



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

Laura Brandimarte, University of Arizona

joint work with Jerg Gutmann and Gerd Muehlheusser (U Hamburg), Franziska Weber (Erasmus U)

January 26, 2026 – Washington, DC

Motivation: two different stories about AI adoption

The screenshot shows the Eurostat website interface. At the top, there is a browser address bar with the URL ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2. Below the address bar is a dark navigation bar with the text "An official website of the European Union" and a dropdown menu "How do you know?". The main header features the Eurostat logo, a "Log in" button, a language selector set to "English", and a search bar with the placeholder text "Enter search term" and a "Search" button. A blue navigation bar contains links for "Home", "Data", "News", "Publications", "About us", "Contact us", and "Help". Below this, a breadcrumb trail reads "Home > News > News articles". The main content area displays "NEWS ARTICLES | 11 December 2025" followed by the article title "20% of EU enterprises use AI technologies".

Motivation: two different stories about AI adoption

Do people in different countries have various degrees of *privacy concerns* regarding the use of such technologies?

Methodology

- Randomized experiment with participants across the US and Europe
 - Measuring willingness to adopt *Smart-Scan*, a hypothetical AI-based app
 - Given access to the user's email correspondence, Smart-Scan simplifies writing and enhances quality of emails
- Manipulated dimensions
 - Default activation
 - Salience of data privacy risks
 - Regulatory regime
- Effect of personal characteristics: risk preferences, trust, privacy concerns, and views on algorithmic decision-making
- Preview of findings: default and salience do not seem to matter, more privacy-protective regulatory regimes do (as well as personal characteristics)

Hypotheses

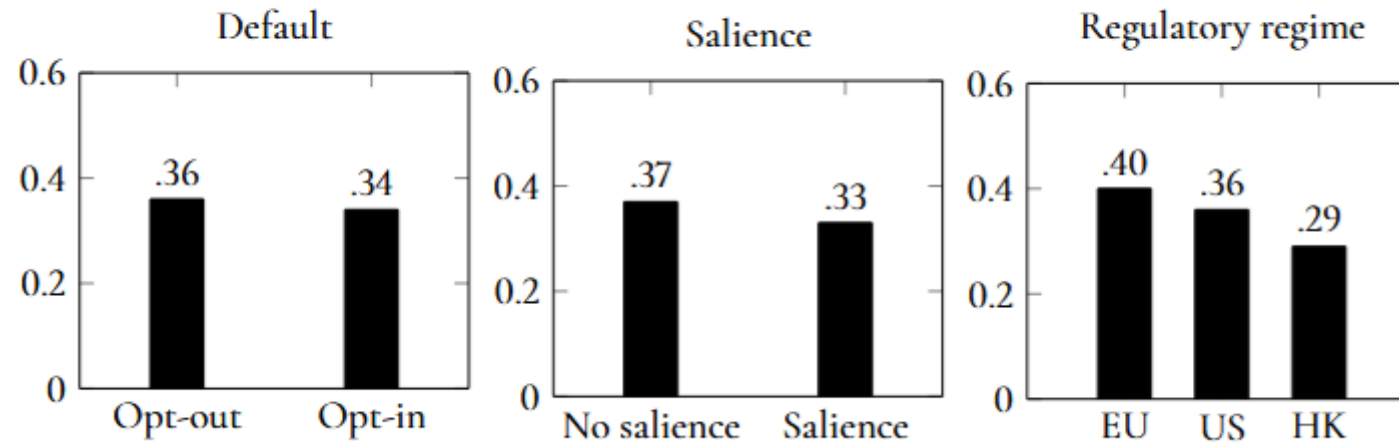
Hypothesis	Willingness to adopt Smart-Scan is higher, when...
H1 (Default)	it is activated by default
H2 (Salience)	less information about data privacy risks is provided
H3 (Regulatory regime)	data is better protected by law
H4 (Home bias)	data is stored in individuals' home jurisdiction
H5 (Privacy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

Experimental Design

- Randomized survey ran in April 2024 with 1,734 participants recruited from Prolific (890 from the US, 844 from Europe after excluding those who failed attention checks)
- 2(Default) x 2(Salience) x 3(Regulation) factorial design
 - Default: varies whether Smart-Scan needs to be activated by the user or it is automatically activated
 - Salience: varies whether subjects are given more detailed information on the privacy risk of using Smart-Scan (sharing their data as well as the data of contacts with whom they exchange emails)
 - Regulatory regime: varies the jurisdiction governing data protection by varying the location of the servers on which data is stored (EU, US, or Hong Kong)
- Measures of risk preferences and generalized trust (Falk et al. 2018, 2023)
- General concerns regarding the use of algorithms (Horowitz and Kahn 2021)
- Internet Privacy Concerns (IPC) scale (Hong and Thong 2013)
- Demographics
- (Pre-registered on OSF)

Findings

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

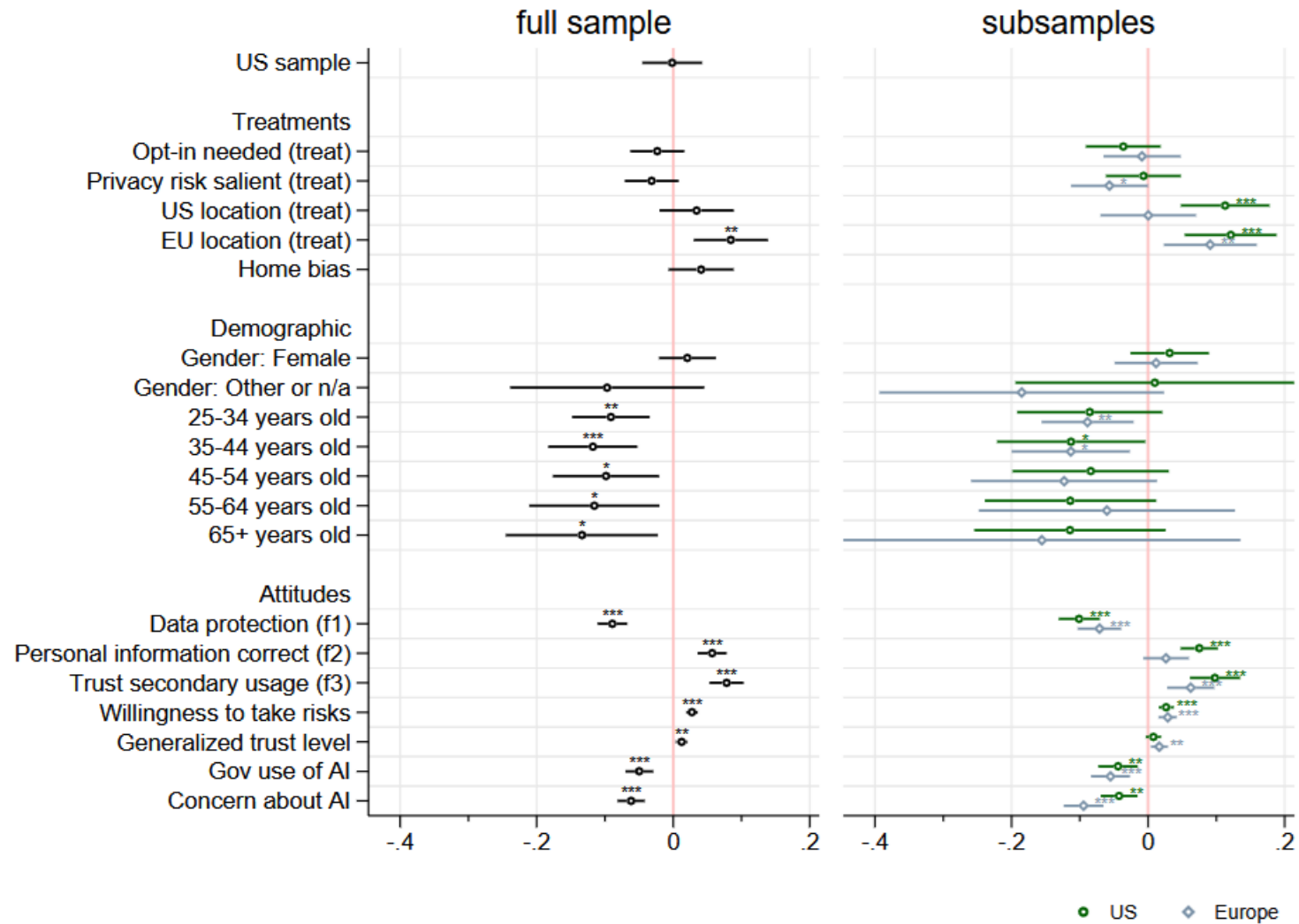


	(1)	(2)	(3)	(4)
Opt-in	-0.018 (0.023)	-0.018 (0.023)	-0.019 (0.022)	-0.023 (0.020)
Salient risk	-0.033 (0.023)	-0.035 (0.023)	-0.031 (0.022)	-0.032 (0.020)
US location	0.073 (0.028)**	0.041 (0.031)	0.039 (0.031)	0.034 (0.028)
EU location	0.113 (0.028)***	0.082 (0.031)**	0.083 (0.030)**	0.084 (0.028)**
Home bias		0.063 (0.028)*	0.063 (0.027)*	0.041 (0.024) ⁺
Data protection				-0.089 (0.011)***
Personal info correct				0.057 (0.011)***
Trust secondary use				0.078 (0.013)***
Risk propensity				0.027 (0.004)***
Generalized trust				0.012 (0.004)**
Gov use of algos				-0.050 (0.010)***
Concern about AI				-0.062 (0.010)***
Age/gender dummies	No	No	Yes	Yes
US sample dummy	Yes	Yes	Yes	Yes
N	1,734	1,734	1,734	1,734
R ²	0.016	0.020	0.055	0.300

Findings

- Willingness to use Smart-Scan is 8-11 percentage points higher if the data is stored in the EU rather than in Hong Kong
- Home bias (1 either if the participant lives in the US and the data is stored on servers in the US or if the participant lives in continental Europe and the data is stored on servers in the EU): a server located in one's home jurisdiction increases willingness to use by 4-6 percentage points
 - Estimated under the assumption that there is one homogeneous home bias – when we relax that assumption, we find significant home bias for US participants only

Figure 2: Willingness to use the app



Individual characteristics

- Factors from the IPC scale: participants who prefer strong data protection, who do not trust websites regarding the secondary use of data, or who do not care for websites to maintain correct personal data are less willing to use the app
- Risk preference and generalized trust: higher willingness to take risks and higher level of trust are both positively correlated with willingness to use Smart-Scan
- General attitudes towards algorithms and AI: participants who want governments to prioritize privacy concerns and who are generally concerned about AI are less likely to use Smart-Scan

Robustness tests

- Alternative dependent variables:
 - (i) how convinced participants are of Smart-Scan (5-point Likert scale)
 - (ii) how many other participants they expect to adopt it (five intervals: less than 20%, 20% to 39%, and so on)
 - The latter question is incentivized: five randomly selected participants who chose the correct interval received a bonus payment of £40 (about US\$50)
- Linear probability model (OLS) instead of probit specification
- Stricter participant inclusion criteria: salience reduces willingness to use Smart-Scan; US jurisdiction preferred to Hong Kong
- Extension: when manipulating salience of jurisdiction protection, results do not change (salience still does not matter)

Implications

- Jurisdiction matters
 - Stronger data protection afforded by GDPR and related legislation assuages concerns about sharing data with data-intensive applications
 - Either keep servers in the EU or extend EU-like protections to servers located in the US
- From a policy perspective, strict regulation in the EU may have de facto spillovers into other regions, with non EU-based organizations adopting tighter standards of protection for their customers worldwide
- Individual characteristics matter, so superior functionality alone may not be enough for a new product to penetrate a market if consumers have options

Thank you!

Q&A

lbrandimarte@arizona.edu