' adoption decisions, and hence the market penetration of such products.

Indeed, from a managerial perspective, data protection regulation is only one of many factors that an organization must take into account when deciding where to locate their servers. Considerations of climate, purely economic costs, workforce availability, etc. play a considerable role. However, from a user perspective, which is the one taken here, the regulatory regime is arguably one of the most (if not the only) relevant factor affecting the willingness to adopt a free AI-based app: accessibility or other information safety concerns may vary with the specific provider but, keeping the provider constant, those concerns also stay constant. Future work might explore the effect of trust/loyalty towards specific providers on the adoption of AI-based and similar products.

7 Conclusion

AI has tremendous potential to increase the quality of products and services, making users more satisfied, more productive, and more efficient. However, AI also presents new privacy risks due to the amount of data—both personal and organizational—it requires to deliver such benefits. In this paper, we present the results of a randomized survey experiment, with participants from the US and Europe, investigating whether privacy-relevant factors affect the willingness to adopt an AI-enhanced email app.

Interestingly, we find that while default settings (opt-in vs. opt-out) and salience (explicit, transparent information on the type of data shared with the system) do not show significant effects, the regulatory framework governing data protection is an important factor in adoption decisions. When it comes to the server location, strict data protection regulation, such as the European GDPR positively affects participants' willingness to adopt the technology compared to less stringent regulatory frameworks such as those in force in the US or Hong Kong.

Our findings suggest that high data protection constitutes a potential strategic advantage for organizations, which may therefore decide to locate their servers in the EU. From a policy perspective, they also indicate that strict regulation in the EU may have de facto spillovers into other regions, with non EU-based organizations adopting tighter standards of protection for their customers worldwide.

References

Acemoglu, Daron. 2024. "Harms of AI." In *The Oxford Handbook of AI Governance*. Oxford University Press, 660–706.

Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper et al. 2017. "Nudges for privacy and security: Understanding and assisting users' choices online." *ACM Computing Surveys (CSUR)* 50 (3):1–41.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2020. "Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age." *Journal of Consumer Psychology* 30 (4):736–758.

Acquisti, Alessandro and Jens Grossklags. 2007. "What can behavioral economics teach us about privacy?" In *Digital Privacy*. Auerbach Publications, 363–378.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The economics of privacy." *Journal of Economic Literature* 54 (2):442–492.

Albert, Derek A and Daniel Smilek. 2023. "Comparing attentional disengagement between Prolific and MTurk samples." *Scientific Reports* 13 (1):20574.

Alkhatib, Sami, Jenny Waycott, George Buchanan, Marthie Grobler, and Shuo Wang. 2020. "Privacy by design in aged care monitoring devices? Well, not quite yet!" In *Proceedings of the 32nd Australian Conference on Human-Computer Interaction*. 492–505.

Anaraky, Reza Ghaiumy, Tahereh Nabizadeh, Bart P Knijnenburg, and Marten Risius. 2018. "Reducing default and framing effects in privacy decision-making." In *Proceedings of the Seventeenth Annual Pre-ICIS Workshop on HCI Research in MIS*. 1–6.

Beshears, John, James J. Choi, David Laibson, and Brigitte C. Madrian. 2009. "The importance of default options for retirement saving outcomes: Evidence from the United States." In *Social Security Policy in a Changing Environment*, edited by Jeffrey R. Brown, Jeffrey B. Liebman, and David A. Wise. Chicago: University of Chicago Press, 167–198.

Brown, Allison J. 2020. ""Should I stay or should I leave?": Exploring (dis) continued Facebook use after the Cambridge Analytica scandal." *Social Media + Society* 6 (1):1–8.

Buckman, Joseph R, Jesse C Bockstedt, and Matthew J Hashim. 2019. "Relative privacy valuations under varying disclosure characteristics." *Information Systems Research* 30 (2):375–388.

Chau, Patrick Y K. 1996. "An empirical assessment of a modified technology acceptance model." *Journal of Management Information Systems* 13 (2):185–204.

Chellappa, Ramnath K and Raymond G Sin. 2005. "Personalization versus privacy: An empirical examination of the online consumer's dilemma." *Information Technology and Management* 6:181–202.

Cunningham, Mitchell, Michael Regan, Timothy Horberry, Kamal Weeratunga, and Vinayak Dixit. 2019. "Public opinion about automated vehicles in Australia: Results from a large-scale national survey." *Transportation Research Part A: Policy and Practice* 129:1–18.

Davis, Fred D, R P Bagozzi, and P R Warshaw. 1989. "Technology acceptance model." *Journal of Management Science* 35 (8):982–1003.

Davis, Kevin E and Florencia Marotta-Wurgler. 2024. "Filling the void: How EU privacy law spills over to the US." *Journal of Law and Empirical Analysis* 1 (1):1–21.

Dawid, Herbert, Xuan Di, Peter M Kort, and Gerd Muehlheusser. 2024. "Autonomous vehicles policy and safety investment: An equilibrium analysis with endogenous demand." *Transportation Research Part B: Methodological* 182:102908.

Dawid, Herbert and Gerd Muehlheusser. 2022. "Smart products: Liability, investments in product safety, and the timing of market introduction." *Journal of Economic Dynamics and Control* 134:104288.

Dhagarra, Devendra, Mohit Goswami, and Gopal Kumar. 2020. "Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective." *International Journal of Medical Informatics* 141:104164.

Dinev, Tamara, Allen R McConnell, and H Jeff Smith. 2015. "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box." *Information Systems Research* 26 (4):639–655.

Douglas, Benjamin D, Patrick J Ewell, and Markus Brauer. 2023. "Data quality in online human-subjects research: Comparisons between MTurk, Prolific, CloudResearch, Qualtrics, and SONA." *Plos one* 18 (3):e0279720.

Enke, Benjamin. 2020. "Moral values and voting." *Journal of Political Economy* 128 (10):3679–3729.

Falk, Armin, Anke Becker, Thomas Dohmen, Benjamin Enke, David Huffman, and Uwe Sunde. 2018. "Global evidence on economic preferences." *The Quarterly Journal of Economics* 133 (4):1645–1692.

Falk, Armin, Anke Becker, Thomas Dohmen, David Huffman, and Uwe Sunde. 2023. "The preference survey module: A validated instrument for measuring risk, time, and social preferences." *Management Science* 69 (4):1935–1950.

Featherman, Mauricio S and Paul A Pavlou. 2003. "Predicting e-services adoption: A perceived risk facets perspective." *International Journal of Human-Computer Studies* 59 (4):451–474.

Feess, Eberhard and Gerd Muehlheusser. 2024. "Autonomous vehicles: Moral dilemmas and adoption incentives." *Transportation Research Part B: Methodological* 181:102894.

Frankenreiter, Jens. 2022. "Cost-based California effects." *Yale Journal on Regulation* 39 (3):1155–1217.

Gaar, Eduard, David Scherer, and Dirk Schiereck. 2020. "The home bias and the local bias: A survey." *Management Review Quarterly* 72:1–57.

Godinho de Matos, Miguel and Idris Adjerid. 2022. "Consumer consent and firm targeting after GDPR: The case of a large telecom provider." *Management Science* 68 (5):3330–3378.

Graßl, Paul, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. 2021. "Dark and bright patterns in cookie consent requests." *Journal of Digital Social Research* 31 (1):1–38.

Guriev, Sergei and Daniel Treisman. 2022. *Spin Dictators: The Changing Face of Tyranny in the 21st Century*. Princeton University Press.

Hermstrüwer, Yoan and Stephan Dickert. 2017. "Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge." *International Review of Law and Economics* 51:38–49.

Hillman, Arye L. 2010. "Expressive behavior in economics and politics." *European Journal of Political Economy* 26 (4):403–418.

Hong, Soo Jung and Hichang Cho. 2023. "Privacy management and health information sharing via contact tracing during the COVID-19 pandemic: A hypothetical study on AI-based technologies." *Health Communication* 38 (5):913–924.

Hong, Weiyin and James Y L Thong. 2013. "Internet privacy concerns: An integrated conceptualization and four empirical studies." *MIS Quarterly* 37 (1):275–298.

Horowitz, Michael C and Lauren Kahn. 2021. "What influences attitudes about artificial intelligence adoption: Evidence from U.S. local officials." *PLoS One* 16 (10):e0257732.

Jachimowicz, Jon M, Shannon Duncan, Elke U Weber, and Eric J Johnson. 2019. "When and why defaults influence decisions: A meta-analysis of default effects." *Behavioural Public Policy* 3 (2):159–186.

Johnson, Eric J and Daniel Goldstein. 2003. "Do defaults save lives?" *Science* 302 (5649):1338–1339.

Johnson, Garrett A. 2024. "Economic research on privacy regulation: Lessons from the GDPR and beyond." In *The Economics of Privacy*, edited by Avi Goldfarb and Catherine E. Tucker, chap. 4. Chicago: University of Chicago Press, 97–126.

Johnson, Garrett A, Scott K Shriver, and Samuel G Goldberg. 2023. "Privacy and market concentration: Intended and unintended consequences of the GDPR." *Management Science* 69 (10):5695–5721.

Komiak, Sherrie and Izak Benbasat. 2006. "The effects of personalization and familiarity on trust and adoption of recommendation agents." *MIS Quarterly* 30 (4):941–960.

Kyriakidis, Miltos, Riender Happee, and Joost de Winter. 2015. "Public opinion on automated driving: Results of an international questionnaire among 5000 respondents." *Transportation Research Part F: Traffic Psychology and Behaviour* 32:127–140.

Lee, Dong-Joo, Jae-Hyeon Ahn, and Youngsok Bang. 2011. "Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection." *MIS Quarterly* 35 (2):423–444.

Leon, Pedro, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. 2012. "Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising." In *Proceedings of the SIGCHI conference on human factors in computing systems*. 589–598.

Madrian, Brigitte and Dennis Shea. 2001. "The power of suggestion: Inertia in 401 (k) participation and savings behavior." *The Quarterly Journal of Economics* 116 (4):1149–1187.

Meredith, Lisa S, David P Eisenman, Hilary Rhodes, Gery Ryan, and Anna Long. 2007. "Trust influences response to public health messages during a bioterrorist event." *Journal of Health Communication* 12 (3):217–232.

Miltgen, Caroline Lancelot, Aleš Popovič, and Tiago Oliveira. 2013. "Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context." *Decision Support Systems* 56:103–114.

Peer, Eyal, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. "Beyond the Turk: Alternative platforms for crowdsourcing behavioral research." *Journal of Experimental Social Psychology* 70:153–163.

Peer, Eyal, David Rothschild, Andrew Gordon, Zak Evernden, and Ekaterina Damer. 2021. "Data quality of platforms and panels for online behavioral research." *Behavior Research Methods* 54:1–20.

Pew Research Center. 2019. "Americans and privacy: Concerned, confused and feeling lack of control over their personal information." Available online at: `www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf`, last accessed on 20.03.2025.

Shabanpour, Ramin, Nima Golshani, Ali Shamshiripour, and Abolfazl Kouros Mohammadian. 2018. "Eliciting preferences for adoption of fully automated vehicles using best-worst analysis." *Transportation Research Part C: Emerging Technologies* 93:463–478.

Thaler, Richard H and Cass R Sunstein. 2008. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.

Tsai, Janice Y, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. "The effect of online privacy information on purchasing behavior: An experimental study." *Information Systems Research* 22 (2):254–268.

Venkatesh, Viswanath, Michael G Morris, Gordon B Davis, and Fred D Davis. 2003. "User acceptance of information technology: Toward a unified view." *MIS Quarterly* 27:425–478.

Voss, W Gregory and Kimberly A Houser. 2019. "Personal data and the GDPR: Providing a competitive advantage for US companies." *American Business Law Journal* 56 (2):287–344.

Whang, Steven Euijong, Yuji Roh, Hwanjun Song, and Jae-Gil Lee. 2023. "Data collection and quality challenges in deep learning: A data-centric AI perspective." *The VLDB Journal* 32 (4):791–813.

Wright, Logan. 2023. "Fractured foundations: Assessing risks to Hong Kong's business environment." Available online at: `www.atlanticcouncil.org/in-depth-research-reports/report/fractured-foundations-assessing-risks-to-hong-kongs-business-environment`, last accessed on 20.03.2025.

Online Appendix

A Instructions

In this Appendix, we provide the instructions of our online experiment. Headings (in bold) starting with "Screen" separate the screens, but these headings are not shown to participants. We also include several clarifying comments (also not shown to participants), which begin with "Note:" and are set in italics.

Screen 1 (Welcome)

Welcome to our study! This page contains important information.

Purpose: Your answers will be used by researchers at [OMITTED] for research purposes only and you will remain completely anonymous.

Topics: Our questions concern your interest in using smart products as well as some socio-demographic characteristics.

Time and payment: This survey takes about 10 minutes of your time. You will get a fixed payment of £1.5 (about $1.9) for completing the survey and some questions allow you to earn bonus payments, which will be paid out after our data collection is completed. We intersperse some simple questions to test if you are paying attention. Note that your payment and bonus payment depend on correctly answering these questions. Details concerning the bonus are provided in the survey. Your payment is processed by Prolific.

For questions, concerns, or complaints about the study you may contact [OMITTED].

By continuing, you agree to take part in our study and that your anonymized data will be used by researchers at [OMITTED] for research purposes only.

Additional information: You can leave the study at any time. In this case, you will not get paid and your data is erased.

Do you agree to the above terms?

- Yes, I agree.
- No, I do not agree.

Based on the above description, does your payment depend on answering the attention checks correctly? *(Note: Attention check 1)*

- Yes
- No

What is your Prolific ID? – *Please note that this response should auto-fill with the correct ID. Enter your ID if this is not the case. The ID is only used to authorize your payment.*

Screen 2 (App description)

Consider that a new software add-on called **Smart-Scan** becomes available.
It works for all common email apps and on all devices on which you use email (e.g., computer, tablet, and mobile phone).

What are the benefits of Smart-Scan?

Smart-Scan offers a variety of novel features, such as personalized grammar and spell check, automatic full-text translation, a high-quality dictionary, and thesaurus functions. Smart-Scan is based on an AI algorithm that improves the quality of your writing. It is able to quickly and conveniently formulate error-free, professional, yet authentic texts.

Smart-Scan will continuously improve its understanding of good writing, and it will learn from your e-mail correspondence about your personal writing style.
Moreover, Smart-Scan supports many common languages and hence can also assist you with any correspondence you might have in a foreign language (e.g., during a stay abroad).

How much does it cost?

In contrast to pricey commercial products with comparable functions, Smart-Scan is free of charge.

Screen 3 (App description)

How does Smart-Scan work?

Smart-Scan is based on a powerful AI algorithm that has been trained with a large number of anonymized documents (e.g., incoming and outgoing emails, attachments, and other documents) written by millions of users around the globe. This allows Smart-Scan to formulate natural text, detect and correct common spelling errors, as well as grammar and translation issues.

For example, suppose you want to write an email message to your landlord asking for a personal meeting to discuss an issue concerning your lease.

1. You input some text as a prompt. 2. Then, Smart-Scan will propose a message draft which you can modify as you please. 3. Before sending the message, Smart-Scan will check its spelling and give stylistic recommendations.

Prompt:

write a letter to my landlord to schedule a personal meeting

Output:

Dear [Landlord],

I hope this email finds you well. I am writing to request a personal meeting with you to discuss an issue concerning my lease. I would like to schedule a meeting at your earliest convenience, either in person or via phone/video call. Please let me know a few dates and times that work for you, and I will do my best to accommodate your schedule.

I appreciate your consideration and look forward to discussing this matter with you.

Sincerely,

[Your Name]

Screen 4 (comprehension)

Which of the following characteristics describe Smart-Scan? (Choose all answers that are correct.)

(Note: Comprehension check. If a subject gave an incorrect answer, they were transferred back to Screen 2. The order of the answers was randomized in each round.)

- Smart-Scan costs the same as a cup of coffee per year. *(Note: false)*
- Smart-Scan does not access any of your data. *(Note: false)*
- Smart-Scan is free of charge. *(Note: correct)*
- Smart-Scan will improve by analyzing your e-mail correspondence. *(Note: correct)*

Screen 5 (Treatments)

(Note: Screens 5 and 6 include information treatments, as indicated below. These were randomly chosen, i.e., with a probability of 33% or 50%, depending on the number of variants.)

How can I get Smart-Scan?

Smart-Scan is available with the next update of your email app.

You need to activate it before you can use it. *(Note: Only shown in opt-in treatment.)* It is automatically activated and ready to use. *(Note: Only shown in opt-out treatment.)*

You can deactivate it at any time.

However, once shared with Smart-Scan, your shared data cannot be retracted.

Screen 6 (Treatments)

Which data is shared?

In order to function properly, Smart-Scan requires access to your email correspondence. It will process both your data and the data of the people you correspond with.

This includes their names, (email) addresses, personal information, and the content of documents you exchange with each other. *(Note: Only shown in salient treatment.)*

Where is my data stored?

Your data will be stored on servers located in … [1] US-location-treatment: "the United States" (US) ; [2] EU-location-treatment: "the European Union" (EU) ; [3] HK-location-treatment: "Hong Kong". It is protected in compliance with current data protection legislation.

(Note: The following "location-salience" treatment is added with 50% probability and matches the location allocated in the location treatment.)

Public safety is high on the agenda of US lawmakers and servers can be accessed by third parties in certain circumstances. *(Note: Only shown in location-salient treatment and if location treatment is US.)*

Data protection is high on the agenda of EU lawmakers and servers can be accessed by third parties only in exceptional circumstances. *(Note: Only shown in location-salient treatment and if location treatment is EU.)*

Public safety is high on the agenda of Hong Kong lawmakers and servers can be accessed by third parties in certain circumstances. *(Note: Only shown in location-salient treatment and if location treatment is HK.)*

Screen 7 (Decisions / evaluations)

In light of its costs and benefits, how convincing do you find Smart-Scan?

- Not at all convincing
- Somewhat convincing
- Convincing
- Very convincing
- Extremely convincing

Given what you know about Smart-Scan, would you … **opt-in treament: "activate it?" ; opt-out treatment: "keep it activated?"**

- Yes
- No

Screen 8 (Decisions / evaluations)

Why do you not want to use Smart-Scan? Choose all options that apply. *(Note: Shown only to subjects who answered the previous question with "No".)*

- I already have a comparable program
- I have no need for such a program
- I have privacy concerns

What do you think: How many other survey participants would … opt-in treament: "activate Smart-Scan?" ; opt-out treatment: "keep Smart-Scan activated?"

Five randomly selected participants who chose the correct interval will receive a bonus payment of £40 (about $50).

- Less than 20%
- 20% to 39%
- 40% to 59%
- 60% to 79%
- 80% or more

Screen 9 (Decisions / evaluations)

Suppose that Smart-Scan is not yet available, but there is a crowdfunding campaign to finance its development. How much would you be willing to contribute (in $)?

How much do you think other participants of our survey would contribute (in $)?

Screen 10 (Economic attitudes)

(Note: The next two questions are from the Global Preference Survey (GPS) by Falk et al. 2018; 2023.)

How do you see yourself: Are you a person who is generally willing to take risks, or do you try to avoid taking risks?

Please use a scale from 0 to 10, where a 0 means you are "completely unwilling to take risks" and a 10 means you are "very willing to take risks". You can also use the values in-between to indicate where you fall on the scale.

How well does the following statement describe you as a person? As long as I am not convinced otherwise, I assume that people have only the best intentions.

Please use a scale from 0 to 10, where 0 means "does not describe me at all" and a 10 means "describes me perfectly". You can also use the values in-between to indicate where you fall on the scale.

How well does the following statement describe you as a person? I am someone who pays attention to this survey. *(Note: Attention check 2)*

Please use a scale from 0 to 10, where 5 means "I am paying attention to this survey" and any other value means "I have not read this text". Please select 5 for us to be able to pay you.

Screen 11 (AI attitudes)

(Note: The next two questions are from Horowitz and Kahn 2021.)

Artificial Intelligence Concerns

In the following section you will be given statements about the use of algorithms. Please answer the questions about your possible concerns.

In thinking about adopting the use of algorithms, how should governments balance the potential to gain useful information that could improve public safety with the potential to violate people's individual privacy?

- Strongly support gaining information over the risk to privacy
- Somewhat support gaining information over the risk to privacy
- Equally important
- Somewhat support protecting privacy over gaining information
- Strongly support protecting privacy over gaining information

How concerned are you about the potential for bias in algorithms?

- Not at all concerned
- Slightly concerned
- Moderately concerned
- Very concerned
- Extremely concerned

Screen 12 (Privacy attitudes)

(Note: Of the following 19 questions, 18 are from the Internet Privacy Concerns (IPC) scale by Hong and Thong 2013, and one is an attention check. The order of question blocks and questions within blocks is randomized.)

Internet Privacy Concerns

In the following section, you will be given several statements about online privacy. Please select to what extent you agree or disagree with each statement.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
When websites ask me for personal information, I sometimes think twice before providing it.	☐	☐	☐	☐	☐	☐	☐
I am concerned that websites are collecting too much personal information about me.	☐	☐	☐	☐	☐	☐	☐
It usually bothers me when websites ask me for personal information.	☐	☐	☐	☐	☐	☐	☐

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
When people give personal information to a website for some reason, the website would never use the information for any other purpose.	☐	☐	☐	☐	☐	☐	☐
Websites would never share personal information with other companies unless it has been authorized by the individuals who provided the information.	☐	☐	☐	☐	☐	☐	☐
Websites would never sell the personal information in their computer databases to other companies.	☐	☐	☐	☐	☐	☐	☐

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
Websites should take more steps to make sure that the personal information in their files is accurate.	☐	☐	☐	☐	☐	☐	☐
This is an attention check. Select disagree to pass. *(Note: Attention check 3)*	☐	☐	☐	☐	☐	☐	☐
Websites should have better procedures to correct errors in personal information.	☐	☐	☐	☐	☐	☐	☐
Websites should devote more time and effort to verifying the accuracy of the personal information in their databases.	☐	☐	☐	☐	☐	☐	☐

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
Websites should take more steps to make sure that unauthorized people cannot access personal information in their computers.	☐	☐	☐	☐	☐	☐	☐
Websites should devote more time and effort to preventing unauthorized access to personal information	☐	☐	☐	☐	☐	☐	☐
Website databases that contain personal information should be protected from unauthorized access.	☐	☐	☐	☐	☐	☐	☐

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction with websites.	☐	☐	☐	☐	☐	☐	☐
Consumer control of personal information lies at the heart of consumer privacy.	☐	☐	☐	☐	☐	☐	☐
Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared by websites.	☐	☐	☐	☐	☐	☐	☐

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
Websites seeking personal information online should disclose the way the data are collected, processed, and used.	☐	☐	☐	☐	☐	☐	☐
A good consumer online privacy policy should have a clear and conspicuous disclosure.	☐	☐	☐	☐	☐	☐	☐
It is very important to me that I am aware and knowledgeable about how my personal information will be used by websites.	☐	☐	☐	☐	☐	☐	☐

Screen 13 (Socio-demographic questionnaire)

How old are you?

- Under 18
- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55-64 years old
- 65+ years old

What is your gender?

- Female
- Male
- Non-binary / third gender
- Prefer not to say

Choose one or more races to indicate what you consider yourself to be.

- Asian
- Black
- Hispanic or Latino
- White / Caucasian
- Other
- Prefer not to say

In which country were you born?

(Note: Country list provided.)

In which country do you currently reside?

(Note: Country list provided.)

What is the highest level of education that you have completed?

- Some primary education
- Completed primary
- Some secondary education
- Completed secondary
- Vocational or similar
- Some university but no degree
- University bachelors degree
- Graduate or professional degree (MA, MS, MBA, PhD, JD, MD, DDS etc.)
- Prefer not to say

B Factor analysis

Figure B.1: Scree plot of eigenvalues after factor analysis

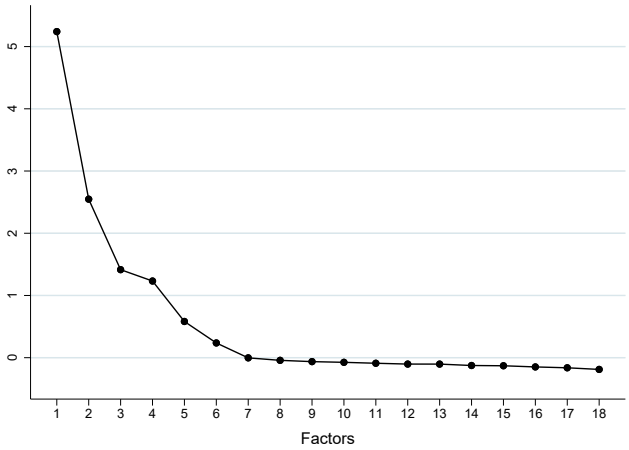


Table B.1: Rotated factor loadings (loadings smaller than **0.3** omitted)

	Factor1	Factor2	Factor3	Uniqueness
IPC: Collection, Q1	0.571	.	.	0.673
IPC: Collection, Q2	0.578	.	.	0.663
IPC: Collection, Q3	0.578	.	.	0.663
IPC: Secondary usage, Q1	.	.	0.769	0.363
IPC: Secondary usage, Q2	.	.	0.820	0.309
IPC: Secondary usage, Q3	.	.	0.779	0.384
IPC: Errors, Q1	.	0.882	.	0.213
IPC: Errors, Q2	.	0.804	.	0.342
IPC: Errors, Q3	.	0.868	.	0.238
IPC: Improper access, Q1	0.677	.	.	0.495
IPC: Improper access, Q2	0.722	.	.	0.441
IPC: Improper access, Q3	0.697	.	.	0.461
IPC: Control, Q1	0.578	.	.	0.660
IPC: Control, Q2	0.575	.	.	0.667
IPC: Control, Q3	0.617	.	.	0.613
IPC: Awareness, Q1	0.648	.	.	0.548
IPC: Awareness, Q2	0.617	.	.	0.594
IPC: Awareness, Q3	0.714	.	.	0.470

C Full descriptive statistics

In addition to the variables reported in Table 1 in main text, Table C.1 below also shows information on the factor scores as well as all further variables that are only used in the additional analysis conducted in Appendix D.

Table C.1: Full descriptive statistics

	Full sample				Europe	US	Non-users	Users
	Mean	SD	Min	Max	Mean	Mean	Mean	Mean
Would you use the app?	0.35	0.48	0	1	0.35	0.34	0.00	1.00
How convincing is the app?	2.66	1.21	1	5	2.69	2.62	2.07	3.75
How many others would use the app?	2.70	1.09	1	5	2.78	2.62	2.29	3.46
Opt-in needed (treat)	0.50	0.50	0	1	0.49	0.50	0.50	0.48
Privacy risk salient (treat)	0.50	0.50	0	1	0.49	0.51	0.52	0.48
Location salient (treat)	0.51	0.50	0	1	0.52	0.50	0.51	0.51
US server location (treat)	0.33	0.47	0	1	0.34	0.32	0.32	0.34
EU server location (treat)	0.32	0.47	0	1	0.32	0.33	0.30	0.37
Home bias	0.32	0.47	0	1	0.32	0.32	0.29	0.38
Home bias in the US	0.17	0.37	0	1	0.00	0.32	0.15	0.19
Home bias in Europe	0.15	0.36	0	1	0.32	0.00	0.14	0.19
IPC: Collection	5.73	1.07	1	7	5.69	5.76	5.96	5.29
IPC: Secondary usage	2.67	1.66	1	7	2.54	2.79	2.41	3.14
IPC: Control	4.84	1.35	1	7	4.51	5.15	4.70	5.10
IPC: Errors	6.47	0.81	1	7	6.46	6.48	6.61	6.22
IPC: Improper access	5.80	0.92	2.3	7	5.71	5.88	5.93	5.55
IPC: Awareness	6.25	0.80	2.7	7	6.17	6.32	6.38	6.00
Data protection (f1)	-0.00	0.95	-4.9	1.6	-0.06	0.05	0.21	-0.39
Personal information correct (f2)	0.00	0.90	-1.5	2.8	-0.07	0.06	-0.11	0.20
Trust secondary usage (f3)	-0.00	0.93	-2.8	1.7	-0.22	0.21	-0.10	0.19
Willingness to take risks	4.81	2.39	0	10	5.04	4.60	4.47	5.47
Generalized trust level	4.91	2.49	0	10	4.85	4.96	4.68	5.32
Gov use of AI	3.87	1.02	1	5	3.81	3.93	4.08	3.48
Concern about AI	3.23	1.03	1	5	3.19	3.27	3.41	2.89
Gender: Female	0.40	0.49	0	1	0.36	0.45	0.42	0.38
Gender: Other or n/a	0.03	0.17	0	1	0.03	0.03	0.04	0.01
25-34 years old	0.39	0.49	0	1	0.47	0.31	0.39	0.38
35-44 years old	0.22	0.41	0	1	0.18	0.25	0.23	0.19
45-54 years old	0.12	0.32	0	1	0.06	0.18	0.12	0.11
55-64 years old	0.06	0.25	0	1	0.02	0.11	0.07	0.05
65+ years old	0.04	0.20	0	1	0.01	0.07	0.04	0.03
US sample	0.51	0.50	0	1	0.00	1.00	0.52	0.51

Notes: Number of observations: Full sample: $N = 1,734$, Europe: $N = 844$, US: $N = 890$, Non-users: $N = 1,129$, Users: $N = 605$. .

D Robustness tests and additional results

D.1 Robustness test 1: Alternative dependent variables

Table D.1: How convincing is the app

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	-0.070	-0.072	-0.077	-0.103*
	(0.050)	(0.050)	(0.051)	(0.051)
Privacy risk salient (treat)	-0.071	-0.074	-0.067	-0.071
	(0.050)	(0.050)	(0.051)	(0.052)
US server location (treat)	0.187**	0.124(+)	0.117(+)	0.119(+)
	(0.062)	(0.068)	(0.068)	(0.069)
EU server location (treat)	0.216***	0.156*	0.161*	0.178*
	(0.061)	(0.068)	(0.069)	(0.070)
Home bias		0.125*	0.128*	0.104(+)
		(0.062)	(0.062)	(0.062)
Data protection (f1)				-0.113***
				(0.030)
Personal information correct (f2)				0.131***
				(0.030)
Trust secondary usage (f3)				0.146***
				(0.031)
Willingness to take risks				0.059***
				(0.013)
Generalized trust level				0.033**
				(0.012)
Gov use of AI				-0.216***
				(0.030)
Concern about AI				-0.173***
				(0.029)
Cutoff 1	-0.825***	-0.828***	-1.134***	-2.091***
	(0.064)	(0.064)	(0.082)	(0.187)
Cutoff 2	0.039	0.037	-0.252**	-1.095***
	(0.062)	(0.062)	(0.080)	(0.185)
Cutoff 3	0.591***	0.589***	0.308***	-0.468*
	(0.064)	(0.064)	(0.081)	(0.184)
Cutoff 4	1.525***	1.526***	1.252***	0.561**
	(0.072)	(0.072)	(0.087)	(0.187)
Age and gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,734	1,734	1,734
Nagelkerke R-sq.	0.012	0.015	0.043	0.220

Notes: Ordered Probit regression coefficients with robust SE in parentheses. Ordered categorical dependent variable indicates: How convincing is the app? - extremely/.../not at all. $^{(+)}$: $p < 0.10$, * : $p < 0.05$, ** : $p < 0.01$, *** : $p < 0.001$.

Table D.2: How many others would use the app

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	0.016	0.016	0.012	0.003
	(0.050)	(0.050)	(0.050)	(0.051)
Privacy risk salient (treat)	-0.094(+)	-0.094(+)	-0.091(+)	-0.082
	(0.050)	(0.051)	(0.051)	(0.051)
US server location (treat)	0.326***	0.325***	0.332***	0.334***
	(0.062)	(0.069)	(0.069)	(0.069)
EU server location (treat)	0.346***	0.345***	0.350***	0.373***
	(0.062)	(0.070)	(0.070)	(0.071)
Home bias		0.001	-0.000	-0.027
		(0.062)	(0.061)	(0.062)
Data protection (f1)				-0.081**
				(0.031)
Personal information correct (f2)				0.073*
				(0.031)
Trust secondary usage (f3)				0.086**
				(0.030)
Willingness to take risks				0.065***
				(0.012)
Generalized trust level				0.036**
				(0.011)
Gov use of AI				-0.063*
				(0.029)
Concern about AI				-0.021
				(0.027)
Cutoff 1	-1.004***	-1.004***	-1.248***	-1.051***
	(0.066)	(0.066)	(0.089)	(0.182)
Cutoff 2	0.008	0.008	-0.228**	0.001
	(0.063)	(0.063)	(0.086)	(0.181)
Cutoff 3	0.776***	0.776***	0.545***	0.807***
	(0.065)	(0.065)	(0.087)	(0.182)
Cutoff 4	1.800***	1.800***	1.580***	1.883***
	(0.077)	(0.077)	(0.096)	(0.188)
Age and gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,734	1,734	1,734
Nagelkerke R-sq.	0.032	0.032	0.047	0.110

Notes: Ordered Probit regression coefficients with robust SE in parentheses. Ordered categorical dependent variable indicates: How many others would use the app? - 20% intervals. $^{(+)}$: $p < 0.10$, * : $p < 0.05$, ** : $p < 0.01$, *** : $p < 0.001$.

D.2 Robustness test 2: Linear probability models (OLS)

Table D.3: Willingness to use the app (OLS)

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	-0.018	-0.019	-0.020	-0.023
	(0.023)	(0.023)	(0.023)	(0.020)
Privacy risk salient (treat)	-0.033	-0.035	-0.030	-0.027
	(0.023)	(0.023)	(0.023)	(0.021)
US server location (treat)	0.071**	0.038	0.038	0.033
	(0.027)	(0.031)	(0.030)	(0.028)
EU server location (treat)	0.113***	0.081**	0.083**	0.085**
	(0.028)	(0.031)	(0.031)	(0.028)
Home bias		0.066*	0.066*	0.052*
		(0.029)	(0.028)	(0.025)
Data protection (f1)				-0.097***
				(0.012)
Personal information correct (f2)				0.061***
				(0.012)
Trust secondary usage (f3)				0.067***
				(0.011)
Willingness to take risks				0.028***
				(0.004)
Generalized trust level				0.011**
				(0.004)
Gov use of AI				-0.053***
				(0.011)
Concern about AI				-0.055***
				(0.010)
Age and gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,734	1,734	1,734
R-sq.	0.011	0.015	0.040	0.218

Notes: OLS regression coefficients with robust SE in parentheses. Binary dependent variable indicates: Would you use the app? - yes/no. $^{(+)}: p < 0.10$, $^{*}: p < 0.05$, $^{**}: p < 0.01$, $^{***}: p < 0.001$.

Table D.4: How convincing is the app (OLS)

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	-0.076	-0.077	-0.082	-0.099(+)
	(0.058)	(0.058)	(0.057)	(0.052)
Privacy risk salient (treat)	-0.074	-0.078	-0.070	-0.065
	(0.058)	(0.058)	(0.058)	(0.053)
US server location (treat)	0.216**	0.137(+)	0.127(+)	0.116(+)
	(0.071)	(0.078)	(0.077)	(0.070)
EU server location (treat)	0.251***	0.176*	0.181*	0.179*
	(0.070)	(0.078)	(0.078)	(0.071)
Home bias		0.157*	0.158*	0.123(+)
		(0.072)	(0.071)	(0.064)
Data protection (f1)				-0.129***
				(0.031)
Personal information correct (f2)				0.133***
				(0.031)
Trust secondary usage (f3)				0.139***
				(0.030)
Willingness to take risks				0.062***
				(0.012)
Generalized trust level				0.036**
				(0.012)
Gov use of AI				-0.219***
				(0.030)
Concern about AI				-0.166***
				(0.029)
Age and gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,734	1,734	1,734
R-sq.	0.011	0.014	0.040	0.209

Notes: OLS regression coefficients with robust SE in parentheses. Ordered categorical dependent variable indicates: How convincing is the app? - extremely/.../not at all. $^{(+)}: p < 0.10$, $^{*}: p < 0.05$, $^{**}: p < 0.01$, $^{***}: p < 0.001$.

Table D.5: How many others would use the app (OLS)

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	0.020	0.020	0.016	0.008
	(0.052)	(0.052)	(0.051)	(0.050)
Privacy risk salient (treat)	-0.103*	-0.102*	-0.099(+)	-0.086(+)
	(0.052)	(0.052)	(0.052)	(0.050)
US server location (treat)	0.331***	0.332***	0.336***	0.325***
	(0.062)	(0.070)	(0.070)	(0.068)
EU server location (treat)	0.351***	0.352***	0.354***	0.364***
	(0.063)	(0.071)	(0.070)	(0.069)
Home bias		-0.002	-0.002	-0.026
		(0.064)	(0.063)	(0.062)
Data protection (f1)				-0.080**
				(0.031)
Personal information correct (f2)				0.079**
				(0.030)
Trust secondary usage (f3)				0.083**
				(0.029)
Willingness to take risks				0.065***
				(0.012)
Generalized trust level				0.035**
				(0.011)
Gov use of AI				-0.061*
				(0.029)
Concern about AI				-0.018
				(0.027)
Age and gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,734	1,734	1,734
R-sq.	0.030	0.030	0.044	0.105

Notes: OLS regression coefficients with robust SE in parentheses. Ordered categorical dependent variable indicates: How many others would use the app? - 20% intervals. $^{(+)}$: $p < 0.10$, * : $p < 0.05$, ** : $p < 0.01$, *** : $p < 0.001$.

D.3 Robustness test 3: Excluding lower quality observations

Table D.6: Willingness to use the app (comprehension check)

	(1)	(2)	(3)	(4)
Opt-in needed (treat)	-0.023	-0.028	-0.021	-0.036
	(0.020)	(0.020)	(0.021)	(0.024)
Privacy risk salient (treat)	-0.032	-0.034$^{(+)}$	-0.039$^{(+)}$	-0.053*
	(0.020)	(0.020)	(0.021)	(0.024)
US server location (treat)	0.034	0.041	0.052$^{(+)}$	0.080*
	(0.028)	(0.028)	(0.028)	(0.032)
EU server location (treat)	0.084**	0.085**	0.085**	0.113***
	(0.028)	(0.028)	(0.029)	(0.033)
Home bias	0.041$^{(+)}$	0.039	0.035	0.022
	(0.024)	(0.024)	(0.025)	(0.028)
Data protection (f1)	-0.089***	-0.091***	-0.085***	-0.084***
	(0.011)	(0.011)	(0.012)	(0.013)
Personal information correct (f2)	0.057***	0.058***	0.054***	0.046***
	(0.011)	(0.011)	(0.011)	(0.013)
Trust secondary usage (f3)	0.078***	0.076***	0.074***	0.060***
	(0.013)	(0.013)	(0.013)	(0.015)
Willingness to take risks	0.027***	0.028***	0.027***	0.025***
	(0.004)	(0.004)	(0.004)	(0.005)
Generalized trust level	0.012**	0.012**	0.013**	0.012*
	(0.004)	(0.004)	(0.004)	(0.005)
Gov use of AI	-0.050***	-0.049***	-0.051***	-0.058***
	(0.010)	(0.010)	(0.011)	(0.012)
Concern about AI	-0.062***	-0.064***	-0.066***	-0.069***
	(0.010)	(0.010)	(0.010)	(0.012)
Age and gender dummies	Yes	Yes	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
Respondents	1,734	1,688	1,600	1,200
Nagelkerke R-sq.	0.300	0.308	0.303	0.309

Notes: Average marginal effects based on Probit models with robust SE in parentheses. Binary dependent variable indicates: Would you use the app? - yes/no. (1): full sample, (2): took less than four comprehension checks to pass, (3): ... less than three, (4): passed at the first attempt. $^{(+)}$: $p < 0.10$, * : $p < 0.05$, ** : $p < 0.01$, *** : $p < 0.001$.

D.4 Additional results 1: Willingness to use the app across subsamples

Table D.7: Willingness to use the app (subsamples)

	(1)	(2)	(3)	(4)	(5)
Opt-in needed (treat)	-0.079	-0.081	-0.030	-0.125	-0.030
	(0.068)	(0.068)	(0.098)	(0.096)	(0.098)
Privacy risk salient (treat)	-0.106	-0.102	-0.192*	-0.024	-0.192*
	(0.068)	(0.068)	(0.098)	(0.096)	(0.098)
US server location (treat)	0.116	-0.016	0.001	0.389***	0.001
	(0.094)	(0.120)	(0.121)	(0.116)	(0.121)
EU server location (treat)	0.285**	0.417***	0.309**	0.417***	0.309**
	(0.094)	(0.119)	(0.120)	(0.120)	(0.120)
Home bias	0.138(+)				
	(0.082)				
Home bias in the US		0.403*			
		(0.166)			
Home bias in Europe		-0.128			
		(0.168)			
Data protection (f1)	-0.301***	-0.302***	-0.242***	-0.347***	-0.242***
	(0.039)	(0.039)	(0.057)	(0.057)	(0.057)
Personal information correct (f2)	0.192***	0.193***	0.089	0.258***	0.089
	(0.037)	(0.038)	(0.058)	(0.050)	(0.058)
Trust secondary usage (f3)	0.264***	0.264***	0.212***	0.338***	0.212***
	(0.044)	(0.044)	(0.061)	(0.067)	(0.061)
Willingness to take risks	0.093***	0.094***	0.097***	0.092***	0.097***
	(0.015)	(0.015)	(0.024)	(0.020)	(0.024)
Generalized trust level	0.041**	0.042**	0.056**	0.027	0.056**
	(0.014)	(0.014)	(0.022)	(0.020)	(0.022)
Gov use of AI	-0.167***	-0.167***	-0.187***	-0.152**	-0.187***
	(0.036)	(0.036)	(0.050)	(0.051)	(0.050)
Concern about AI	-0.209***	-0.208***	-0.321***	-0.146**	-0.321***
	(0.035)	(0.035)	(0.053)	(0.048)	(0.053)
US * Opt-in needed (treat)					-0.095
					(0.137)
US * Privacy risk salient (treat)					0.169
					(0.137)
US * US server location (treat)					0.388*
					(0.168)
US * EU server location (treat)					0.107
					(0.170)
US * Data protection (f1)					-0.105
					(0.080)
US * Personal information correct (f2)					0.169*
					(0.076)
US * Trust secondary usage (f3)					0.125
					(0.091)
US * Willingness to take risks					-0.005
					(0.031)
US * Generalized trust level					-0.029
					(0.029)
US * Gov use of AI					0.035
					(0.072)
US * Concern about AI					0.175*
					(0.071)
Age and gender dummies	Yes	Yes	Yes	Yes	Yes
US sample dummy	Yes	Yes	No	No	Yes
Respondents	1,734	1,734	844	890	1,734
Nagelkerke R-sq.	0.300	0.302	0.312	0.313	0.313

Notes: Probit regression coefficients with robust SE in parentheses. Binary dependent variable indicates: Would you use the app? - yes/no. (1): main model as in Column 4 of Table 2, (2): location-specific home biases, (3): Europe sample, (4): US sample, (5): Test effect differences between EU and US (interaction model). $^{(+)}$: $p < 0.10$, * : $p < 0.05$, ** : $p < 0.01$, *** : $p < 0.001$.

D.5 Additional results 2: Treatment with location salience

Table D.8: Willingness to use the app (location salience)

	(1)	(2)	(3)
US server location (treat)	0.027	0.110	0.293**
	(0.037)	(0.096)	(0.093)
EU server location (treat)	0.073(+)	0.161(+)	0.287**
	(0.039)	(0.095)	(0.091)
Location salient (treat)	-0.027	-0.115	-0.097
	(0.034)	(0.090)	(0.084)
Salience * US server location (treat)	0.011	0.006	0.063
	(0.049)	(0.129)	(0.121)
Salience * EU server location (treat)	0.022	0.026	0.151
	(0.051)	(0.129)	(0.123)
Location-unrelated independent variables	Yes	Yes	Yes
Respondents	1,734	1,734	1,734
R-sq.	0.218	0.210	0.106

Notes: OLS regression coefficients with robust SE in parentheses. (1): Binary dependent variable indicates: Would you use the app? - yes/no. (2): Ordered categorical dependent variable indicates: How convincing is the app? - extremely/.../not at all. (3): Ordered categorical dependent variable indicates: How many others would use the app? - 20% intervals. $^{(+)}: p < 0.10$, $^{*}: p < 0.05$, $^{**}: p < 0.01$, $^{***}: p < 0.001$.