

How Much is Your Privacy Worth? Keep Your Friends Close and AI Closer

June Ma*

November 15, 2025

Job Market Paper

[Click here for latest version](#)

Abstract

Why do individuals claim to value privacy, yet readily share their data with AI assistants? I develop a framework to explain the privacy tradeoffs individuals make in disclosing personal data across different contexts, and reconcile this ‘privacy paradox’. Using a discrete choice experiment, I estimate privacy valuations across different data types and recipients under this model, extending to AI and social contexts not previously studied. I find the value individuals place on privacy from social contacts can exceed that from institutions, despite privacy laws focusing on the latter. The emergence of AI complicates this distinction, and I document the existence of an AI privacy puzzle: individuals are largely unconcerned about privacy from AI assistants, even for information they withhold from close contacts, yet attach a premium on privacy from the firms that develop them. Individuals value certain dimensions of privacy more than others, and this multidimensionality explains the privacy paradox. I show that control over data disclosure matters to the value of privacy. When individuals lose control, its value is substantially higher and is derived from the potential consequences of unauthorised diffusion. These findings provide a foundation for more effective privacy regulation, AI governance, and product design.

JEL No. C91, D83, D91, K20, L51, L86, O33, O38

*Department of Economics, Harvard University. Contact: junema@fas.harvard.edu. This study was determined to be IRB exempt by the Harvard University Institutional Review Board (IRB25-0496). I am deeply grateful to Lauren Cohen, Scott Kominers, Ken Rogoff, and Larry Summers for their guidance and support. I also thank Eva Ascarza, Malcolm Baker, John Campbell, Ramon Casadesus-Masanell, Julian De Freitas, Chiara Farronato, Kris Ferreira, Joshua Gans, Amit Goldenberg, Avi Goldfarb, Robin Greenwood, Sam Hanson, Leslie John, Elizabeth Linos, Max Miller, Marco Sammon, Andrei Shleifer, Jeremy Stein, Adi Sunderam, Catherine Tucker, Luis Viceira, Jonathan Wallen, Feng Zhu, and seminar participants at Harvard for their helpful advice and feedback. Support from the Lab for Economic Applications and Policy at Harvard is gratefully acknowledged.

1 Introduction

Individuals claim to value privacy, yet routinely share personal data. This apparent contradiction between stated preferences and observed behaviour is known as the ‘privacy paradox’ (Norberg et al. 2007; Athey et al. 2017; Chen et al. 2021; Colnago et al. 2023). However, much of the existing economic literature and legal frameworks treat privacy as monolithic, a simplification that overlooks the tradeoffs individuals consider in making voluntary data disclosures. I develop a framework to explain these tradeoffs, and use it to provide empirical evidence of the multidimensional nature of privacy, thereby reconciling the privacy paradox.

Privacy concerns raised by increasing internet use have led to the enactment of modern privacy regulations such as the General Data Protection Regulation (GDPR) in the EU and UK, and the California Consumer Privacy Act (CCPA) to protect consumers’ digital data. These frameworks are based on the conception of data privacy as *control* over personal information in Westin (1968), granting consumers certain rights over their data, and restricting how organisations can use it. While these laws are designed to increase the control consumers have over their data, they only assign value to privacy when a breach results in harmful *consequences*. The loss of control is a necessary, but not sufficient, condition for compensation.

This dynamic between *control* and *consequence* is consistent with how individuals think about privacy. When asked to define data privacy, I find individuals typically take a normative stance based on *control*, consistent with Westin (1968). However, when faced with the loss of privacy through involuntary data diffusion, individuals are most concerned about *consequences*, rather than the loss of control itself. While individuals describe data privacy through control, what they actually value when control is lost are the harms that privacy would have prevented. This distinction is important in understanding what privacy preferences and valuations measure.

Existing empirical work largely assumes a *control* model of privacy, in which estimates are derived from contexts involving the voluntary disclosure of personal information to insti-

tutions (e.g. Tsai et al. 2011; Acquisti et al. 2013; Savage & Waldman 2015).¹ More recently, Lin (2022) differentiates between *intrinsic* (privacy as a ‘final good’, where it is protected as matter of personal taste), and *instrumental* (privacy as an ‘intermediate good’, where it is protected to avoid certain harms) components of privacy following Farrell (2012), and finds an average intrinsic willingness to accept of no more than \$2.37 for a demographic variable. In that paper, instrumental privacy is taken to be the consumer’s beliefs about loss from disclosure data to a firm, where there is no subsequent diffusion. By contrast, Hann et al. (2007) incorporate the risks of data diffusion, and estimate the value of protection against secondary uses of personal data such as unauthorised access and errors to be between \$30.49 and \$44. These differences highlight how the value of privacy may be understated when the consequences of privacy loss are not considered.

Using a discrete choice experiment, I provide the first set of privacy valuation estimates across a range of data types and recipients according to a consequence framing of privacy. These results provide an empirical counterpart to Kim et al. (2021), who conceptually differentiate between active (voluntary) and passive (involuntary) disclosure across social and commercial contexts. This approach allows trade offs across different contexts to be quantified and compared without requiring participants to reveal personal information. The resulting valuations are substantially higher than those implied by voluntary disclosures under the control model. While individuals are willing to pay \$256 to prevent a one-off leak of their identity data to a firm, they are not concerned about firms receiving their browsing activity. This suggests that consumer privacy protections, such as the GDPR, could be more effectively tailored to consumers’ needs, reducing unnecessary burden to firms (Johnson 2024).

These estimates provide the first empirical evidence of the importance of social privacy, showing individuals place a higher value on preventing data from being seen by close family

¹Acquisti et al. (2016), Goldfarb & Que (2023), and Acquisti (2024) provide surveys of the literature on the economics of privacy, including privacy valuation studies. Acquisti et al. (2015) provide a survey of the empirical research on privacy behaviour more broadly.

or friends compared with firms or government agencies in certain contexts. This reflects another dimension of the context dependence of privacy in quantifying Nissenbaum (2004), who defines privacy as the appropriateness of information flows relative to social norms in her theory of ‘contextual integrity’. Individuals are willing to pay a positive premium to protect information containing personal admissions or private remarks about others from close contacts. To the extent that such information could include habits or opinions that do not conform with social norms, these valuations support the literature on social image.² For example, Bursztyn et al. (2020) and Braghieri (2024) provide evidence that individuals strategically misrepresent their private political views in accordance with social norms. These findings raise important questions for privacy regulation, which has primarily focused on institutions while overlooking the social dimensions of privacy.

I also document the existence of an AI privacy puzzle. As AI assistants has become increasingly embedded in daily life, their use has extended beyond productivity tools to quasi-social roles such as therapist, friend, or even romantic partner, and the results likely reflect these uses. Individuals place a negative value on privacy from AI assistants, even for data they would pay a premium for to protect from close contacts, which to AI assistants could reflect the absence of social frictions. John et al. (2011) provide evidence that individuals have an increased willingness to disclose sensitive information when asked indirectly or in settings that appear less professional, while Goldfarb et al. (2015) find individuals disclose more information on digital platforms compared with humans. AI assistants also possess anthropomorphic qualities that lead to perceptions that they are less judgmental compared with humans (Geiecke & Jaravel 2024), and are more available (De Freitas, Uğuralp, Uğuralp & Puntoni 2025), which could explain this result. However, AI is seen as both a friend and a foe. While individuals discount privacy from AI assistants, they attach a premium to privacy from the firms behind them, highlighting the dual identity of AI.

This paper develops a framework and provides empirical evidence for understanding

²Bursztyn & Jensen (2017) provide a survey of the literature.

privacy as a multidimensional concept shaped by context and consequence. It provides the first empirical estimates of how individuals tradeoff and value privacy across both social and institutional settings, and how AI blurs this distinction. The results demonstrate that the privacy paradox does not reflect contradictory differences, but rather the privacy tradeoffs individuals across different contexts. These findings raise important considerations for data privacy regulation, AI governance, and product design.

The paper proceeds as follows. Section 2 develops a conceptual framework for individuals' data disclosure decisions incorporating the risk of involuntary diffusion. Section 3 details the empirical strategy and survey design. Section 4 reports and discusses the implications of the privacy valuations from the discrete choice experiment. Section 5 further examines how individuals view privacy in relation to AI, highlighting the gap between AI assistants and the firms behind them. Section 6 concludes, and suggests directions for future research.

2 Conceptual framework

The existence of the privacy paradox relies on individuals reported privacy preferences, and their behaviour in disclosing personal data in exchange for very little as evidence that they are not actually concerned about privacy. This assumes individuals derive minimal benefit from voluntary disclosures. However, the literature on privacy decision making suggests that voluntary disclosures do not reflect a lack of care, but instead reflect an exchange of value (Acquisti et al. 2020). Casadesus-Masanell & Hervas-Drane (2015) provide an equilibrium model of firm competition with privacy, in which consumers consider the costs and benefits of voluntary disclosure. I focus on consumer utility maximisation problem, extending it to include consideration of the risks and harms from involuntary downstream diffusion.

2.1 What does it mean to value privacy?

Before providing a conceptual framework or empirical estimates of the value of privacy, it is essential to understand what it means. Privacy is not monolithic and means different things to different people, and is context dependent (Acquisti et al. 2016). To understand how individuals think about privacy, and what it means to be concerned about it, I surveyed participants on their mental models.³

First, I asked participants ‘what does data privacy mean to you?’, and used GPT-5 to categorise their open ended responses.⁴ As expected, responses were diverse, and as one astute participant noted it is ‘a blanket phrase...that means different things to different people’. Others questioned its existence altogether with one response suggesting it is ‘[s]omething that really doesn’t exist any longer’. Just over 16 per cent of responses did not offer substantive conceptual definitions because they were circular (e.g. ‘data privacy means privacy of data’), provided examples of certain data types considered to be private, or were otherwise unintelligible. Of the remaining responses, 90 per cent considered data privacy as the ability to control or protect personal information, consistent with Westin (1968). The other 10 per cent defined data privacy in the negative, based on particular consequences that necessitate the loss of control or protection (e.g. ‘[n]ot having my identity stolen or my info sold to 3rd partners [*sic*]’).

By contrast, when participants were asked what would concern them if their personal data was leaked, only nine per cent indicated loss of control as their primary concern.⁵ Six per cent were most concerned about surveillance or tracking, while the remaining 85 per cent were split across different harmful consequences (e.g. identity theft, fraud, social or professional consequences). This suggests that while loss of control over one’s data is undesirable, individuals do not perceive any loss until they suffer actual harm. It follows

³Section 3.1 provides a detailed data description.

⁴Appendix A.1 provides the prompt used.

⁵Participants were asked to choose from a list of options curated from open ended responses during piloting displayed in randomised order.

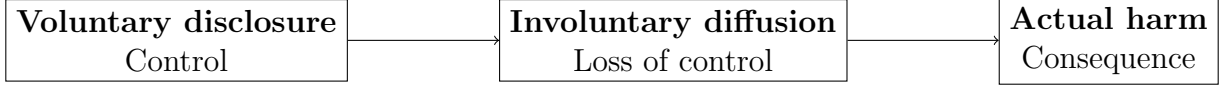


Figure 1: Data disclosure and diffusion process

that the value of privacy is derived from these consequences, consistent with legal safeguards.

These responses demonstrate that individuals' models of privacy are context dependent. When asked to define data privacy, individuals tend to give idealistic and normative responses that reflect intrinsic preferences to control personal information. However, when asked about concerns over losing privacy, they focus on harmful consequences of diffusion, rather than the mechanisms that create such risks. Thus, general questions about whether people care about privacy are likely to reflect the normative desire for control, while the economic value of privacy arises from preventing the harmful consequences from involuntary diffusion.

2.2 Model

I model the data disclosure and diffusion process described in Figure 1 as it relates to a particular voluntary disclosure of a data type to a particular recipient.

Suppose individual i gets a benefit $b_i(j, k) \geq 0$ from disclosing data type k to a recipient j , such as moral support from a friend after telling them a secret, or a service from a firm or government agency that requires the provision of certain personal details. For that same disclosure, the individual also incurs damage $d_i(j, k) \geq 0$, such as embarrassment or an intrinsic preference for privacy. Let $\delta_{i,j;l} \in [0, 1)$ be a relationship specific discount factor for $l = \{\text{benefit}, \text{damage}\}$. The higher $\delta_{i,j}^l$, the closer the personal relationship between i and j , and the longer individual i will derive a benefit or incur damage from a making the disclosure. For example, an individual may expect to have repeated personal interactions with a friend, so what they disclose to them will be retained in memory throughout the relationship, whereas an interaction with a representative of an institution is more likely to be one-off. The discount factor is assumed to be asymmetric between benefits and damages to allow for their persistence to differ.

The present value of individual i 's net benefit from disclosing data type k to a recipient j is

$$v_i(j, k) = \sum_{t=0}^n \delta_{i,j;b}^t b_{i,t}(j, k) - \delta_{i,j;d}^t d_{i,t}(j, k),$$

where n is the number of periods i and j interact in.

Let i 's beliefs that the data may subsequently be diffused to some other recipient j' – whether because of j 's actions or not – be $\hat{p}_i(j, k; j') \in [0, 1]$, then individual i 's utility from making such a disclosure is

$$U_i^{\text{disclose}}(j, k) = \underbrace{v_i(j, k)}_{\text{control}} + \sum_{j' \neq j} \hat{p}_i(j, k; j') \underbrace{v_i(j', k)}_{\text{consequence}}.$$

Normalise the utility of non disclosure to zero

$$U_i^{\text{don't disclose}}(j, k) = 0.$$

Then individual i will make a data disclosure of data type k to recipient j iff

$$v_i(j, k) + \sum_{j' \neq j} \hat{p}_i(j, k; j') v_i(j', k) \geq 0.$$

However, once data is disclosed, subsequent involuntary diffusion is possible. If the individual is particularly sensitive to some recipient j' accessing data type k , then $v_i(j', k)$ will be negative and large in magnitude, and may result in the individual choosing not to disclose that information to j even if $v_i(j, k) > 0$. Similarly, the higher the probability of diffusion to a recipient the individual is sensitive to (e.g. j is a gossip, has poor data security, or privacy regulations are weak or not enforced), the less likely they are to disclose to j .

Now suppose an individual can pay some cost $c(j', k)$ to prevent data type k from being diffused to j' . For example, people pay for VPNs, which can prevent their browsing activity

from being visible to their internet service provider. Individual i will pay this cost iff it is less than or equal to the expected loss from diffusion

$$c(j', k) \leq \hat{p}_i(j', k) \max\{0, -v_i(j', k)\}.$$

Hence, an individual’s maximum willingness to pay to prevent data type k from reaching j' is equal to the expected net damage from diffusion. This represents an individual’s consequential valuation of privacy.

This framework reconciles the privacy paradox decomposing voluntary data disclosure decisions into contextual privacy valuations based on control and consequence. It captures the idea that voluntary data disclosures do not reflect a lack of concern about privacy, but involve an exchange from which an individual derives a net benefit. For example, this framework can explain why it is rational for an individual to provide their email address to a retailer for a small discount. If the individual considers this discount to be worth more than the direct cost of giving up their email, and the expected indirect cost of subsequent diffusion, such as to third party marketers, then this disclosure is consistent with an intrinsic preference for privacy.

3 Empirical strategy

3.1 Data description

I recruited representative samples of participants from the United States (US) ($N = 498$) and the United Kingdom (UK) ($N = 500$) on Prolific in July and August 2025 to take part in an incentivised study on personal data decisions. The US representative sample is stratified on age, sex, ethnicity, and political affiliation, while the UK representative sample is stratified on age, sex, and political affiliation.⁶

⁶Prolific does not yet permit the UK sample to be stratified on ethnicity and political affiliation simultaneously. Political affiliation was chosen over ethnicity as it is less concentrated, and can be estimated more

The two country samples were recruited separately using Prolific’s preset stratification based on US and UK census data. The surveys were identical between the two samples except for minor adjustments to names, spelling, and currency to ensure cultural relevance. There were no eligibility restrictions on participation other than demographic quotas.

3.1.1 Discrete Choice Experiment

The survey centered around a discrete choice experiment (DCE) designed to elicit how participants trade-off different attributes that are relevant to the privacy of their personal data. The use of a DCE to elicit privacy preferences is innovative as it enables participants to make realistic privacy decisions without disclosing any personal data. DCEs have previously been used in privacy applications in Choi et al. (2025) and Fairweather et al. (2024), which focused on financial transactions data in a central bank digital currency context. Both these studies estimated modest willingness to pay for privacy of bank account transactions.

To capture the consequence model of privacy, the DCE was framed as a ransom scenario requiring participants to make trade offs between different dimensions of privacy. Figure 2 provides the preamble and an example of a choice set shown to participants.

Participants in each sample were randomised into two groups, with each being shown a different block of 12 choice sets to minimise survey fatigue. A forced choice approach required participants to select which of the two potential leaks they would most want to prevent to ensure they made trade-offs. Allowing participants to opt out could conflate different motives: a genuine indifference between scenarios (whether they want to prevent both or not), and an intrinsic desire to maintain one’s privacy.

The DCE included three attributes: data type, data recipient, and the ransom value, each with four levels. The ransom value is a proxy for the value individuals place on particular data type and recipient pairs, and was required to quantify participants’ preferences. The one-off ransom values of \$10, \$30, \$70, \$120 were calibrated in pilots to ensure that participants were

precisely given limitations on sample size.

*Imagine someone – a hacker, or even someone you know – has access to some of your personal data, and is threatening to leak it to specific people or organizations unless you pay a ransom. In the following 12 questions, you will be shown two scenarios. Choose the scenario you would most want to prevent based on the type of data, who would receive it, and the ransom amount.*⁷

Choose the scenario you would most want to prevent based on the type of data, who would receive it, and the ransom amount.

► Definitions (click or tap to show or hide)

	Scenario A	Scenario B
Data type	Browsing activity	Private judgmental remarks
Recipient	A government agency	Someone close to you
Ransom	\$120	\$70

Pay ransom to prevent:

Scenario A Scenario B

☐ ☐

Figure 2: An example of a DCE choice set

making trade offs based on all attributes, rather than only on cost differentials. The values are realistic and broadly in line with the range of annual VPN subscription costs.

The following data type and recipients were included as attributes. Participants were shown these definitions and examples prior to commencing the DCE tasks, and were able to access them as required.

Data types

- **Browsing activity:** information about your online behavior and habits (e.g. records of your searches, websites visited, and app usage – excluding private conversations)

- **Private judgmental remarks:** judgmental or critical comments you’ve made about others in private, including any about the potential recipient of the leak (e.g. screenshots, recordings or transcripts of private conversations containing these remarks)
- **Personal admissions:** personal secrets you’ve only shared with a select few, not including the potential recipient of the leak (e.g. screenshots, recordings or transcripts of private conversations containing these admissions)
- **Identity data:** personal details routinely collected, stored, and used by the government to issue identification documents and provide services (e.g. name, address, DOB, SSN, biometric data, income, or certain healthcare records)

Potential data recipients

- **Someone close to you** (e.g. your partner, a family member, or a friend)
- **An AI assistant** (e.g. ChatGPT, Google Gemini, Microsoft Copilot)
- **A private company** (e.g. a bank, retailer, social media platform, or AI company)
- **A government agency** (e.g. the IRS, health department, or police)

The levels of these attributes were selected to represent the most salient and relevant dimensions of privacy in the digital environment. Notably, data types and recipients relevant to social privacy were included, to explore a dimension of privacy that has not previously been empirically studied. The rise of AI assistant use adds a new dimension in blurring the distinction between a confidant and the product of a firm for some. This dual role makes them uniquely important to study in understanding how people value privacy today.

An additional attribute that was considered was the potential consequence of each scenario. However, consequences vary by lived experience, so this was excluded to prevent projecting irrelevant scenarios onto participants. Furthermore, the inclusion of consequences would have resulted in illogical combinations, such as the loss of friendship because your

identity data was leaked to a government agency.

Given three attributes with four levels each, the full factorial design of the DCE has 2016 possible pairs. With limitations on sample size and survey fatigue, the choice sets were chosen to maximise D-efficiency using Hole (2015). The minimum number of choice sets required was 16 to identify both main and interaction effects. However, to increase statistical precision while balancing potential survey fatigue, 24 choice sets were generated and randomised into two blocks of 12. The initial choice sets were constructed with zero priors, while the final choice sets used the priors from pilot results to increase the efficiency of the design.

3.1.2 Other survey questions

Participants were asked the same questions after the DCE tasks regardless of their randomised block. This included a series of questions on their top personal data concerns by consequence, data type, and recipient, with the latter two mirroring the attribute levels in the DCE. The ordering of options was randomised in each of these questions. Participants were also asked if they had ever been the victim of a personal data leak.

I collected information on participants' AI assistant use, and their most frequently used assistant from a randomised list, with the option to specify others. To understand how participants distinguish AI assistants and their firms, a series of six paired comparisons was included asking participants who they were more concerned about accessing their personal data: AI assistants or their parent firm. The order of these comparisons was randomised, as was the order of the names of the AI assistant and its parent. Participants were given options of equal concern, and opting out due to unfamiliarity with at least one of the options. Participants who reported no AI assistant use were directed to the final set of demographic questions.

Demographic questions collected information not available through Prolific, including social media use, highest level of education, employment status, relationship status, and annual

personal income. Participants were asked to report personal income instead of household income to align with the study’s privacy focus. The survey concluded with an open-ended question asking participants to define ‘data privacy’.

The median completion time was 6 minutes and 52 seconds for the US sample and 6 minutes and 27 seconds for the UK sample.

3.2 Quality checks

Representativeness Both samples targeted $N = 500$, but this was not met for the US sample, with places for males of mixed ethnicity aged 55-100 – one Independent and one Republican – were unable to be filled. There was only one place available in each of these cells.

Attention check An attention check was placed after the DCE tasks. The table format was identical to the layout in Figure 2, but with both data types as X, data recipients set as Y, and ransom as \$0, such that participants who were paying attention might immediately think that it was a survey error. Participants were instructed to select a third scenario ‘Scenario C’ that was not shown in the table. This was designed to prevent straightlining, that was a minor issue in piloting.

While straightlining could also reflect a participant’s actual preferences, none appeared in either sample. In the US, 46 participants were screened out by the attention check or timed out of the survey, and 30 in the UK. These participants were asked to return their submissions without completing the survey, such that their places could be offered to others to maintain representative samples.

3.3 Estimation

I model participants’ choices in the DCE using a random utility model (RUM), which assumes that decision makers choose the alternative from a discrete choice set that maximises their

utility. Utility is a function of the attribute levels of each alternative and an random error term.

In the context of the present DCE, individual i chooses from two alternatives $l \in \{A, B\}$. Each alternative is defined by a recipient j , a data type k , and a ransom amount c . The utility that i derives from alternative l is

$$U_{il} = V_{il} + \varepsilon_{il} ,$$

where V_{il} is systematic utility over observed attributes, and ε_{il} is random utility from unobserved attributes.

The probability that i chooses alternative A is

$$\begin{aligned} \mathbb{P}_{iA} &= \mathbb{P}(U_{iA} > U_{iB}) \\ &= \mathbb{P}(V_{iA} + \varepsilon_{iA} > V_{iB} + \varepsilon_{iB}) \\ &= \mathbb{P}(\varepsilon_{iA} - \varepsilon_{iB} > V_{iB} - V_{iA}) \end{aligned}$$

Under McFadden's choice model (McFadden 1974), these probabilities are estimated using conditional logit by

$$\mathbb{P}_{iA} = \frac{\exp(V_{iA})}{\exp(V_{iA}) + \exp(V_{iB})} .$$

The key assumption of this model is the independence of irrelevant alternatives (IIA) property – that adding or removing alternatives does not affect the relative probabilities of choosing the existing alternatives. In subsection 4.6, I show that relaxing this assumption does not materially change results.

Systematic utility, considering both main and interaction effects, is

$$V_{il} = \beta_1 c_{il} + \sum_{j=1}^3 \beta_2 \mathbf{1}\{j_{il} = j\} + \sum_{k=1}^3 \beta_3 \mathbf{1}\{k_{il} = k\} + \sum_{j=1}^3 \sum_{k=1}^3 \beta_4 \mathbf{1}\{j_{il} = j\} \mathbf{1}\{k_{il} = k\}.$$

Without loss of generality, willingness to pay to block the leaking of data type k to recipient j relative to a baseline of (j_0, k_0) can then be derived as

$$\text{WTP}(j, k) = \frac{\beta_2 + \beta_3 + \beta_4}{\beta_1}, \quad (1)$$

which is the empirical analogue to $-v_i(j, k)$ defined in Section 2.

4 What is Data Privacy Worth?

This section presents the first estimates of privacy under the consequence model, including valuations in social contexts that have not been previously studied empirically. As these willingness to pay (WTP) estimates are derived from the same DCE, they allow for direct comparison of how individuals value privacy in different contexts. I focus on the US sample unless otherwise stated.

4.1 Baseline preferences

Table 3 reports baseline conditional logit estimates for the US sample. The baseline model captures unconditional privacy preferences by data type and recipient. Browsing activity and someone close to you are used reference categories as the data type likely to be least sensitive, and the data recipient likely to be most trusted. The cost coefficient is negative and significant as expected, indicating that participants were less likely to prevent more expensive scenarios, though this effect is small.

Figure 3 translates preferences into WTP estimates implied by the regression coefficients using (1). By data type, individuals place the highest value on protecting identity data, with

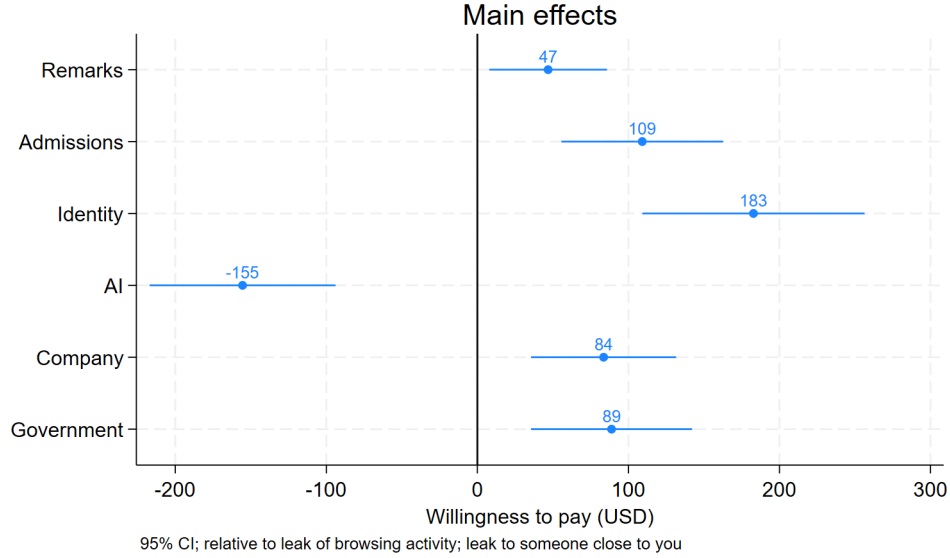


Figure 3: Willingness to Pay – Main effects

an average WTP of \$183 relative to browsing activity, followed by personal admissions and private remarks at \$109 and \$47. These results are all significant. The ordering is intuitive in reflecting the worst case scenario for each type of data leak. A leak of identity data can enable fraud or identity theft, and personal admissions can reveal secrets that could damage social or professional relationships. While the leaking of private remarks could result in similar harm to personal admissions, imaging shows that self-disclosure results in greater activity in the brain’s reward system than disclosures about others (Tamir & Mitchell 2012). This suggests that people perceive personal admissions as more central to their identity, and therefore more costly to have exposed. Finally, for the average person, one imagines that browsing activity would at most reveal embarrassing habits and preferences, rather than serious illegal activity.

With respect to recipients, individuals are willing to pay similar amounts to block leaks to government agencies (\$89) and companies (\$84) relative to someone close to them. Perhaps surprisingly, participants have a negative valuation for blocking leaks to AI assistants of -\$156. However, the negative WTP should not be interpreted as participants being willing to be paid for their personal data, but reflects that the disutility of disclosure is lower to AI

assistants relative to close personal contacts. One possible interpretation of this dynamic is that individuals view AI assistants as less socially consequential than human recipients, and retain control over AI conversations, reversing the dynamic individual-firm dynamic.

4.2 Context dependent preferences

Table 4 reports the regression results for data type and recipient interactions. The cost coefficient is negative and significant as expected, albeit small. These estimates indicate that, relative to browsing activity being leaked to a close contact, the odds of blocking a leak are contextual. These nuances are masked by average baseline preferences, which are misleading.

Figure 4 shows implied WTP estimates. Browsing activity is not considered to be sensitive to any data recipient, and particularly not to AI assistants, with individuals having a significantly negative WTP of $-\$110$. This suggests that targeted advertising, which makes use of browsing habits, is not considered particularly harmful, and helps explain why browsing history has been valued as low as $\$2.28$ (Savage & Waldman 2015). Only one per cent of participants indicated targeted ads or marketing as their top concern over a data leak. Understanding which aspects of privacy individuals care about more is important to informing the design and implementation of privacy regulation. For example, Dubé et al. (2025) find data-based personalised marketing is not necessarily harmful to consumers, but that privacy regulations may favour wealthier consumers and larger companies, and stifle innovation.

I provide the first empirical estimates of social privacy, which involves scenarios in which individuals value retaining information privacy from their social contacts. The results show that willingness to pay to prevent the leak of private remarks is driven by close contacts, with the average WTP of $\$155$ being significant. Thus, individuals value social privacy more than institutional privacy in certain circumstances. By comparison, the average WTP to prevent private remarks about government agencies from reaching them is not significantly different from zero, despite the power governments hold over citizens. One interpretation is that this

reflects the protection of free speech in democratic societies, where criticism of governmental institutions carries little cost. Similarly, individuals are not willing to pay positive amounts to prevent remarks from being diffused to firms or AI assistants. These findings reflect the relative damage of the potential consequences of the diffusion of this information by recipient. The diffusion of an offensive remark made behind a friend's back to them could damage that relationship, whereas it is unclear whether any consequence would result from such remarks made about institutional recipients, supporting the notion that the value of privacy is derived from the harm caused by losing it.

Similarly, individuals are willing to pay \$123 to avoid a personal admission being leaked to close contacts, and \$104 to government agencies, but not to firms or AI assistants. This positive and significant valuation on privacy from government here could reflect a desire to prevent self-incriminating information being shared, since the government has enforcement power. The relative magnitude of these valuations are consistent with individuals' reported concerns, with 12.9 per cent indicating that they were most concerned about the social consequences of a data leak, while 5.6 per cent indicated surveillance as their primary concern. By contrast, AI assistants and firms can do relatively little with personal admissions. The higher value individuals place on preventing private judgmental remarks being diffused to close contacts compared with personal admissions suggests that social relationships are valued more than judgment or personal embarrassment.

Individuals have the highest WTP to prevent the involuntary diffusion of identity data to firms, for which privacy is valued at \$256, and is the only data type individuals are sensitive about in relation to firms. This is consistent with individuals' stated concerns, with 61.2 per cent reporting security risks such as identity theft or fraud as the top data leak concern. Interestingly, despite the identity data being defined as details that are stored by government to provide public services, the WTP to prevent diffusion to government agencies is significant at \$125. This could reflect an aversion to data sharing between agencies, perhaps due to concerns about mission creep or misuse. Individuals are not sensitive to the diffusion of their

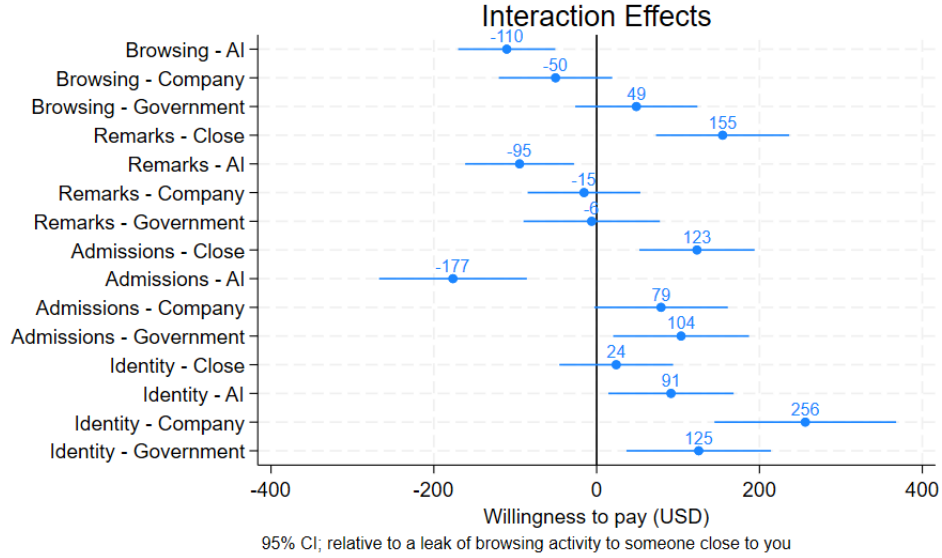


Figure 4: Willingness to Pay – Interaction effects

identity data to close contacts. Intuitively, identity data is likely to reveal little to trusted close contacts who may already have knowledge of it.

By contrast, identity data is the only data type for which individuals have a positive value for privacy from AI assistants that is significant at \$91, a preference that is masked by the baseline result. This suggests that individuals are still cautious of AI assistants being a product of the firms, though the difference between the point estimates is large. Individuals otherwise have a negative WTP for privacy from AI assistants across other data types. AI assistants may be considered relatively harmless since individuals are in control of AI conversations, and can delete memories or conversations at their will. The estimate for personal admissions of $-\$177$ particularly stands out in comparison to close contacts. This likely reflects the use of AI assistants as companions, which are considered to be less judgmental and more available than human companions (De Freitas, Oğuz-Uğuralp, Uğuralp & Puntoni 2025). AI blurs the distinction between social and institutional privacy, and is viewed as both a friend and a foe.

4.3 Reconciling the privacy paradox

These findings highlight the contextual dependence of privacy valuations. This multidimensionality is not captured by surveys simply asking individuals how much they care about privacy, treating it as monolithic. Individuals care strongly about privacy in certain circumstances, and little in others. By extending the empirical analysis to two new dimensions in social privacy and involuntary diffusion, I demonstrate that individuals do put substantial value on privacy in certain contexts, contrary to existing estimates. I reconcile the privacy paradox, showing strong stated privacy preferences are consistent with privacy valuations in certain dimensions. At the same time, these results also highlight that the privacy paradox is not a stable concept, and depends on how privacy is defined and measured.

4.4 Heterogeneity in privacy preferences

I find limited evidence on heterogeneity in privacy preferences under the consequence model of privacy. Consistent with Goldfarb & Tucker (2012), Acquisti et al. (2015), and Lin (2022), I find that privacy sensitivity increases in age, and that women tend to be more privacy sensitive, but I do not find significant differences based on income.

Table 5 reports regression results with an age interaction centered at the sample mean of 46 years. The interaction is significant on all data type and recipient pairs, with the exception of private judgmental remarks or identity data leaked to a close personal contact. Each additional year of age increases the odds of blocking a data type and recipient pair by up to 4.3 per cent, or \$12.20. In contrast to the findings in Goldfarb & Tucker (2012), older individuals tend to be more concerned about privacy in institutional contexts, especially from government agencies, rather than personal contacts. These differences could reflect the consideration of the involuntarily diffusion of data in this study, instead of assuming individuals have complete control over their data as in other studies.

Figure 5 shows the ordering of concern by data recipient for browsing activity as measured

by willingness to pay is unchanged by age. Younger individuals are not willing to pay to prevent their browsing activity being diffused regardless of the recipient, but the value individuals place on the privacy of their browsing activity eventually becomes positive for all recipients with age. The change in concern per additional year of age is highest for government agencies. Younger individuals on average are most concerned about private judgmental remarks being shared with close contacts, who are the category of recipient those aged 20 are willing to pay a positive amount to block diffusion. The age interaction on private judgmental remarks and close contacts is not significant, with government agencies, firms, and AI assistants being more concerning with each year of age in that order. By age 80, individuals are more concerned about government agencies and firms accessing their private judgmental remarks than close contacts on average, though they have a positive willingness to pay for all potential recipients. Personal admissions are the only data type that is significant when interacted with close contacts and age. The changes in the patterns of ordering by data recipient over age are the same as for private judgmental remarks. Similarly, younger individuals are least concerned about government agencies gaining access to their identity data, but become the second most concerning from around age 40 onwards.

Private judgmental remarks, and personal admissions are more likely to reveal personal opinions, or secrets than identity data, which largely comprises factual information. Thus, the involuntary diffusion of these data to close contacts are more likely to have social consequences, such as judgment, relationship deterioration, reputational loss, or embarrassment. The shift towards greater concern about institutional privacy away from social privacy with age could reflect how relationship characteristics change over time, with older individuals tend to have fewer but more stable and higher quality social relationships, reducing the potential consequences of data diffusion to close contacts (Carstensen 1992). Consistent with this, older individuals are more concerned about personal admissions being revealed to close contacts than private judgmental remarks suggests that they are more concerned about personal embarrassment or judgment than damaging relationships.

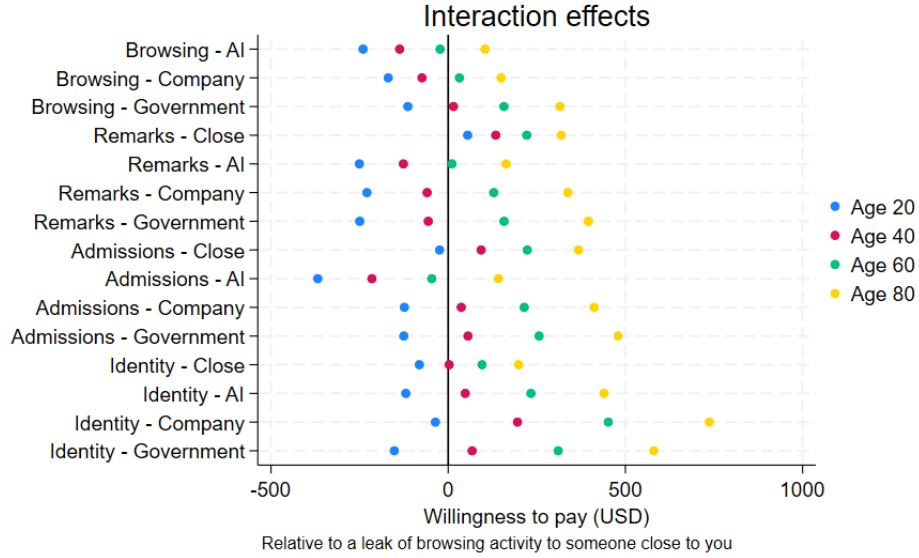


Figure 5: Willingness to Pay by Age (USD)

Focusing on differences by data type holding potential recipient, individuals are most concerned about identity data in relation to AI assistants and firms regardless of age. However, younger individuals are most concerned about protecting their browsing activity from government agencies than their identity data, while older individuals are consistently least concerned about their browsing activity regardless of potential recipient. These patterns could reflect internet use, with younger cohorts more likely to be online almost constantly.⁸

Table 6 reports regression results including an interaction term for sex. Males are generally less privacy sensitive than females, and are up to 52 percentage points less likely to prevent involuntary data diffusion. However, these differences are only significant with respect to the diffusion of private judgmental remarks to close contacts and government agencies, and personal admissions or identity data to government agencies. Notably, males are more cost sensitive in relation to privacy, being 0.3 percentage points less likely to block a data leak for each additional dollar it costs. Figure 6 shows the implied WTP estimates. The estimates for men are not significantly different from zero or are negative in most contexts, while women place positive value on protecting their data for most scenarios, particularly

⁸<https://pewrsr.ch/3JTxDUpN>.

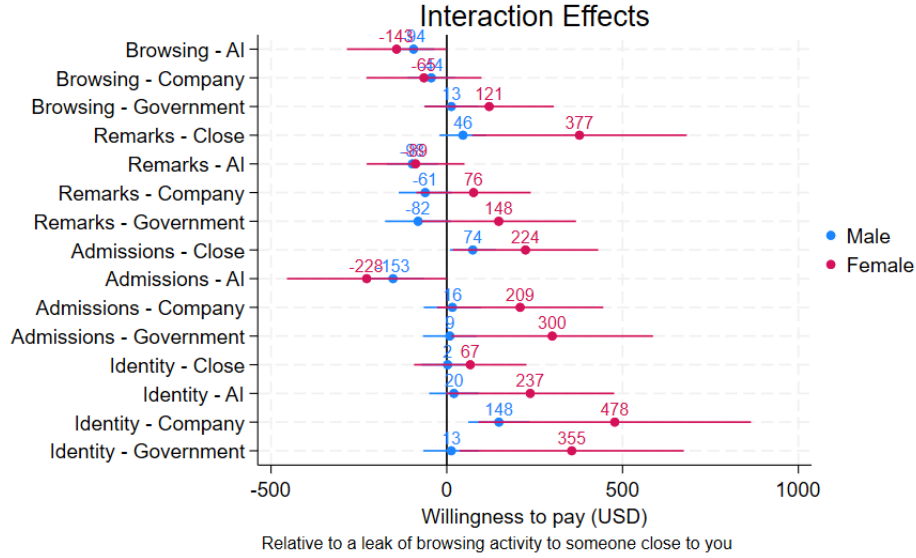


Figure 6: Willingness to Pay by Sex (USD)

in social contexts and the disclosure of identity data to institutions. For example, women are willing to pay \$377 to prevent private judgmental remarks from being leaked to someone close to them, but the valuation for men is not significantly different from zero. Women have higher privacy valuations on average in all contexts with the exception of browsing activity leaked to AI assistants or companies, and personal admissions leaked to AI assistants. Despite large differences in point estimates, the differences between the sexes are not significant due to large variance in the privacy preferences of females.

I also explore heterogeneity in privacy preferences by income, ethnicity, migrant status, political affiliation, relationship status, employment status, education, previous data breach experience, AI use, and social media use.⁹ There is limited evidence that privacy preferences vary significantly across subgroups within these variables, and no clear patterns emerge by data type or recipient.

The income interaction is negative for cost and for all firm and government combinations, and for AI assistants for browsing activity and personal admissions only. Though none of the income interactions are significant, the signs on the interactions may nevertheless appear

⁹The regression results are reported in Appendix B

to be counterintuitive. However, they are consistent to an extent with Lin (2022), who finds higher income individuals have lower instrumental privacy preferences – beliefs over how firms will use data – for income data. It is possible that this logic extends to other contexts, and higher income individuals may be less concerned about consequences stemming from the loss of privacy in institutional contexts. Another possible explanation for these results is the self-reporting of income, and inability to capture the upper tail of the income distribution in the study.

In the sample, 63 per cent of participants identify as white, with remaining participants spread across four ethnicity groups. I compare white and non white participants to ensure there is sufficient statistical power, and find limited differences by this split. Similarly, only five per cent of participants could be imputed as an upper bound on migrants based on country of birth, and there are no significant differences based on this interaction.

There are also few significant differences by political affiliation, which is representative of the US population. Independents and Republicans are significantly more concerned about privacy from AI assistants than Democrats over certain data types, they are 75 and 91 percentage points more likely to block private judgmental remarks from AI assistants. Independents are also 82 percentage points more likely to block identity data from AI assistants. The interactions on other data type and recipient combinations for Independents and Republicans are not significant, but are positive except in social contexts involving the diffusion of private judgmental remarks and personal admissions to close contacts. These findings suggest political affiliation has limited impact on privacy preferences.

There were no clear patterns by education or employment status. Employment status interactions appear to reflect age patterns, with students being consistently less willing to pay for privacy compared with those employed full time, and retirees consistently being more willing to pay.

In the US sample, 42 per cent of participants reported that they had previously been the victim of a data leak. The interaction for previous data breach victims was positive

on all data type and recipient combinations, as well as cost, as expected. However, it was only significant for personal admissions being diffused to AI assistants, with those previously having experienced a breach 64 percentage points more likely to block that scenario.

A large majority of participants indicated AI and social media use at 84 and 97 per cent of participants, limiting statistical power, though in both cases the sign of the interactions was negative for most scenarios, which is expected given the large amount of data disclosed using these services.

Overall, these findings reinforce the idea that privacy preferences are context dependent rather than driven by demographic factors.

4.5 Cross cultural comparison: US and UK

I pool the US and UK samples to test whether privacy preferences and valuations differ across countries. Table 7 reports regression results with an interaction for the UK. Participants from both countries have similar privacy preferences, with most country interactions being statistically indistinguishable from zero. British participants are significantly less likely to be concerned about the disclosure of their identity data to someone close to them, with 37 per cent lower odds. British participants also have 31 per cent lower odds of blocking their browsing activity from a government agency.

Figure 7 shows the implied WTP estimates. Differences in privacy valuations were not significant in any context. However, point estimates suggest that British participants were consistently less concerned about government than their American counterparts, and more sensitive about their browsing activity being leaked to a firm. These findings likely reflect differences in the focus of privacy laws. In the US, the right to privacy is grounded in the Constitution, and applies to freedom from governmental intrusion. By contrast, the GDPR in the UK focuses on data privacy from organisations, and is particularly salient for browsing activity given GDPR notice pop ups when browsing online.

Table 8 reports the regression results for UK participants by age. The signs on the age

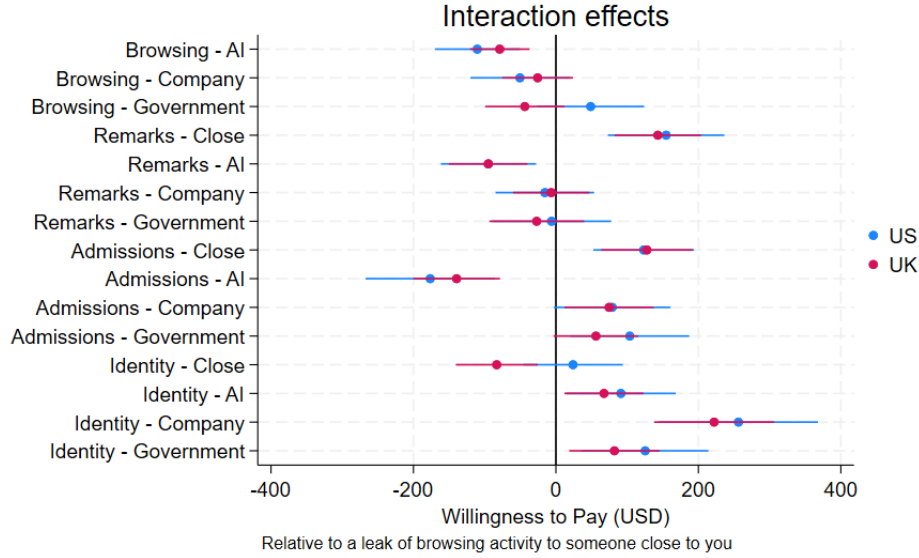


Figure 7: Willingness to Pay by Country

interactions are positive except for private judgmental remarks diffused to close contacts. This is consistent with the US results that show individuals become more privacy sensitive with age. However, unlike in the US, age differences are only significant in the institutionally relevant contexts of browsing activity or identity data diffused to firms or government agencies, but not in any social contexts. Older individuals are also less likely to pay to block data diffusion with each year of age, and this effect is significant, though very modest.

Table 9 reports regression results by sex. Consistent with US findings, the signs on the interactions suggest females are more privacy sensitive in every context, though not all coefficients are significant. The sign on the cost interaction is positive but not significant for males, in contrast to US results. Figure 8 transforms these results into willingness to pay estimates, which reinforce the lower privacy concern in relation to government agencies compared with firms in the UK observed in the aggregate estimates. Differences between the sexes are less pronounced in social contexts than in the US, but more pronounced in relation to AI assistants.

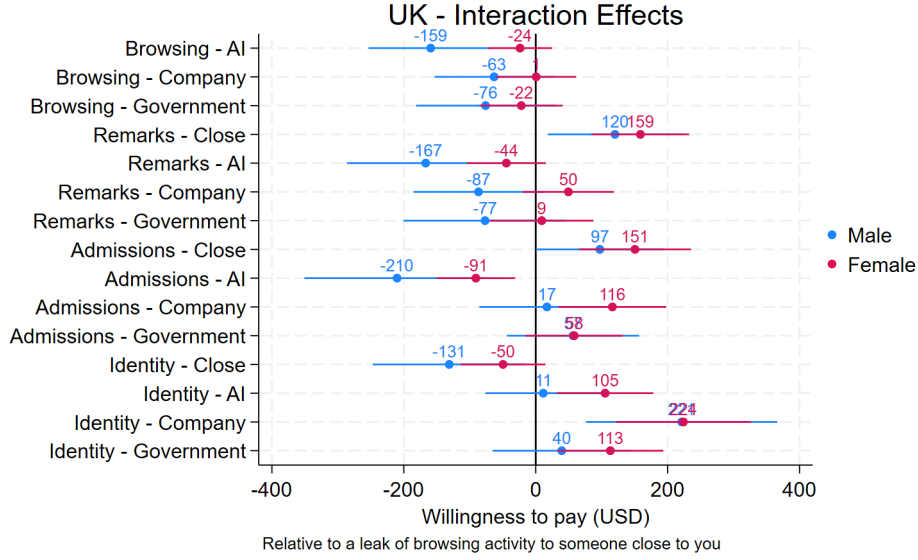


Figure 8: UK – Willingness to Pay by Sex (USD)

4.6 Robustness checks

Alternative specifications I compare the conditional logit specification with a mixed logit specification to relax the IIA assumption by allowing random coefficients. Table 10 reports the results allowing all coefficients to be random in the baseline unconditional specification. The signs, significance, and ordering of the coefficients are consistent between the conditional logit and mixed logit specifications, leading to the same substantive conclusions.¹⁰

The magnitude of the coefficients from the mixed logit specification are larger, with the exception of the cost coefficient. The implied WTP estimates are slightly larger in magnitude compared with the estimates from the conditional logit, with the exception of personal admissions. The standard errors are larger in the mixed logit specification.

As the substantive conclusions of the two models are the same, the conditional logit specification was preferred for its simplicity, lower variability, and more conservative estimates.

Trade offs As a robustness check on the DCE design itself, I examine whether participants systematically favoured certain attribute levels across choice tasks. Table ?? shows

¹⁰The interactions model does not converge under a mixed logit specification.

that choices were broadly distributed across levels for each attribute. The ordering of the frequency of choices by data type is consistent with privacy preferences and valuations from the unconditional baseline model, with identity data being most frequently protected. By data recipient, AI assistants were least frequently chosen, consistent with the unconditional baseline model, while close personal contacts were most frequently chosen – a departure from those results. This reinforces the importance of context in privacy decisions over personal data. The highest cost option was least frequently chosen, though cost choices were otherwise fairly evenly distributed. Choices were also fairly evenly distributed across choice sets, suggesting that none were strictly dominant or dominated.

These patterns suggest that participants were not defaulting to any single attribute level, and were making tradeoffs across attributes, consistent with the DCE design.

Limitations Privacy is a sensitive topic, and self selection into or out of the survey is a potential concern. All participants were recruited via Prolific, which requires registrants to provide demographic information at sign up. Ironically, this requirement likely results in bias of the sample towards individuals with relatively weaker privacy preferences and valuations, given their willingness to share personal details as a condition of platform use. Moreover, all participants completed the survey online, meaning individuals who do not use the internet are not represented. While this excludes a small segment of the population, the focus of this study on digital data makes online participants a reasonable target population.

Statistical power was limited by sample size, particularly for subgroup analyses of conditional models where estimates were noisier. Nonetheless, the patterns identified were broadly consistent across specifications and robustness checks, supporting the validity of the core findings.

As with all discrete choice experiments, the design has inherent limitations. While the hypothetical nature of the scenarios has the advantage of measuring privacy preferences without requiring participants to disclose any of the data types studied, their decisions

decisions may not fully replicate real world behaviour.

The framing of DCE scenarios was necessarily stylised and deliberately vague. For example, a personal admission being leaked to a close personal contact could range from the revelation of a relatively harmless habit that could lead to embarrassment, to a more damaging revelation such as illegal activity. These would be expected to be valued very differently. However, it was not feasible to specify precise examples without making scenarios likely becoming irrelevant to many participants or substantially reducing statistical power. Instead, data types and recipients were defined broadly, with prompts for participants to project their own interpretations based on their subjective experiences. Hence, the estimates likely capture more granular dimensions of privacy than were explicitly studied.

The ransom framing without given participants a budget constraint could have made trade offs less consequential. However, robustness checks suggest that participants did make meaningful trade offs across attributes, and that the results reflect genuine preferences and valuations.

As with all surveys, social desirability bias may have influenced responses, though the anonymity of responses would likely have mitigated this to an extent. The study was conducted in the US and UK, which are both advanced digital economies. While the limited differences between the privacy preferences and valuations between these two economies suggest the findings may be generalised to other advanced digital economies, the external validity of the results to countries with different cultural norms, regulatory regimes, institutional trust, and levels of digitisation is unclear.

While these limitations mean that point estimates should be interpreted with caution, they do not undermine the core findings, the consistency of results across specifications suggests that the main conclusions of the study are robust.

5 AI: Friend and Foe?

The DCE results reveal a new puzzle: individuals appear to treat AI as both a friend and a foe. Individuals are systematically less concerned about privacy from AI assistants than close contacts (with the exception of identity data), and firms. This is despite AI companies being listed as an example of a company in the DCE. On average, participants assign a negative WTP of $-\$156$ to blocking their data from AI assistants unconditionally, and only have a positive WTP of $\$91$ for identity data. By contrast, participants are willing to pay $\$84$ to block their data from a company unconditionally. This valuation increases to $\$256$ when conditioning on identity data. Willingness to pay for privacy from firms is higher for every data type than from AI assistants. Stated concerns reinforce this pattern: 45 per cent of participants named companies as the data leak recipient of most concern, compared with nine per cent for AI assistants.

To test whether this puzzle arises from the grouping of AI companies within companies more broadly, I include a series of AI-specific questions for participants who indicate AI assistant use. This captures 417 participants, equivalent to 84 per cent of the US sample. Each participant reported their most used AI assistant, and then answered a series of six comparisons between specific AI assistant and parent company pairs, indicating which they were more concerned about. Unlike the DCE tasks, participants were able to select ‘equally concerned’ or indicate that they had not heard of at least one of the options.

OpenAI’s ChatGPT was the most commonly used AI assistant, accounting for 67 per cent of AI assistant users in the US. This was followed by Google Gemini and Microsoft Copilot at 15 per cent and nine per cent. xAI’s Grok and Anthropic’s Claude followed with 2-4 per cent. No participants indicated that Meta’s Llama was their most used AI assistant, while those who chose other were most likely to use DeepSeek.

Table 1 shows who participants would be most concerned about being able to access their data by each AI assistant-company pair. In the absence of forced choice, between 42 and 79 per cent of AI users indicated equal concern. However, participants were otherwise

Table 1: AI Assistant and Company Concerns

%	ChatGPT	Claude	Copilot	Gemini	Grok	Llama	Total
AI assistant	8.36	6.93	5.14	5.02	3.58	2.03	5.18
AI company	9.80	4.06	16.61	21.03	18.76	36.92	17.86
Equally concerned	78.61	43.13	72.52	72.04	53.88	42.77	60.49
Not familiar	3.23	45.88	5.73	1.91	23.78	18.28	16.47

consistently more concerned about the AI company than its AI assistant.¹¹ This gap is especially pronounced for diversified technology firms. Overall, 19 per cent of participants indicated that they were equally concerned in all six comparisons, while 80 per cent of participants never chose an AI assistant as being more concerning, compared with 52 per cent for AI companies. It is unclear whether participants who reported equal concern did so because they recognised them as the same entity, or due to an intrinsic preference for privacy since they were not required to make a trade off as in the DCE tasks. Exploring the AI puzzle using a DCE could provide more evidence in this regard.

To formally test the AI puzzle, I restrict the sample to responses in which participants had heard of both the AI assistant and company in each pair, and could make an informed decision. This captures 88 per cent of responses across 417 participants. I combine responses of equal concern greater concern over companies in an indicator variable for company concern equal to one, and zero when the assistant is more concerning. I test whether the puzzle is stronger for diversified ‘Big Tech’ firms (Google, Microsoft, Meta, xAI), compared with AI focused firms (Anthropic, OpenAI).¹²

Table 2 reports logistic regression results. In both the main and extension specifications, the constant and Big Tech coefficients are significant. In both cases, the results imply a probability of being at least as concerned about an AI company than its AI assistant of 93 per cent. This increases by 5 percentage points for Big Tech companies. It is possible that greater familiarity with companies than their AI assistants contributed to the finding

¹¹Anthropic’s Claude is an exception, but this is likely due to its limited recognition in the sample.

¹²While xAI is an AI company, it was grouped with other diversified technology firms as its subsidiary X Corp. owns the X social media platform.

Table 2: AI Puzzle

	(1) Main	(2) Average Marginal Effects	(3) Extension	(4) Average Marginal Effects
Big Tech	0.83*** (0.16)	0.05*** (0.01)	0.83*** (0.16)	0.05*** (0.01)
Age			0.01 (0.01)	0.00 (0.00)
Male			-0.16 (0.22)	-0.01 (0.01)
Constant	2.13*** (0.13)		2.40*** (0.35)	
Observations	2,194	2,194	2,194	2,194

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

that the AI puzzle is stronger for established technology companies, especially those with high profile data privacy scandals (e.g. the Facebook-Cambridge Analytica scandal). Age centered at the sample mean and sex do not have a significant effect as they did in the broader privacy study. Age is not a significant predictor of AI use, which is broadly similar across the age spectrum, though more intensely used by younger cohorts. By contrast, sex is a significant predictor of AI use, with the probability of AI use being 9.8 per cent higher for males.

The AI puzzle raises a regulatory dilemma. On one hand, participants show little concern about AI assistants, suggesting regulation should not impose protections that consumers do not value. On the other hand, individuals may underestimate risks because they misperceive assistants as independent confidants rather than products of firms, or because they misunderstand the applicable data policies or regulations. This is highlighted by the absence of legal privilege for AI assistant conversations, especially when used as substitutes for professional services such as legal assistance or therapy, as was noted by OpenAI CEO Sam Altman.¹³

¹³<https://www.ft.com/content/31e528b3-9800-4743-af0a-f5c3b80032d0>.

Regulation should therefore address awareness and default protections, particularly for sensitive contexts. For firms, the AI paradox shows that product design can meaningfully change consumers’ disclosure preferences. The humanlike characteristics of AI assistants appears to reduce perceived privacy risks, or at least increases the benefit of personal data disclosures. Embedding AI assistants into platforms may therefore increase customer engagement and data flows to take advantage of the apparent dual identity that an AI assistant can bring its parent company.

6 Conclusion

This paper develops a framework for understanding how individuals make tradeoffs between different dimensions of privacy, and provides the first empirical estimates of these multidimensional preferences. I show that privacy derives its value from the consequences of involuntary data diffusion, rather than control over voluntary disclosures. Individuals often value privacy from close social contacts as much as privacy from firms or governments, despite regulatory focus on the latter. This framework and evidence reconciles the ‘privacy paradox’. Apparent inconsistencies between individuals’ stated privacy preferences and behaviour reflect differing contexts, not contradictions. I highlight how emerging technologies can challenge social and institutional boundaries, and document the existence of an AI privacy puzzle: individuals are systematically less concerned about privacy from AI assistants than from the companies that develop them, and often their close contacts. Understanding the drivers of this puzzle presents an interesting question for future research. These results establish a foundation for understanding privacy as a multidimensional concept, and offer guidance for more effective regulation, AI governance, and product design.

A Appendix

A.1 Data privacy meaning prompt

This version of the prompt resulted from an iterative process that included manual cross-checks to ensure appropriate categorisation.

Categorise these responses by the following mental models of data privacy they match most closely:

1. Control/ownership: data privacy means I own my data and/or control who sees it. People can only access my data with my consent or permission
2. Protection: data privacy means that data that I have shared is secure and protected from third parties
3. Consequence: data privacy is defined in the negative as when certain consequences don't happen (e.g. identity theft, hack, leak, selling of data)
4. Non-existence: data privacy does not exist
5. Information type: data privacy has been defined by listing specific information types
6. Privacy: circular responses that mention 'private' or 'privacy' without sufficient context to fit into other categories (e.g. data that is private)
7. Uncategorized: vague or uninterpretable responses

If a response fits into multiple categories, assign to the dominant category, and if there is no dominant category, the category first mentioned.

A.2 Regression results

Table 3: US – Main Effects

	(1) Conditional logit	(2) Odds ratio
Browsing activity	0 (.)	1 (.)
Private judgmental remarks	0.164** (2.67)	1.178** (2.67)
Personal admissions	0.381*** (5.62)	1.464*** (5.62)
Identity data	0.639*** (9.66)	1.894*** (9.66)
Someone close to you	0 (.)	1 (.)
AI assistant	-0.543*** (-8.79)	0.581*** (-8.79)
Company	0.292*** (3.95)	1.339*** (3.95)
Government	0.311*** (3.83)	1.364*** (3.83)
Cost	-0.00349*** (-5.70)	0.997*** (-5.70)
Observations	11952	11952
Pseudo R^2	0.042	0.042

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 4: US – Interaction Effects

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 (.)	1 (.)
Browsing activity $\times$ AI assistant	-0.387*** (-4.13)	0.679*** (-4.13)
Browsing activity $\times$ Company	-0.177 (-1.50)	0.838 (-1.50)
Browsing activity $\times$ Government	0.171 (1.28)	1.186 (1.28)
Private judgmental remarks $\times$ Someone close to you	0.542*** (5.04)	1.720*** (5.04)
Private judgmental remarks $\times$ AI assistant	-0.332** (-3.06)	0.718** (-3.06)
Private judgmental remarks $\times$ Company	-0.0542 (-0.44)	0.947 (-0.44)
Private judgmental remarks $\times$ Government	-0.0214 (-0.14)	0.979 (-0.14)
Personal admissions $\times$ Someone close to you	0.432*** (4.46)	1.540*** (4.46)
Personal admissions $\times$ AI assistant	-0.618*** (-5.30)	0.539*** (-5.30)
Personal admissions $\times$ Company	0.277* (1.99)	1.319* (1.99)
Personal admissions $\times$ Government	0.363** (2.71)	1.438** (2.71)
Identity data $\times$ Someone close to you	0.0842 (0.68)	1.088 (0.68)
Identity data $\times$ AI assistant	0.320** (2.62)	1.377** (2.62)
Identity data $\times$ Company	0.898*** (6.72)	2.455*** (6.72)
Identity data $\times$ Government	0.439** (3.18)	1.552** (3.18)
Cost	-0.00350*** (-5.55)	0.997*** (-5.55)
Observations	11952	11952
Pseudo R^2	0.056	0.056

 t statistics in parentheses* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 5: US – Age

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.381*** (-4.01)	0.683*** (-4.01)
Browsing activity $\times$ Company	-0.166 (-1.38)	0.847 (-1.38)
Browsing activity $\times$ Government	0.180 (1.33)	1.197 (1.33)
Private judgmental remarks $\times$ Someone close to you	0.552*** (5.00)	1.737*** (5.00)
Private judgmental remarks $\times$ AI assistant	-0.323** (-2.95)	0.724** (-2.95)
Private judgmental remarks $\times$ Company	-0.0414 (-0.33)	0.959 (-0.33)
Private judgmental remarks $\times$ Government	-0.00646 (-0.04)	0.994 (-0.04)
Personal admissions $\times$ Someone close to you	0.445*** (4.54)	1.561*** (4.54)
Personal admissions $\times$ AI assistant	-0.608*** (-5.18)	0.544*** (-5.18)
Personal admissions $\times$ Company	0.289* (2.06)	1.336* (2.06)
Personal admissions $\times$ Government	0.377** (2.81)	1.458** (2.81)
Identity data $\times$ Someone close to you	0.0930 (0.74)	1.097 (0.74)
Identity data $\times$ AI assistant	0.336** (2.68)	1.399** (2.68)
Identity data $\times$ Company	0.920*** (6.88)	2.509*** (6.88)
Identity data $\times$ Government	0.456*** (3.31)	1.578*** (3.31)
Browsing activity $\times$ AI assistant $\times$ Age	0.0206*** (3.49)	1.021*** (3.49)
Browsing activity $\times$ Company $\times$ Age	0.0186* (2.38)	1.019* (2.38)
Browsing activity $\times$ Government $\times$ Age	0.0240** (2.74)	1.024** (2.74)
Private judgmental remarks $\times$ Someone close to you $\times$ Age	0.0137	1.014

	(1.93)	(1.93)
Private judgmental remarks $\times$ AI assistant $\times$ Age	0.0244*** (3.50)	1.025*** (3.50)
Private judgmental remarks $\times$ Company $\times$ Age	0.0325*** (4.09)	1.033*** (4.09)
Private judgmental remarks $\times$ Government $\times$ Age	0.0368*** (3.95)	1.038*** (3.95)
Personal admissions $\times$ Someone close to you $\times$ Age	0.0212*** (3.40)	1.021*** (3.40)
Personal admissions $\times$ AI assistant $\times$ Age	0.0306*** (3.98)	1.031*** (3.98)
Personal admissions $\times$ Company $\times$ Age	0.0298*** (3.34)	1.030*** (3.34)
Personal admissions $\times$ Government $\times$ Age	0.0335*** (4.04)	1.034*** (4.04)
Identity data $\times$ Someone close to you $\times$ Age	0.0158 (1.90)	1.016 (1.90)
Identity data $\times$ AI assistant $\times$ Age	0.0311*** (3.78)	1.032*** (3.78)
Identity data $\times$ Company $\times$ Age	0.0418*** (4.94)	1.043*** (4.94)
Identity data $\times$ Government $\times$ Age	0.0406*** (4.83)	1.041*** (4.83)
Cost	-0.00353*** (-5.51)	0.996*** (-5.51)
Cost $\times$ Age	0.00000900 (0.21)	1.000 (0.21)
Observations	11952	11952
Pseudo R^2	0.064	0.064

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 6: US – Sex (female baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.324* (-2.42)	0.723* (-2.42)
Browsing activity $\times$ Company	-0.147 (-0.83)	0.863 (-0.83)
Browsing activity $\times$ Government	0.274 (1.43)	1.315 (1.43)
Private judgmental remarks $\times$ Someone close to you	0.857*** (5.73)	2.356*** (5.73)
Private judgmental remarks $\times$ AI assistant	-0.201 (-1.33)	0.818 (-1.33)
Private judgmental remarks $\times$ Company	0.173 (1.00)	1.189 (1.00)
Private judgmental remarks $\times$ Government	0.335 (1.59)	1.399 (1.59)
Personal admissions $\times$ Someone close to you	0.508*** (3.80)	1.663*** (3.80)
Personal admissions $\times$ AI assistant	-0.517** (-2.95)	0.596** (-2.95)
Personal admissions $\times$ Company	0.474* (2.44)	1.606* (2.44)
Personal admissions $\times$ Government	0.681*** (3.55)	1.975*** (3.55)
Identity data $\times$ Someone close to you	0.152 (0.87)	1.164 (0.87)
Identity data $\times$ AI assistant	0.539** (3.02)	1.714** (3.02)
Identity data $\times$ Company	1.085*** (5.65)	2.959*** (5.65)
Identity data $\times$ Government	0.807*** (4.11)	2.241*** (4.11)
Browsing activity $\times$ AI assistant $\times$ Male	-0.129 (-0.68)	0.879 (-0.68)
Browsing activity $\times$ Company $\times$ Male	-0.0648 (-0.27)	0.937 (-0.27)
Browsing activity $\times$ Government $\times$ Male	-0.212 (-0.79)	0.809 (-0.79)
Private judgmental remarks $\times$ Someone close to you $\times$ Male	-0.636**	0.529**

	(-2.95)	(-2.95)
Private judgmental remarks $\times$ AI assistant $\times$ Male	-0.267 (-1.23)	0.765 (-1.23)
Private judgmental remarks $\times$ Company $\times$ Male	-0.467 (-1.89)	0.627 (-1.89)
Private judgmental remarks $\times$ Government $\times$ Male	-0.727* (-2.43)	0.483* (-2.43)
Personal admissions $\times$ Someone close to you $\times$ Male	-0.153 (-0.79)	0.858 (-0.79)
Personal admissions $\times$ AI assistant $\times$ Male	-0.216 (-0.92)	0.805 (-0.92)
Personal admissions $\times$ Company $\times$ Male	-0.397 (-1.42)	0.672 (-1.42)
Personal admissions $\times$ Government $\times$ Male	-0.639* (-2.38)	0.528* (-2.38)
Identity data $\times$ Someone close to you $\times$ Male	-0.140 (-0.56)	0.869 (-0.56)
Identity data $\times$ AI assistant $\times$ Male	-0.442 (-1.79)	0.643 (-1.79)
Identity data $\times$ Company $\times$ Male	-0.373 (-1.40)	0.689 (-1.40)
Identity data $\times$ Government $\times$ Male	-0.746** (-2.70)	0.474** (-2.70)
Cost	-0.00227** (-2.63)	0.998** (-2.63)
Male $\times$ Cost	-0.00253* (-1.99)	0.997* (-1.99)
Observations	11952	11952
Pseudo R^2	0.061	0.061

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 7: US and UK – Interaction Effects (US baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.387*** (-4.13)	0.679*** (-4.13)
Browsing activity $\times$ Company	-0.177 (-1.50)	0.838 (-1.50)
Browsing activity $\times$ Government	0.171 (1.28)	1.186 (1.28)
Private judgmental remarks $\times$ Someone close to you	0.542*** (5.04)	1.720*** (5.04)
Private judgmental remarks $\times$ AI assistant	-0.332** (-3.06)	0.718** (-3.06)
Private judgmental remarks $\times$ Company	-0.0542 (-0.44)	0.947 (-0.44)
Private judgmental remarks $\times$ Government	-0.0214 (-0.14)	0.979 (-0.14)
Personal admissions $\times$ Someone close to you	0.432*** (4.46)	1.540*** (4.46)
Personal admissions $\times$ AI assistant	-0.618*** (-5.31)	0.539*** (-5.31)
Personal admissions $\times$ Company	0.277* (1.99)	1.319* (1.99)
Personal admissions $\times$ Government	0.363** (2.72)	1.438** (2.72)
Identity data $\times$ Someone close to you	0.0842 (0.68)	1.088 (0.68)
Identity data $\times$ AI assistant	0.320** (2.62)	1.377** (2.62)
Identity data $\times$ Company	0.898*** (6.72)	2.455*** (6.72)
Identity data $\times$ Government	0.439** (3.19)	1.552** (3.19)
Browsing activity $\times$ AI assistant $\times$ UK	0.0226 (0.17)	1.023 (0.17)
Browsing activity $\times$ Company $\times$ UK	0.0583 (0.35)	1.060 (0.35)
Browsing activity $\times$ Government $\times$ UK	-0.373* (-2.02)	0.689* (-2.02)
Private judgmental remarks $\times$ Someone close to you $\times$ UK	0.119	1.126

	(0.78)	(0.78)
Private judgmental remarks $\times$ AI assistant $\times$ UK	-0.107 (-0.66)	0.898 (-0.66)
Private judgmental remarks $\times$ Company $\times$ UK	0.0237 (0.13)	1.024 (0.13)
Private judgmental remarks $\times$ Government $\times$ UK	-0.103 (-0.48)	0.902 (-0.48)
Personal admissions $\times$ Someone close to you $\times$ UK	0.159 (1.06)	1.172 (1.06)
Personal admissions $\times$ AI assistant $\times$ UK	-0.0255 (-0.15)	0.975 (-0.15)
Personal admissions $\times$ Company $\times$ UK	0.0681 (0.34)	1.071 (0.34)
Personal admissions $\times$ Government $\times$ UK	-0.104 (-0.55)	0.901 (-0.55)
Identity data $\times$ Someone close to you $\times$ UK	-0.468** (-2.61)	0.626** (-2.61)
Identity data $\times$ AI assistant $\times$ UK	-0.00803 (-0.05)	0.992 (-0.05)
Identity data $\times$ Company $\times$ UK	0.128 (0.66)	1.137 (0.66)
Identity data $\times$ Government $\times$ UK	-0.0598 (-0.31)	0.942 (-0.31)
Cost	-0.00350*** (-5.55)	0.997*** (-5.55)
UK $\times$ Cost	-0.00112 (-1.24)	0.999 (-1.24)
Observations	23952	23952
Pseudo R^2	0.069	0.069

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 8: UK – Age

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.368*** (-3.93)	0.692*** (-3.93)
Browsing activity $\times$ Company	-0.112 (-0.97)	0.894 (-0.97)
Browsing activity $\times$ Government	-0.206 (-1.60)	0.814 (-1.60)
Private judgmental remarks $\times$ Someone close to you	0.667*** (6.03)	1.948*** (6.03)
Private judgmental remarks $\times$ AI assistant	-0.440*** (-3.65)	0.644*** (-3.65)
Private judgmental remarks $\times$ Company	-0.0264 (-0.21)	0.974 (-0.21)
Private judgmental remarks $\times$ Government	-0.129 (-0.82)	0.879 (-0.82)
Personal admissions $\times$ Someone close to you	0.594*** (5.13)	1.812*** (5.13)
Personal admissions $\times$ AI assistant	-0.647*** (-5.50)	0.523*** (-5.50)
Personal admissions $\times$ Company	0.340* (2.38)	1.404* (2.38)
Personal admissions $\times$ Government	0.257 (1.91)	1.293 (1.91)
Identity data $\times$ Someone close to you	-0.378** (-2.90)	0.685** (-2.90)
Identity data $\times$ AI assistant	0.311** (2.67)	1.365** (2.67)
Identity data $\times$ Company	1.055*** (7.41)	2.871*** (7.41)
Identity data $\times$ Government	0.379** (2.74)	1.461** (2.74)
Browsing activity $\times$ AI assistant $\times$ Age	0.00143 (0.24)	1.001 (0.24)
Browsing activity $\times$ Company $\times$ Age	0.0236** (3.10)	1.024** (3.10)
Browsing activity $\times$ Government $\times$ Age	0.0212* (2.53)	1.021* (2.53)
Private judgmental remarks $\times$ Someone close to you $\times$ Age	-0.00138	0.999

	(-0.20)	(-0.20)
Private judgmental remarks $\times$ AI assistant $\times$ Age	0.00778 (0.98)	1.008 (0.98)
Private judgmental remarks $\times$ Company $\times$ Age	0.00860 (1.14)	1.009 (1.14)
Private judgmental remarks $\times$ Government $\times$ Age	0.0137 (1.43)	1.014 (1.43)
Personal admissions $\times$ Someone close to you $\times$ Age	0.00665 (0.94)	1.007 (0.94)
Personal admissions $\times$ AI assistant $\times$ Age	0.0122 (1.58)	1.012 (1.58)
Personal admissions $\times$ Company $\times$ Age	0.0149 (1.62)	1.015 (1.62)
Personal admissions $\times$ Government $\times$ Age	0.0127 (1.49)	1.013 (1.49)
Identity data $\times$ Someone close to you $\times$ Age	0.0189* (2.18)	1.019* (2.18)
Identity data $\times$ AI assistant $\times$ Age	0.0144 (1.93)	1.015 (1.93)
Identity data $\times$ Company $\times$ Age	0.0363*** (4.04)	1.037*** (4.04)
Identity data $\times$ Government $\times$ Age	0.0264** (2.93)	1.027** (2.93)
Cost	-0.00470*** (-7.27)	0.995*** (-7.27)
Cost $\times$ Age	-0.0000925* (-2.36)	1.000* (-2.36)
Observations	12000	12000
Pseudo R^2	0.088	0.088

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 9: UK – Sex (female baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.130 (-0.95)	0.878 (-0.95)
Browsing activity $\times$ Company	0.00381 (0.02)	1.004 (0.02)
Browsing activity $\times$ Government	-0.119 (-0.68)	0.888 (-0.68)
Private judgmental remarks $\times$ Someone close to you	0.866*** (5.67)	2.377*** (5.67)
Private judgmental remarks $\times$ AI assistant	-0.243 (-1.45)	0.784 (-1.45)
Private judgmental remarks $\times$ Company	0.270 (1.49)	1.310 (1.49)
Private judgmental remarks $\times$ Government	0.0498 (0.23)	1.051 (0.23)
Personal admissions $\times$ Someone close to you	0.821*** (4.59)	2.274*** (4.59)
Personal admissions $\times$ AI assistant	-0.495** (-3.07)	0.609** (-3.07)
Personal admissions $\times$ Company	0.634** (3.14)	1.886** (3.14)
Personal admissions $\times$ Government	0.319 (1.64)	1.375 (1.64)
Identity data $\times$ Someone close to you	-0.270 (-1.49)	0.763 (-1.49)
Identity data $\times$ AI assistant	0.575*** (3.54)	1.776*** (3.54)
Identity data $\times$ Company	1.223*** (5.97)	3.396*** (5.97)
Identity data $\times$ Government	0.618** (3.18)	1.855** (3.18)
Browsing activity $\times$ AI assistant $\times$ Male	-0.473* (-2.51)	0.623* (-2.51)
Browsing activity $\times$ Company $\times$ Male	-0.243 (-1.03)	0.784 (-1.03)
Browsing activity $\times$ Government $\times$ Male	-0.169 (-0.66)	0.845 (-0.66)
Private judgmental remarks $\times$ Someone close to you $\times$ Male	-0.411	0.663

	(-1.87)	(-1.87)
Private judgmental remarks $\times$ AI assistant $\times$ Male	-0.389 (-1.60)	0.678 (-1.60)
Private judgmental remarks $\times$ Company $\times$ Male	-0.599* (-2.36)	0.550* (-2.36)
Private judgmental remarks $\times$ Government $\times$ Male	-0.341 (-1.08)	0.711 (-1.08)
Personal admissions $\times$ Someone close to you $\times$ Male	-0.453 (-1.95)	0.636 (-1.95)
Personal admissions $\times$ AI assistant $\times$ Male	-0.301 (-1.27)	0.740 (-1.27)
Personal admissions $\times$ Company $\times$ Male	-0.570* (-2.01)	0.565* (-2.01)
Personal admissions $\times$ Government $\times$ Male	-0.104 (-0.39)	0.901 (-0.39)
Identity data $\times$ Someone close to you $\times$ Male	-0.226 (-0.86)	0.797 (-0.86)
Identity data $\times$ AI assistant $\times$ Male	-0.531* (-2.28)	0.588* (-2.28)
Identity data $\times$ Company $\times$ Male	-0.384 (-1.35)	0.681 (-1.35)
Identity data $\times$ Government $\times$ Male	-0.468 (-1.68)	0.626 (-1.68)
Cost	-0.00546*** (-6.36)	0.995*** (-6.36)
Male $\times$ Cost	0.00167 (1.30)	1.002 (1.30)
Observations	12000	12000
Pseudo R^2	0.086	0.086

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

A.3 Robustness checks

Table 10: US – Robustness

	(1) Conditional logit	(2) Mixed logit
Browsing activity	0 -	0 -
Private judgmental remarks	0.164** (2.67)	0.270** (2.87)
Personal admissions	0.381*** (5.62)	0.545*** (5.07)
Identity data	0.639*** (9.66)	1.021*** (9.33)
Someone close to you	0 -	0 -
AI assistant	-0.543*** (-8.79)	-0.867*** (-7.79)
Company	0.292*** (3.95)	0.510*** (4.52)
Government	0.311*** (3.83)	0.509*** (4.23)
Cost	-0.00349*** (-5.70)	-0.00544*** (-4.89)
Observations	11952	11952
Pseudo R^2	0.042	

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 11: Frequency of Chosen Attribute Levels

Data type	%	Recipient	%	Ransom	%
Browsing activity	21.82	Someone close to you	27.56	\$10	25.52
Private judgmental remarks	23.36	AI assistant	21.40	\$30	24.98
Personal admissions	25.62	Company	25.52	\$70	27.74
Identity data	29.20	Government	25.52	\$120	21.75

References

- Acquisti, A. (2024), The Economics of Privacy at a Crossroads, in ‘The Economics of Privacy’, University of Chicago Press, pp. 21–72.
- Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015), ‘Privacy and Human Behavior in the Age of Information’, *Science* **347**(6221), 509–514.
- Acquisti, A., Brandimarte, L. & Loewenstein, G. (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, A., John, L. K. & Loewenstein, G. (2013), ‘What is Privacy Worth?’, *The Journal of Legal Studies* **42**(2), 249–274.
- Acquisti, A., Taylor, C. & Wagman, L. (2016), ‘The Economics of Privacy’, *Journal of Economic Literature* **54**(2), 442–492.
- Athey, S., Catalini, C. & Tucker, C. (2017), The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, Working Paper 23488, National Bureau of Economic Research.
- Braghieri, L. (2024), ‘Political Correctness, Social Image, and Information Transmission’, *American Economic Review* **114**(12), 3877–3904.
- Bursztyn, L., Egorov, G. & Fiorin, S. (2020), ‘From Extreme to Mainstream: The Erosion of Social Norms’, *American Economic Review* **110**(11), 3522–3548.
- Bursztyn, L. & Jensen, R. (2017), ‘Social Image and Economic Behavior in the Field: Identifying, Understanding, and Shaping Social Pressure’, *Annual Review of Economics* **9**(1), 131–153.
- Carstensen, L. L. (1992), ‘Social and emotional patterns in adulthood: support for socioemotional selectivity theory.’, *Psychology and aging* **7**(3), 331.
- Casadesus-Masanell, R. & Hervás-Drane, A. (2015), ‘Competing with Privacy’, *Management Science* **61**(1), 229–246.
- Chen, L., Huang, Y., Ouyang, S. & Xiong, W. (2021), The Data Privacy Paradox and Digital Demand, Working Paper 28854, National Bureau of Economic Research.
URL: <http://www.nber.org/papers/w28854>
- Choi, S., Kim, B., Kim, Y. S. & Kwon, O. (2025), ‘Central Bank Digital Currency and Privacy: A Randomized Survey Experiment’, *International Economic Review* **66**(2), 823–847.
- Colnago, J., Cranor, L. F. & Acquisti, A. (2023), Is There a Reverse Privacy Paradox? An Exploratory Analysis of Gaps Between Privacy Perspectives and Privacy-Seeking Behaviors, in ‘Proceedings on Privacy Enhancing Technologies Symposium’, pp. 455–476.

- De Freitas, J., Oğuz-Uğuralp, Z., Uğuralp, A. K. & Puntoni, S. (2025), ‘AI Companions Reduce Loneliness’, *Journal of Consumer Research* p. ucaf040.
- De Freitas, J., Uğuralp, Z., Uğuralp, A. K. & Puntoni, S. (2025), ‘Why Most Resist AI Companions’.
- Dubé, J.-P., Lynch, J. G., Bergemann, D., Demirer, M., Goldfarb, A., Johnson, G., Lambrecht, A., Lin, T., Tuchman, A. & Tucker, C. (2025), ‘The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing’, *Marketing Science* **44**(5), 975–984.
- Fairweather, Z., Fiebig, D., Gorajek, A., Guttman, R., Ma, J. & Mulqueeney, J. (2024), Valuing Safety and Privacy in Retail Central Bank Digital Currency, Discussion Paper 2024-02, Reserve Bank of Australia.
- Farrell, J. (2012), ‘Can Privacy Be Just Another Good’, *Journal on Telecommunications & High Technology Law* **10**, 251.
- Geiecke, F. & Jaravel, X. (2024), ‘Conversations at Scale: Robust AI-led Interviews with a Simple Open-source Platform’, *Available at SSRN 4974382*.
- Goldfarb, A., McDevitt, R. C., Samila, S. & Silverman, B. S. (2015), ‘The Effect of Social Interaction on Economic Transactions: Evidence from Changes in Two Retail Formats’, *Management Science* **61**(12), 2963–2981.
- Goldfarb, A. & Que, V. F. (2023), ‘The Economics of Digital Privacy’, *Annual Review of Economics* **15**, 267–286.
- Goldfarb, A. & Tucker, C. (2012), ‘Shifts in Privacy Concerns’, *American Economic Review* **102**(3), 349–353.
- Hann, I.-H., Hui, K.-L., Lee, S.-Y. T. & Png, I. P. (2007), ‘Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach’, *Journal of Management Information Systems* **24**(2), 13–42.
- Hole, A. R. (2015), ‘DCREATE: Stata Module to Create Efficient Designs for Discrete Choice Experiments’, Statistical Software Components, Boston College Department of Economics. **URL:** <https://ideas.repec.org/c/boc/bocode/s458059.html>
- John, L. K., Acquisti, A. & Loewenstein, G. (2011), ‘Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information’, *Journal of Consumer Research* **37**(5), 858–873.
- Johnson, G. (2024), *Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond*, University of Chicago Press.
- Kim, T., Barasz, K. & John, L. K. (2021), ‘Consumer Disclosure’, *Consumer Psychology Review* **4**(1), 59–69.

- Lin, T. (2022), ‘Valuing Intrinsic and Instrumental Preferences for Privacy’, *Marketing Science* **41**(4), 663–681.
- McFadden, D. (1974), Conditional logit analysis of qualitative choice behavior, in P. Zarembka, ed., ‘Frontiers in Econometrics’, Academic Press, New York, pp. 105–142.
- Nissenbaum, H. (2004), ‘Privacy as Contextual Integrity’, *Washington Law Review* **79**, 119.
- Norberg, P. A., Horne, D. R. & Horne, D. A. (2007), ‘The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors’, *Journal of Consumer Affairs* **41**(1), 100–126.
- Savage, S. J. & Waldman, D. M. (2015), ‘Privacy Tradeoffs in Smartphone Applications’, *Economics Letters* **137**, 171–175.
- Tamir, D. I. & Mitchell, J. P. (2012), ‘Disclosing information about the self is intrinsically rewarding’, *Proceedings of the National Academy of Sciences* **109**(21), 8038–8043.
URL: <https://www.pnas.org/doi/abs/10.1073/pnas.1202129109>
- Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. (2011), ‘The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study’, *Information Systems Research* **22**(2), 254–268.
- Westin, A. F. (1968), ‘Privacy and Freedom’, *Washington and Lee Law Review* **25**(1), 166.

B Supplementary appendix

Table 12: US – Income (USD 10k)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.371*** (-3.91)	0.690*** (-3.91)
Browsing activity $\times$ Company	-0.142 (-1.18)	0.868 (-1.18)
Browsing activity $\times$ Government	0.185 (1.35)	1.203 (1.35)
Private judgmental remarks $\times$ Someone close to you	0.581*** (5.27)	1.789*** (5.27)
Private judgmental remarks $\times$ AI assistant	-0.307** (-2.80)	0.735** (-2.80)
Private judgmental remarks $\times$ Company	-0.0261 (-0.21)	0.974 (-0.21)
Private judgmental remarks $\times$ Government	-0.00581 (-0.04)	0.994 (-0.04)
Personal admissions $\times$ Someone close to you	0.458*** (4.66)	1.581*** (4.66)
Personal admissions $\times$ AI assistant	-0.584*** (-4.91)	0.558*** (-4.91)
Personal admissions $\times$ Company	0.315* (2.21)	1.370* (2.21)
Personal admissions $\times$ Government	0.383** (2.80)	1.466** (2.80)
Identity data $\times$ Someone close to you	0.117 (0.93)	1.125 (0.93)
Identity data $\times$ AI assistant	0.331** (2.65)	1.392** (2.65)
Identity data $\times$ Company	0.928*** (6.80)	2.530*** (6.80)
Identity data $\times$ Government	0.451** (3.19)	1.571** (3.19)
Browsing activity $\times$ AI assistant $\times$ Income	-0.0409 (-1.88)	0.960 (-1.88)
Browsing activity $\times$ Company $\times$ Income	-0.00412 (-0.16)	0.996 (-0.16)
Browsing activity $\times$ Government $\times$ Income	-0.0210	0.979

	(-0.71)	(-0.71)
Private judgmental remarks $\times$ Someone close to you $\times$ Income	0.0183 (0.75)	1.018 (0.75)
Private judgmental remarks $\times$ AI assistant $\times$ Income	0.000129 (0.01)	1.000 (0.01)
Private judgmental remarks $\times$ Company $\times$ Income	-0.00412 (-0.15)	0.996 (-0.15)
Private judgmental remarks $\times$ Government $\times$ Income	-0.0189 (-0.56)	0.981 (-0.56)
Personal admissions $\times$ Someone close to you $\times$ Income	0.0214 (0.93)	1.022 (0.93)
Personal admissions $\times$ AI assistant $\times$ Income	-0.00467 (-0.18)	0.995 (-0.18)
Personal admissions $\times$ Company $\times$ Income	-0.0257 (-0.82)	0.975 (-0.82)
Personal admissions $\times$ Government $\times$ Income	-0.0327 (-0.99)	0.968 (-0.99)
Identity data $\times$ Someone close to you $\times$ Income	0.00590 (0.21)	1.006 (0.21)
Identity data $\times$ AI assistant $\times$ Income	-0.0409 (-1.56)	0.960 (-1.56)
Identity data $\times$ Company $\times$ Income	-0.0429 (-1.32)	0.958 (-1.32)
Identity data $\times$ Government $\times$ Income	-0.0470 (-1.58)	0.954 (-1.58)
Cost	-0.00366*** (-5.67)	0.996*** (-5.67)
Cost $\times$ Income	-0.0000909 (-0.66)	1.000 (-0.66)
Observations	11688	11688
Pseudo R^2	0.060	0.060

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 13: US – Ethnicity (white baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.473*** (-3.96)	0.623*** (-3.96)
Browsing activity $\times$ Company	-0.213 (-1.40)	0.808 (-1.40)
Browsing activity $\times$ Government	0.139 (0.84)	1.149 (0.84)
Private judgmental remarks $\times$ Someone close to you	0.310* (2.30)	1.363* (2.30)
Private judgmental remarks $\times$ AI assistant	-0.397** (-2.87)	0.672** (-2.87)
Private judgmental remarks $\times$ Company	-0.00364 (-0.02)	0.996 (-0.02)
Private judgmental remarks $\times$ Government	0.208 (1.11)	1.231 (1.11)
Personal admissions $\times$ Someone close to you	0.449*** (3.66)	1.567*** (3.66)
Personal admissions $\times$ AI assistant	-0.612*** (-4.23)	0.542*** (-4.23)
Personal admissions $\times$ Company	0.326 (1.87)	1.386 (1.87)
Personal admissions $\times$ Government	0.495** (3.01)	1.640** (3.01)
Identity data $\times$ Someone close to you	-0.0591 (-0.39)	0.943 (-0.39)
Identity data $\times$ AI assistant	0.153 (0.95)	1.165 (0.95)
Identity data $\times$ Company	1.062*** (6.31)	2.892*** (6.31)
Identity data $\times$ Government	0.535** (3.05)	1.707** (3.05)
Browsing activity $\times$ AI assistant $\times$ Non white	0.176 (0.91)	1.193 (0.91)
Browsing activity $\times$ Company $\times$ Non white	0.0677 (0.28)	1.070 (0.28)
Browsing activity $\times$ Government $\times$ Non white	0.0862 (0.31)	1.090 (0.31)
Private judgmental remarks $\times$ Someone close to you $\times$ Non white	0.591**	1.805**

	(2.64)	(2.64)
Private judgmental remarks $\times$ AI assistant $\times$ Non white	0.149 (0.67)	1.161 (0.67)
Private judgmental remarks $\times$ Company $\times$ Non white	-0.168 (-0.67)	0.845 (-0.67)
Private judgmental remarks $\times$ Government $\times$ Non white	-0.618* (-1.97)	0.539* (-1.97)
Personal admissions $\times$ Someone close to you $\times$ Non white	-0.0919 (-0.46)	0.912 (-0.46)
Personal admissions $\times$ AI assistant $\times$ Non white	-0.0397 (-0.16)	0.961 (-0.16)
Personal admissions $\times$ Company $\times$ Non white	-0.158 (-0.54)	0.854 (-0.54)
Personal admissions $\times$ Government $\times$ Non white	-0.356 (-1.26)	0.701 (-1.26)
Identity data $\times$ Someone close to you $\times$ Non white	0.367 (1.40)	1.443 (1.40)
Identity data $\times$ AI assistant $\times$ Non white	0.418 (1.68)	1.519 (1.68)
Identity data $\times$ Company $\times$ Non white	-0.448 (-1.60)	0.639 (-1.60)
Identity data $\times$ Government $\times$ Non white	-0.244 (-0.86)	0.783 (-0.86)
Cost	-0.00435*** (-5.61)	0.996*** (-5.61)
Non white $\times$ Cost	0.00181 (1.38)	1.002 (1.38)
Observations	11952	11952
Pseudo R^2	0.061	0.061

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 14: US – Migrant status

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.341*** (-3.56)	0.711*** (-3.56)
Browsing activity $\times$ Company	-0.193 (-1.59)	0.825 (-1.59)
Browsing activity $\times$ Government	0.171 (1.25)	1.187 (1.25)
Private judgmental remarks $\times$ Someone close to you	0.554*** (5.03)	1.741*** (5.03)
Private judgmental remarks $\times$ AI assistant	-0.313** (-2.81)	0.731** (-2.81)
Private judgmental remarks $\times$ Company	-0.0703 (-0.55)	0.932 (-0.55)
Private judgmental remarks $\times$ Government	-0.0345 (-0.22)	0.966 (-0.22)
Personal admissions $\times$ Someone close to you	0.422*** (4.25)	1.525*** (4.25)
Personal admissions $\times$ AI assistant	-0.626*** (-5.21)	0.535*** (-5.21)
Personal admissions $\times$ Company	0.288* (2.02)	1.334* (2.02)
Personal admissions $\times$ Government	0.339* (2.48)	1.404* (2.48)
Identity data $\times$ Someone close to you	0.0945 (0.75)	1.099 (0.75)
Identity data $\times$ AI assistant	0.323** (2.58)	1.381** (2.58)
Identity data $\times$ Company	0.909*** (6.61)	2.481*** (6.61)
Identity data $\times$ Government	0.480*** (3.39)	1.616*** (3.39)
Browsing activity $\times$ AI assistant $\times$ Migrant	-1.105* (-2.30)	0.331* (-2.30)
Browsing activity $\times$ Company $\times$ Migrant	0.101 (0.18)	1.106 (0.18)
Browsing activity $\times$ Government $\times$ Migrant	0.0102 (0.01)	1.010 (0.01)
Private judgmental remarks $\times$ Someone close to you $\times$ Migrant	-0.419	0.658

	(-0.78)	(-0.78)
Private judgmental remarks $\times$ AI assistant $\times$ Migrant	-0.569 (-1.13)	0.566 (-1.13)
Private judgmental remarks $\times$ Company $\times$ Migrant	0.0844 (0.18)	1.088 (0.18)
Private judgmental remarks $\times$ Government $\times$ Migrant	-0.114 (-0.17)	0.892 (-0.17)
Personal admissions $\times$ Someone close to you $\times$ Migrant	0.0468 (0.11)	1.048 (0.11)
Personal admissions $\times$ AI assistant $\times$ Migrant	0.0131 (0.03)	1.013 (0.03)
Personal admissions $\times$ Company $\times$ Migrant	-0.479 (-0.61)	0.620 (-0.61)
Personal admissions $\times$ Government $\times$ Migrant	0.261 (0.41)	1.298 (0.41)
Identity data $\times$ Someone close to you $\times$ Migrant	-0.297 (-0.44)	0.743 (-0.44)
Identity data $\times$ AI assistant $\times$ Migrant	-0.166 (-0.30)	0.847 (-0.30)
Identity data $\times$ Company $\times$ Migrant	-0.455 (-0.74)	0.634 (-0.74)
Identity data $\times$ Government $\times$ Migrant	-1.046 (-1.69)	0.351 (-1.69)
Cost	-0.00358*** (-5.57)	0.996*** (-5.57)
Migrant $\times$ Cost	0.00189 (0.50)	1.002 (0.50)
Observations	11952	11952
Pseudo R^2	0.058	0.058

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 15: US – Political Affiliation (Democrat baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.747*** (-4.16)	0.474*** (-4.16)
Browsing activity $\times$ Company	-0.442 (-1.95)	0.643 (-1.95)
Browsing activity $\times$ Government	-0.194 (-0.77)	0.824 (-0.77)
Private judgmental remarks $\times$ Someone close to you	0.440* (2.26)	1.553* (2.26)
Private judgmental remarks $\times$ AI assistant	-0.755*** (-3.64)	0.470*** (-3.64)
Private judgmental remarks $\times$ Company	-0.292 (-1.21)	0.747 (-1.21)
Private judgmental remarks $\times$ Government	-0.144 (-0.49)	0.866 (-0.49)
Personal admissions $\times$ Someone close to you	0.458** (2.60)	1.582** (2.60)
Personal admissions $\times$ AI assistant	-0.860*** (-3.75)	0.423*** (-3.75)
Personal admissions $\times$ Company	0.143 (0.51)	1.154 (0.51)
Personal admissions $\times$ Government	0.238 (0.86)	1.268 (0.86)
Identity data $\times$ Someone close to you	0.00214 (0.01)	1.002 (0.01)
Identity data $\times$ AI assistant	0.0679 (0.32)	1.070 (0.32)
Identity data $\times$ Company	0.536* (2.02)	1.709* (2.02)
Identity data $\times$ Government	0.257 (1.00)	1.293 (1.00)
Browsing activity $\times$ AI assistant $\times$ Independent	0.571* (2.47)	1.770* (2.47)
Browsing activity $\times$ AI assistant $\times$ Republican	0.415 (1.68)	1.515 (1.68)
Browsing activity $\times$ Company $\times$ Independent	0.453 (1.56)	1.572 (1.56)
Browsing activity $\times$ Company $\times$ Republican	0.234	1.263

	(0.74)	(0.74)
Browsing activity $\times$ Government $\times$ Independent	0.575 (1.75)	1.778 (1.75)
Browsing activity $\times$ Government $\times$ Republican	0.448 (1.28)	1.565 (1.28)
Private judgmental remarks $\times$ Someone close to you $\times$ Independent	0.282 (1.09)	1.326 (1.09)
Private judgmental remarks $\times$ Someone close to you $\times$ Republican	-0.0400 (-0.14)	0.961 (-0.14)
Private judgmental remarks $\times$ AI assistant $\times$ Independent	0.560* (2.13)	1.751* (2.13)
Private judgmental remarks $\times$ AI assistant $\times$ Republican	0.646* (2.20)	1.909* (2.20)
Private judgmental remarks $\times$ Company $\times$ Independent	0.469 (1.53)	1.598 (1.53)
Private judgmental remarks $\times$ Company $\times$ Republican	0.128 (0.39)	1.137 (0.39)
Private judgmental remarks $\times$ Government $\times$ Independent	0.0203 (0.05)	1.021 (0.05)
Private judgmental remarks $\times$ Government $\times$ Republican	0.397 (0.99)	1.488 (0.99)
Personal admissions $\times$ Someone close to you $\times$ Independent	0.0793 (0.33)	1.082 (0.33)
Personal admissions $\times$ Someone close to you $\times$ Republican	-0.196 (-0.80)	0.822 (-0.80)
Personal admissions $\times$ AI assistant $\times$ Independent	0.276 (0.94)	1.318 (0.94)
Personal admissions $\times$ AI assistant $\times$ Republican	0.412 (1.34)	1.510 (1.34)
Personal admissions $\times$ Company $\times$ Independent	0.101 (0.28)	1.106 (0.28)
Personal admissions $\times$ Company $\times$ Republican	0.308 (0.83)	1.361 (0.83)
Personal admissions $\times$ Government $\times$ Independent	0.0539 (0.16)	1.055 (0.16)
Personal admissions $\times$ Government $\times$ Republican	0.354 (1.00)	1.424 (1.00)
Identity data $\times$ Someone close to you $\times$ Independent	0.0570 (0.19)	1.059 (0.19)
Identity data $\times$ Someone close to you $\times$ Republican	0.201 (0.61)	1.222 (0.61)
Identity data $\times$ AI assistant $\times$ Independent	0.598*	1.818*

	(2.06)	(2.06)
Identity data $\times$ AI assistant $\times$ Republican	0.0350 (0.11)	1.036 (0.11)
Identity data $\times$ Company $\times$ Independent	0.467 (1.41)	1.595 (1.41)
Identity data $\times$ Company $\times$ Republican	0.591 (1.62)	1.805 (1.62)
Identity data $\times$ Government $\times$ Independent	0.260 (0.77)	1.297 (0.77)
Identity data $\times$ Government $\times$ Republican	0.253 (0.70)	1.288 (0.70)
Cost	-0.00332** (-2.97)	0.997** (-2.97)
Independent $\times$ Cost	-0.000529 (-0.37)	0.999 (-0.37)
Republican $\times$ Cost	0.000106 (0.06)	1.000 (0.06)
Observations	11952	11952
Pseudo R^2	0.062	0.062

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 16: US – Relationship status (single baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.369* (-2.56)	0.691* (-2.56)
Browsing activity $\times$ Company	-0.0537 (-0.31)	0.948 (-0.31)
Browsing activity $\times$ Government	0.119 (0.62)	1.126 (0.62)
Private judgmental remarks $\times$ Someone close to you	0.414** (2.69)	1.513** (2.69)
Private judgmental remarks $\times$ AI assistant	-0.375* (-2.35)	0.687* (-2.35)
Private judgmental remarks $\times$ Company	-0.172 (-0.96)	0.842 (-0.96)
Private judgmental remarks $\times$ Government	-0.0125 (-0.06)	0.988 (-0.06)
Personal admissions $\times$ Someone close to you	0.311* (2.27)	1.365* (2.27)
Personal admissions $\times$ AI assistant	-0.643*** (-3.55)	0.526*** (-3.55)
Personal admissions $\times$ Company	0.173 (0.83)	1.188 (0.83)
Personal admissions $\times$ Government	0.409* (2.05)	1.506* (2.05)
Identity data $\times$ Someone close to you	0.0300 (0.17)	1.030 (0.17)
Identity data $\times$ AI assistant	0.402* (2.17)	1.495* (2.17)
Identity data $\times$ Company	0.944*** (4.78)	2.570*** (4.78)
Identity data $\times$ Government	0.372 (1.79)	1.451 (1.79)
Browsing activity $\times$ AI assistant $\times$ In a relationship	0.0782 (0.30)	1.081 (0.30)
Browsing activity $\times$ AI assistant $\times$ Married	-0.0553 (-0.27)	0.946 (-0.27)
Browsing activity $\times$ Company $\times$ In a relationship	0.0370 (0.10)	1.038 (0.10)
Browsing activity $\times$ Company $\times$ Married	-0.317	0.728

	(-1.23)	(-1.23)
Browsing activity $\times$ Government $\times$ In a relationship	0.166 (0.39)	1.180 (0.39)
Browsing activity $\times$ Government $\times$ Married	0.0872 (0.30)	1.091 (0.30)
Private judgmental remarks $\times$ Someone close to you $\times$ In a relationship	0.582 (1.80)	1.790 (1.80)
Private judgmental remarks $\times$ Someone close to you $\times$ Married	0.160 (0.67)	1.174 (0.67)
Private judgmental remarks $\times$ AI assistant $\times$ In a relationship	0.378 (1.20)	1.460 (1.20)
Private judgmental remarks $\times$ AI assistant $\times$ Married	-0.00845 (-0.04)	0.992 (-0.04)
Private judgmental remarks $\times$ Company $\times$ In a relationship	0.528 (1.39)	1.695 (1.39)
Private judgmental remarks $\times$ Company $\times$ Married	0.103 (0.38)	1.109 (0.38)
Private judgmental remarks $\times$ Government $\times$ In a relationship	0.253 (0.56)	1.288 (0.56)
Private judgmental remarks $\times$ Government $\times$ Married	-0.138 (-0.41)	0.872 (-0.41)
Personal admissions $\times$ Someone close to you $\times$ In a relationship	0.584* (1.99)	1.792* (1.99)
Personal admissions $\times$ Someone close to you $\times$ Married	0.113 (0.53)	1.120 (0.53)
Personal admissions $\times$ AI assistant $\times$ In a relationship	-0.184 (-0.46)	0.832 (-0.46)
Personal admissions $\times$ AI assistant $\times$ Married	0.162 (0.65)	1.175 (0.65)
Personal admissions $\times$ Company $\times$ In a relationship	0.00657 (0.02)	1.007 (0.02)
Personal admissions $\times$ Company $\times$ Married	0.310 (0.98)	1.364 (0.98)
Personal admissions $\times$ Government $\times$ In a relationship	-0.133 (-0.32)	0.876 (-0.32)
Personal admissions $\times$ Government $\times$ Married	-0.0515 (-0.17)	0.950 (-0.17)
Identity data $\times$ Someone close to you $\times$ In a relationship	0.288 (0.77)	1.334 (0.77)
Identity data $\times$ Someone close to you $\times$ Married	0.0979 (0.35)	1.103 (0.35)
Identity data $\times$ AI assistant $\times$ In a relationship	0.363	1.438

	(1.04)	(1.04)
Identity data $\times$ AI assistant $\times$ Married	-0.333 (-1.23)	0.716 (-1.23)
Identity data $\times$ Company $\times$ In a relationship	0.0252 (0.07)	1.025 (0.07)
Identity data $\times$ Company $\times$ Married	-0.0752 (-0.25)	0.928 (-0.25)
Identity data $\times$ Government $\times$ In a relationship	-0.00796 (-0.02)	0.992 (-0.02)
Identity data $\times$ Government $\times$ Married	0.184 (0.59)	1.202 (0.59)
Cost	-0.00292** (-3.07)	0.997** (-3.07)
In a relationship $\times$ Cost	-0.00159 (-0.88)	0.998 (-0.88)
Married $\times$ Cost	-0.00106 (-0.75)	0.999 (-0.75)
Observations	11880	11880
Pseudo R^2	0.062	0.062

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 17: US – Employment status (full time baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.531*** (-4.01)	0.588*** (-4.01)
Browsing activity $\times$ Company	-0.102 (-0.61)	0.903 (-0.61)
Browsing activity $\times$ Government	0.0212 (0.11)	1.021 (0.11)
Private judgmental remarks $\times$ Someone close to you	0.511*** (3.44)	1.666*** (3.44)
Private judgmental remarks $\times$ AI assistant	-0.481*** (-3.29)	0.618*** (-3.29)
Private judgmental remarks $\times$ Company	-0.211 (-1.22)	0.810 (-1.22)
Private judgmental remarks $\times$ Government	-0.225 (-1.06)	0.799 (-1.06)
Personal admissions $\times$ Someone close to you	0.453*** (3.40)	1.573*** (3.40)
Personal admissions $\times$ AI assistant	-0.758*** (-4.67)	0.469*** (-4.67)
Personal admissions $\times$ Company	0.0630 (0.31)	1.065 (0.31)
Personal admissions $\times$ Government	0.233 (1.24)	1.262 (1.24)
Identity data $\times$ Someone close to you	0.172 (0.98)	1.187 (0.98)
Identity data $\times$ AI assistant	0.303 (1.80)	1.355 (1.80)
Identity data $\times$ Company	0.673*** (3.61)	1.961*** (3.61)
Identity data $\times$ Government	0.291 (1.44)	1.337 (1.44)
Browsing activity $\times$ AI assistant $\times$ Student	-0.417 (-0.81)	0.659 (-0.81)
Browsing activity $\times$ AI assistant $\times$ Homemaker	-0.340 (-0.48)	0.712 (-0.48)
Browsing activity $\times$ AI assistant $\times$ Unemployed	0.614 (1.68)	1.848 (1.68)
Browsing activity $\times$ AI assistant $\times$ Part-time	0.284	1.328

	(1.15)	(1.15)
Browsing activity $\times$ AI assistant $\times$ Retired	0.543 (1.65)	1.722 (1.65)
Browsing activity $\times$ Company $\times$ Student	-1.147 (-1.82)	0.317 (-1.82)
Browsing activity $\times$ Company $\times$ Homemaker	0.0645 (0.08)	1.067 (0.08)
Browsing activity $\times$ Company $\times$ Unemployed	0.601 (1.35)	1.823 (1.35)
Browsing activity $\times$ Company $\times$ Part-time	-0.508 (-1.60)	0.602 (-1.60)
Browsing activity $\times$ Company $\times$ Retired	0.0326 (0.08)	1.033 (0.08)
Browsing activity $\times$ Government $\times$ Student	-0.142 (-0.16)	0.867 (-0.16)
Browsing activity $\times$ Government $\times$ Homemaker	0.605 (1.23)	1.831 (1.23)
Browsing activity $\times$ Government $\times$ Unemployed	0.552 (1.07)	1.737 (1.07)
Browsing activity $\times$ Government $\times$ Part-time	-0.0934 (-0.27)	0.911 (-0.27)
Browsing activity $\times$ Government $\times$ Retired	0.872* (2.00)	2.391* (2.00)
Private judgmental remarks $\times$ Someone close to you $\times$ Student	-0.415 (-0.69)	0.661 (-0.69)
Private judgmental remarks $\times$ Someone close to you $\times$ Homemaker	1.358* (2.34)	3.887* (2.34)
Private judgmental remarks $\times$ Someone close to you $\times$ Unemployed	0.429 (1.11)	1.536 (1.11)
Private judgmental remarks $\times$ Someone close to you $\times$ Part-time	-0.310 (-1.07)	0.734 (-1.07)
Private judgmental remarks $\times$ Someone close to you $\times$ Retired	0.137 (0.34)	1.146 (0.34)
Private judgmental remarks $\times$ AI assistant $\times$ Student	-0.625 (-1.02)	0.535 (-1.02)
Private judgmental remarks $\times$ AI assistant $\times$ Homemaker	0.763 (1.03)	2.144 (1.03)
Private judgmental remarks $\times$ AI assistant $\times$ Unemployed	0.843 (1.53)	2.323 (1.53)
Private judgmental remarks $\times$ AI assistant $\times$ Part-time	0.146 (0.50)	1.157 (0.50)
Private judgmental remarks $\times$ AI assistant $\times$ Retired	0.378	1.459

	(1.07)	(1.07)
Private judgmental remarks $\times$ Company $\times$ Student	-0.922 (-1.38)	0.398 (-1.38)
Private judgmental remarks $\times$ Company $\times$ Homemaker	0.372 (0.48)	1.451 (0.48)
Private judgmental remarks $\times$ Company $\times$ Unemployed	0.395 (0.83)	1.484 (0.83)
Private judgmental remarks $\times$ Company $\times$ Part-time	0.392 (1.18)	1.480 (1.18)
Private judgmental remarks $\times$ Company $\times$ Retired	0.500 (1.17)	1.649 (1.17)
Private judgmental remarks $\times$ Government $\times$ Student	-0.775 (-1.05)	0.461 (-1.05)
Private judgmental remarks $\times$ Government $\times$ Homemaker	0.398 (0.46)	1.489 (0.46)
Private judgmental remarks $\times$ Government $\times$ Unemployed	0.350 (0.60)	1.420 (0.60)
Private judgmental remarks $\times$ Government $\times$ Part-time	0.349 (0.89)	1.418 (0.89)
Private judgmental remarks $\times$ Government $\times$ Retired	0.916 (1.84)	2.499 (1.84)
Personal admissions $\times$ Someone close to you $\times$ Student	-0.999* (-2.12)	0.368* (-2.12)
Personal admissions $\times$ Someone close to you $\times$ Homemaker	0.357 (0.78)	1.429 (0.78)
Personal admissions $\times$ Someone close to you $\times$ Unemployed	-0.0722 (-0.16)	0.930 (-0.16)
Personal admissions $\times$ Someone close to you $\times$ Part-time	-0.136 (-0.50)	0.873 (-0.50)
Personal admissions $\times$ Someone close to you $\times$ Retired	-0.0150 (-0.05)	0.985 (-0.05)
Personal admissions $\times$ AI assistant $\times$ Student	-0.995 (-1.34)	0.370 (-1.34)
Personal admissions $\times$ AI assistant $\times$ Homemaker	0.260 (0.49)	1.297 (0.49)
Personal admissions $\times$ AI assistant $\times$ Unemployed	0.982* (2.26)	2.669* (2.26)
Personal admissions $\times$ AI assistant $\times$ Part-time	-0.175 (-0.57)	0.840 (-0.57)
Personal admissions $\times$ AI assistant $\times$ Retired	0.813* (2.01)	2.256* (2.01)
Personal admissions $\times$ Company $\times$ Student	-0.637	0.529

	(-0.97)	(-0.97)
Personal admissions $\times$ Company $\times$ Homemaker	0.481 (0.47)	1.618 (0.47)
Personal admissions $\times$ Company $\times$ Unemployed	0.983* (2.12)	2.674* (2.12)
Personal admissions $\times$ Company $\times$ Part-time	0.409 (1.10)	1.506 (1.10)
Personal admissions $\times$ Company $\times$ Retired	0.577 (1.14)	1.781 (1.14)
Personal admissions $\times$ Government $\times$ Student	-1.073 (-1.83)	0.342 (-1.83)
Personal admissions $\times$ Government $\times$ Homemaker	0.915 (0.84)	2.496 (0.84)
Personal admissions $\times$ Government $\times$ Unemployed	0.609 (1.16)	1.839 (1.16)
Personal admissions $\times$ Government $\times$ Part-time	0.126 (0.36)	1.134 (0.36)
Personal admissions $\times$ Government $\times$ Retired	0.561 (1.25)	1.753 (1.25)
Identity data $\times$ Someone close to you $\times$ Student	-0.991 (-1.57)	0.371 (-1.57)
Identity data $\times$ Someone close to you $\times$ Homemaker	0.889 (1.25)	2.432 (1.25)
Identity data $\times$ Someone close to you $\times$ Unemployed	0.379 (0.74)	1.461 (0.74)
Identity data $\times$ Someone close to you $\times$ Part-time	-0.632 (-1.86)	0.531 (-1.86)
Identity data $\times$ Someone close to you $\times$ Retired	0.153 (0.37)	1.166 (0.37)
Identity data $\times$ AI assistant $\times$ Student	-0.538 (-0.99)	0.584 (-0.99)
Identity data $\times$ AI assistant $\times$ Homemaker	0.444 (0.55)	1.559 (0.55)
Identity data $\times$ AI assistant $\times$ Unemployed	0.592 (1.20)	1.807 (1.20)
Identity data $\times$ AI assistant $\times$ Part-time	-0.506 (-1.57)	0.603 (-1.57)
Identity data $\times$ AI assistant $\times$ Retired	0.551 (1.32)	1.736 (1.32)
Identity data $\times$ Company $\times$ Student	-0.898 (-1.49)	0.407 (-1.49)
Identity data $\times$ Company $\times$ Homemaker	0.935	2.548

	(0.81)	(0.81)
Identity data $\times$ Company $\times$ Unemployed	1.423** (2.79)	4.151** (2.79)
Identity data $\times$ Company $\times$ Part-time	0.124 (0.36)	1.132 (0.36)
Identity data $\times$ Company $\times$ Retired	1.191** (2.61)	3.292** (2.61)
Identity data $\times$ Government $\times$ Student	-0.921 (-1.63)	0.398 (-1.63)
Identity data $\times$ Government $\times$ Homemaker	1.853* (2.22)	6.381* (2.22)
Identity data $\times$ Government $\times$ Unemployed	1.041 (1.88)	2.833 (1.88)
Identity data $\times$ Government $\times$ Part-time	-0.234 (-0.68)	0.791 (-0.68)
Identity data $\times$ Government $\times$ Retired	0.936* (2.04)	2.549* (2.04)
Cost	-0.00378*** (-4.87)	0.996*** (-4.87)
Student $\times$ Cost	-0.00105 (-0.28)	0.999 (-0.28)
Homemaker $\times$ Cost	-0.0103* (-2.25)	0.990* (-2.25)
Unemployed $\times$ Cost	0.00400 (1.39)	1.004 (1.39)
Part-time $\times$ Cost	0.00169 (0.98)	1.002 (0.98)
Retired $\times$ Cost	-0.000580 (-0.26)	0.999 (-0.26)
Observations	11520	11520
Pseudo R^2	0.070	0.070

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 18: US – Education (Bachelor’s baseline)

	(1) Conditional logit	(2) Odds ratio
Browsing activity × Someone close to you	0 -	1 -
Browsing activity × AI assistant	-0.708*** (-4.17)	0.493*** (-4.17)
Browsing activity × Company	-0.405* (-1.97)	0.667* (-1.97)
Browsing activity × Government	-0.0757 (-0.32)	0.927 (-0.32)
Private judgmental remarks × Someone close to you	0.495** (2.69)	1.641** (2.69)
Private judgmental remarks × AI assistant	-0.490** (-2.66)	0.613** (-2.66)
Private judgmental remarks × Company	-0.267 (-1.30)	0.766 (-1.30)
Private judgmental remarks × Government	-0.255 (-1.02)	0.775 (-1.02)
Personal admissions × Someone close to you	0.389* (2.32)	1.475* (2.32)
Personal admissions × AI assistant	-0.738*** (-3.76)	0.478*** (-3.76)
Personal admissions × Company	0.211 (0.88)	1.235 (0.88)
Personal admissions × Government	0.115 (0.49)	1.122 (0.49)
Identity data × Someone close to you	0.186 (0.84)	1.205 (0.84)
Identity data × AI assistant	0.147 (0.72)	1.159 (0.72)
Identity data × Company	0.763*** (3.32)	2.144*** (3.32)
Identity data × Government	0.115 (0.49)	1.122 (0.49)
Browsing activity × AI assistant × High school or less	0.371 (1.37)	1.449 (1.37)
Browsing activity × AI assistant × Some college	0.483 (1.66)	1.621 (1.66)
Browsing activity × AI assistant × Associates/technical	0.352 (1.08)	1.422 (1.08)
Browsing activity × AI assistant × Graduate	0.579* (1.08)	1.784* (1.08)

	(2.16)	(2.16)
Browsing activity $\times$ Company $\times$ High school or less	0.157 (0.43)	1.170 (0.43)
Browsing activity $\times$ Company $\times$ Some college	0.544 (1.56)	1.723 (1.56)
Browsing activity $\times$ Company $\times$ Associates/technical	0.133 (0.35)	1.142 (0.35)
Browsing activity $\times$ Company $\times$ Graduate	0.450 (1.29)	1.568 (1.29)
Browsing activity $\times$ Government $\times$ High school or less	-0.294 (-0.67)	0.746 (-0.67)
Browsing activity $\times$ Government $\times$ Some college	0.700 (1.88)	2.014 (1.88)
Browsing activity $\times$ Government $\times$ Associates/technical	0.285 (0.63)	1.329 (0.63)
Browsing activity $\times$ Government $\times$ Graduate	0.575 (1.49)	1.777 (1.49)
Private judgmental remarks $\times$ Someone close to you $\times$ High school or less	-0.249 (-0.77)	0.780 (-0.77)
Private judgmental remarks $\times$ Someone close to you $\times$ Some college	-0.0112 (-0.03)	0.989 (-0.03)
Private judgmental remarks $\times$ Someone close to you $\times$ Associates/technical	0.0672 (0.18)	1.070 (0.18)
Private judgmental remarks $\times$ Someone close to you $\times$ Graduate	0.385 (1.29)	1.469 (1.29)
Private judgmental remarks $\times$ AI assistant $\times$ High school or less	0.182 (0.56)	1.199 (0.56)
Private judgmental remarks $\times$ AI assistant $\times$ Some college	0.281 (0.89)	1.325 (0.89)
Private judgmental remarks $\times$ AI assistant $\times$ Associates/technical	-0.0934 (-0.23)	0.911 (-0.23)
Private judgmental remarks $\times$ AI assistant $\times$ Graduate	0.409 (1.34)	1.505 (1.34)
Private judgmental remarks $\times$ Company $\times$ High school or less	0.147 (0.38)	1.158 (0.38)
Private judgmental remarks $\times$ Company $\times$ Some college	0.282 (0.82)	1.326 (0.82)
Private judgmental remarks $\times$ Company $\times$ Associates/technical	0.368 (0.85)	1.444 (0.85)
Private judgmental remarks $\times$ Company $\times$ Graduate	0.470 (1.31)	1.600 (1.31)

Private judgmental remarks $\times$ Government $\times$ High school or less	0.0779 (0.17)	1.081 (0.17)
Private judgmental remarks $\times$ Government $\times$ Some college	0.284 (0.67)	1.328 (0.67)
Private judgmental remarks $\times$ Government $\times$ Associates/technical	0.220 (0.42)	1.246 (0.42)
Private judgmental remarks $\times$ Government $\times$ Graduate	0.735 (1.72)	2.085 (1.72)
Personal admissions $\times$ Someone close to you $\times$ High school or less	-0.0625 (-0.20)	0.939 (-0.20)
Personal admissions $\times$ Someone close to you $\times$ Some college	0.121 (0.43)	1.128 (0.43)
Personal admissions $\times$ Someone close to you $\times$ Associates/technical	-0.0101 (-0.03)	0.990 (-0.03)
Personal admissions $\times$ Someone close to you $\times$ Graduate	0.113 (0.41)	1.119 (0.41)
Personal admissions $\times$ AI assistant $\times$ High school or less	-0.163 (-0.43)	0.850 (-0.43)
Personal admissions $\times$ AI assistant $\times$ Some college	0.301 (0.86)	1.351 (0.86)
Personal admissions $\times$ AI assistant $\times$ Associates/technical	0.189 (0.48)	1.208 (0.48)
Personal admissions $\times$ AI assistant $\times$ Graduate	0.302 (0.94)	1.352 (0.94)
Personal admissions $\times$ Company $\times$ High school or less	-0.431 (-0.96)	0.650 (-0.96)
Personal admissions $\times$ Company $\times$ Some college	0.0962 (0.24)	1.101 (0.24)
Personal admissions $\times$ Company $\times$ Associates/technical	0.131 (0.30)	1.140 (0.30)
Personal admissions $\times$ Company $\times$ Graduate	0.398 (0.99)	1.489 (0.99)
Personal admissions $\times$ Government $\times$ High school or less	0.0738 (0.17)	1.077 (0.17)
Personal admissions $\times$ Government $\times$ Some college	0.521 (1.32)	1.683 (1.32)
Personal admissions $\times$ Government $\times$ Associates/technical	0.0989 (0.23)	1.104 (0.23)
Personal admissions $\times$ Government $\times$ Graduate	0.638 (1.74)	1.893 (1.74)
Identity data $\times$ Someone close to you $\times$ High school or less	-0.517 (-1.35)	0.596 (-1.35)

Identity data $\times$ Someone close to you $\times$ Some college	0.143 (0.41)	1.154 (0.41)
Identity data $\times$ Someone close to you $\times$ Associates/technical	-0.295 (-0.66)	0.745 (-0.66)
Identity data $\times$ Someone close to you $\times$ Graduate	-0.0897 (-0.25)	0.914 (-0.25)
Identity data $\times$ AI assistant $\times$ High school or less	0.344 (0.89)	1.410 (0.89)
Identity data $\times$ AI assistant $\times$ Some college	0.209 (0.56)	1.232 (0.56)
Identity data $\times$ AI assistant $\times$ Associates/technical	0.234 (0.59)	1.264 (0.59)
Identity data $\times$ AI assistant $\times$ Graduate	0.291 (0.87)	1.338 (0.87)
Identity data $\times$ Company $\times$ High school or less	-0.0672 (-0.17)	0.935 (-0.17)
Identity data $\times$ Company $\times$ Some college	0.628 (1.58)	1.875 (1.58)
Identity data $\times$ Company $\times$ Associates/technical	0.191 (0.43)	1.210 (0.43)
Identity data $\times$ Company $\times$ Graduate	0.117 (0.31)	1.124 (0.31)
Identity data $\times$ Government $\times$ High school or less	-0.0176 (-0.04)	0.983 (-0.04)
Identity data $\times$ Government $\times$ Some college	0.826* (2.00)	2.285* (2.00)
Identity data $\times$ Government $\times$ Associates/technical	0.430 (0.94)	1.537 (0.94)
Identity data $\times$ Government $\times$ Graduate	0.570 (1.46)	1.768 (1.46)
Cost	-0.00130 (-1.26)	0.999 (-1.26)
High school or less $\times$ Cost	-0.00242 (-1.25)	0.998 (-1.25)
Some college $\times$ Cost	-0.00582** (-2.96)	0.994** (-2.96)
Associates/technical $\times$ Cost	-0.00409* (-2.07)	0.996* (-2.07)
Graduate $\times$ Cost	-0.00137 (-0.76)	0.999 (-0.76)
Observations	11928	11928
Pseudo R^2	0.066	0.066
t statistics in parentheses		

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 19: US – Previous data breach

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.483*** (-3.95)	0.617*** (-3.95)
Browsing activity $\times$ Company	-0.317* (-2.10)	0.728* (-2.10)
Browsing activity $\times$ Government	0.0159 (0.09)	1.016 (0.09)
Private judgmental remarks $\times$ Someone close to you	0.489*** (3.44)	1.631*** (3.44)
Private judgmental remarks $\times$ AI assistant	-0.442** (-3.02)	0.643** (-3.02)
Private judgmental remarks $\times$ Company	-0.261 (-1.62)	0.770 (-1.62)
Private judgmental remarks $\times$ Government	-0.172 (-0.85)	0.842 (-0.85)
Personal admissions $\times$ Someone close to you	0.342** (2.66)	1.408** (2.66)
Personal admissions $\times$ AI assistant	-0.828*** (-5.31)	0.437*** (-5.31)
Personal admissions $\times$ Company	0.236 (1.28)	1.266 (1.28)
Personal admissions $\times$ Government	0.226 (1.24)	1.253 (1.24)
Identity data $\times$ Someone close to you	-0.0430 (-0.27)	0.958 (-0.27)
Identity data $\times$ AI assistant	0.142 (0.90)	1.152 (0.90)
Identity data $\times$ Company	0.772*** (4.50)	2.163*** (4.50)
Identity data $\times$ Government	0.252 (1.38)	1.287 (1.38)
Browsing activity $\times$ AI assistant $\times$ Yes	0.225 (1.18)	1.253 (1.18)
Browsing activity $\times$ Company $\times$ Yes	0.329 (1.36)	1.390 (1.36)
Browsing activity $\times$ Government $\times$ Yes	0.361 (1.32)	1.435 (1.32)
Private judgmental remarks $\times$ Someone close to you $\times$ Yes	0.127	1.136

	(0.58)	(0.58)
Private judgmental remarks $\times$ AI assistant $\times$ Yes	0.261 (1.20)	1.298 (1.20)
Private judgmental remarks $\times$ Company $\times$ Yes	0.484 (1.93)	1.623 (1.93)
Private judgmental remarks $\times$ Government $\times$ Yes	0.353 (1.17)	1.424 (1.17)
Personal admissions $\times$ Someone close to you $\times$ Yes	0.212 (1.08)	1.236 (1.08)
Personal admissions $\times$ AI assistant $\times$ Yes	0.492* (2.09)	1.636* (2.09)
Personal admissions $\times$ Company $\times$ Yes	0.100 (0.36)	1.106 (0.36)
Personal admissions $\times$ Government $\times$ Yes	0.322 (1.20)	1.380 (1.20)
Identity data $\times$ Someone close to you $\times$ Yes	0.297 (1.17)	1.346 (1.17)
Identity data $\times$ AI assistant $\times$ Yes	0.419 (1.67)	1.520 (1.67)
Identity data $\times$ Company $\times$ Yes	0.300 (1.10)	1.350 (1.10)
Identity data $\times$ Government $\times$ Yes	0.438 (1.56)	1.550 (1.56)
Cost	-0.00390*** (-4.40)	0.996*** (-4.40)
Yes $\times$ Cost	0.000917 (0.73)	1.001 (0.73)
Observations	11952	11952
Pseudo R^2	0.058	0.058

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 20: US – AI Use

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	-0.405 (-1.76)	0.667 (-1.76)
Browsing activity $\times$ Company	-0.0806 (-0.24)	0.923 (-0.24)
Browsing activity $\times$ Government	0.119 (0.38)	1.126 (0.38)
Private judgmental remarks $\times$ Someone close to you	0.741** (2.98)	2.097** (2.98)
Private judgmental remarks $\times$ AI assistant	-0.308 (-1.03)	0.735 (-1.03)
Private judgmental remarks $\times$ Company	-0.122 (-0.34)	0.885 (-0.34)
Private judgmental remarks $\times$ Government	-0.00477 (-0.01)	0.995 (-0.01)
Personal admissions $\times$ Someone close to you	0.584** (2.60)	1.794** (2.60)
Personal admissions $\times$ AI assistant	-0.642 (-1.90)	0.526 (-1.90)
Personal admissions $\times$ Company	0.573 (1.48)	1.773 (1.48)
Personal admissions $\times$ Government	0.521 (1.31)	1.684 (1.31)
Identity data $\times$ Someone close to you	0.0538 (0.17)	1.055 (0.17)
Identity data $\times$ AI assistant	0.941** (2.78)	2.562** (2.78)
Identity data $\times$ Company	1.401*** (3.66)	4.058*** (3.66)
Identity data $\times$ Government	0.366 (0.89)	1.443 (0.89)
Browsing activity $\times$ AI assistant $\times$ AI use	0.0226 (0.09)	1.023 (0.09)
Browsing activity $\times$ Company $\times$ AI use	-0.119 (-0.34)	0.888 (-0.34)
Browsing activity $\times$ Government $\times$ AI use	0.0617 (0.18)	1.064 (0.18)
Private judgmental remarks $\times$ Someone close to you $\times$ AI use	-0.233	0.792

	(-0.85)	(-0.85)
Private judgmental remarks $\times$ AI assistant $\times$ AI use	-0.0301 (-0.09)	0.970 (-0.09)
Private judgmental remarks $\times$ Company $\times$ AI use	0.0789 (0.21)	1.082 (0.21)
Private judgmental remarks $\times$ Government $\times$ AI use	-0.0219 (-0.05)	0.978 (-0.05)
Personal admissions $\times$ Someone close to you $\times$ AI use	-0.183 (-0.73)	0.833 (-0.73)
Personal admissions $\times$ AI assistant $\times$ AI use	0.0227 (0.06)	1.023 (0.06)
Personal admissions $\times$ Company $\times$ AI use	-0.353 (-0.85)	0.702 (-0.85)
Personal admissions $\times$ Government $\times$ AI use	-0.191 (-0.45)	0.826 (-0.45)
Identity data $\times$ Someone close to you $\times$ AI use	0.0351 (0.10)	1.036 (0.10)
Identity data $\times$ AI assistant $\times$ AI use	-0.733* (-2.02)	0.480* (-2.02)
Identity data $\times$ Company $\times$ AI use	-0.596 (-1.46)	0.551 (-1.46)
Identity data $\times$ Government $\times$ AI use	0.0866 (0.20)	1.090 (0.20)
Cost	-0.00364* (-2.19)	0.996* (-2.19)
AI use $\times$ Cost	0.000179 (0.10)	1.000 (0.10)
Observations	11952	11952
Pseudo R^2	0.059	0.059

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 21: US – Social Media Use

	(1) Conditional logit	(2) Odds ratio
Browsing activity $\times$ Someone close to you	0 -	1 -
Browsing activity $\times$ AI assistant	1.033 (1.32)	2.808 (1.32)
Browsing activity $\times$ Company	-0.00896 (-0.01)	0.991 (-0.01)
Browsing activity $\times$ Government	-0.0489 (-0.05)	0.952 (-0.05)
Private judgmental remarks $\times$ Someone close to you	1.612 (1.65)	5.015 (1.65)
Private judgmental remarks $\times$ AI assistant	0.614 (0.91)	1.848 (0.91)
Private judgmental remarks $\times$ Company	0.519 (0.68)	1.681 (0.68)
Private judgmental remarks $\times$ Government	-0.139 (-0.15)	0.871 (-0.15)
Personal admissions $\times$ Someone close to you	0.433 (0.72)	1.542 (0.72)
Personal admissions $\times$ AI assistant	-0.106 (-0.15)	0.899 (-0.15)
Personal admissions $\times$ Company	2.238 (1.86)	9.377 (1.86)
Personal admissions $\times$ Government	1.099 (1.58)	3.001 (1.58)
Identity data $\times$ Someone close to you	-0.0538 (-0.06)	0.948 (-0.06)
Identity data $\times$ AI assistant	1.111* (2.24)	3.036* (2.24)
Identity data $\times$ Company	2.593** (2.78)	13.38** (2.78)
Identity data $\times$ Government	0.231 (0.28)	1.260 (0.28)
Browsing activity $\times$ AI assistant $\times$ Social media use	-1.454 (-1.85)	0.234 (-1.85)
Browsing activity $\times$ Company $\times$ Social media use	-0.173 (-0.25)	0.841 (-0.25)
Browsing activity $\times$ Government $\times$ Social media use	0.219 (0.20)	1.245 (0.20)
Private judgmental remarks $\times$ Someone close to you $\times$ Social media use	-1.090	0.336

	(-1.11)	(-1.11)
Private judgmental remarks $\times$ AI assistant $\times$ Social media use	-0.969 (-1.42)	0.380 (-1.42)
Private judgmental remarks $\times$ Company $\times$ Social media use	-0.586 (-0.76)	0.557 (-0.76)
Private judgmental remarks $\times$ Government $\times$ Social media use	0.118 (0.13)	1.125 (0.13)
Personal admissions $\times$ Someone close to you $\times$ Social media use	0.0104 (0.02)	1.010 (0.02)
Personal admissions $\times$ AI assistant $\times$ Social media use	-0.531 (-0.73)	0.588 (-0.73)
Personal admissions $\times$ Company $\times$ Social media use	-2.004 (-1.66)	0.135 (-1.66)
Personal admissions $\times$ Government $\times$ Social media use	-0.764 (-1.08)	0.466 (-1.08)
Identity data $\times$ Someone close to you $\times$ Social media use	0.143 (0.15)	1.154 (0.15)
Identity data $\times$ AI assistant $\times$ Social media use	-0.808 (-1.58)	0.446 (-1.58)
Identity data $\times$ Company $\times$ Social media use	-1.743 (-1.85)	0.175 (-1.85)
Identity data $\times$ Government $\times$ Social media use	0.202 (0.24)	1.224 (0.24)
Cost	-0.00639 (-1.25)	0.994 (-1.25)
Social media use $\times$ Cost	0.00292 (0.57)	1.003 (0.57)
Observations	11952	11952
Pseudo R^2	0.059	0.059

t statistics in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$