TAPP Transatlantic Privacy Perceptions

Policies, Practices, and Priorities: Transatlantic Experts' Perceptions on AI and Digital Privacy

—

RESULTS

Wave 7 (September 2025)

Isabela Coelho
Danylo Syrota
Aida Kreider

Executive Summary

Wave 7 of the Transatlantic Privacy Perceptions (TAPP) Panel, conducted from September 2025 to October 2025, presents insights from 57 privacy experts across Europe and the United States on the current state of digital privacy laws, their enforcement, and organizational practices. The results point to a growing divergence in views across the Atlantic, particularly regarding regulatory effectiveness, innovation, and expectations for future developments.

Transatlantic Gap Continues to Widen

Perceptions of digital privacy laws differ between the United States and Europe. In 2025, 96% of US respondents rated the current state of privacy laws as poor or fair, and optimism for improvement dropped to 4%, down from 45% in 2024. In Europe, 58% rated current privacy laws as good or excellent in 2025. However, expectations for future progress have declined, with more respondents shifting toward a neutral or cautious outlook.

Regulation and Innovation: Opposing Views

European experts increasingly view privacy regulation as a driver of innovation in privacy-preserving technologies. In 2025, 58% reported that laws encourage such innovation, up from 41% in 2024. The trend in the US moved in the opposite direction: only 24% expressed this view in 2025, down from 50% in 2024, with most respondents selecting a neutral response regarding the effect of regulation on innovation.

Scope and Enforcement Remain Areas of Debate

In the US, a stable and large majority (92% in 2025) continue to report that privacy laws cover fewer areas than needed. European responses are more varied. While the most common view remains that laws cover fewer areas than needed, the share of respondents perceiving them as too broad has increased over time.

Perceptions of enforcement also diverged further in 2025. In Europe, around 70% of respondents consistently view enforcement as somewhat or mostly effective. In the US, the share expressing confidence in enforcement declined, with two-thirds reporting that practices are enforced only a little or not at all.

Preferences for Policymaking Levels Differ

In 2025, 65% of US respondents preferred a combined federal-and-state approach to privacy policymaking, reversing the federal-only preference recorded in 2024. In Europe, views have remained stable, with 65% favoring EU-level policymaking only and no support for a member-state-only approach.

Organizations Viewed as Underperforming on Privacy

Organizational privacy practices continue to receive low ratings in both regions. In 2025, 92% of US and 79% of European respondents rated current practices as poor or fair. Looking ahead, pessimism rose in the US (73%), while Europe saw a shift toward neutral expectations. Public agencies received the highest privacy protection ratings, followed by traditional private companies, with private AI firms receiving the lowest ratings.

Table of Content

1 Introduction

In the privacy arena, actors from academia, policy, law, tech, journalism, and civil society influence debates, policies, and practices. The size and diversity of sectors, regional, legal, and cultural contexts in the privacy arena presents a challenge for systematically synthesizing its members' conversations and opinions. The Transatlantic Privacy Perceptions (TAPP) project aims to help companies and policymakers learn more about current and future digital privacy concerns and how they can best be addressed through legislation and technology. To this end, it follows and analyzes developments in privacy actors' attitudes, expectations, and concerns around current and emerging issues in digital privacy over time. It is an interdisciplinary research project in privacy, survey methodology, and complex sampling techniques at the Universities of Maryland (UMD) and Munich (LMU).

Conducted since 2022, the survey gathers insights from privacy experts across the United States and Europe to assess the state of data protection, the performance of tech companies, and the impact of artificial intelligence (AI) on privacy policies. The focus of Wave 7 of the Transatlantic Privacy Perceptions (TAPP) Panel, conducted between 17 September 2025 and 15 October 2025, is the Panel's annual module on the current state and effects of privacy laws, regulations, and practices - particularly those related to digital privacy - within the context of respondents' respective countries of work. Respondents are asked to reflect on how these privacy frameworks influence their business operations, highlighting both challenges and areas of progress.

Wave 7 is the TAPP trend analysis that repeats survey items previously asked in Wave 5 (September 2024) and Wave 2 (August 2023). The survey was programmed and distributed using Qualtrics, ensuring compliance with both the EU General Data Protection Regulation and the University of Maryland's ethical standards.

2 Respondents Profile

Fifty-seven individuals provided complete or partial[1] responses, the majority of which were returning respondents (Table 1). An additional 13 individuals began but did not complete the Wave 7 survey; we therefore exclude these individuals from analysis. Compared to the previous trend wave, the number of new respondents was lower: seven valid respondents in Wave 7 compared to 17 in Wave 5.

[1] AAPOR guidelines suggest defining complete interviews (AAPOR 1.1) as greater than 80% of all applicable questions answered and/or 100% of all crucial questions answered, with partial interviews (AAPOR 1.2)

	Completed surveys	Partial completes	Incompletes
Returning respondents	19 (50%)	11 (57.9%)	2 (15.4%)
Previous non-respondents	15 (39.5%)	5 (26.3%)	5 (38.5%)
New respondents	4 (10.5%)	3 (15.8%)	6 (46.1%)
Total	38 (100%)	19 (100%)	13 (100%)

Table 1. Survey participation by respondent type

Of the 57 included respondents, 24 (42%) reported greater familiarity and knowledge with the privacy context in the United States (US), 24 with Europe[2], and seven with other regions, specifically Brazil and Canada. Due to the small number of experts from regions other than the US and Europe, we focus on the 50 respondents from these two areas only.

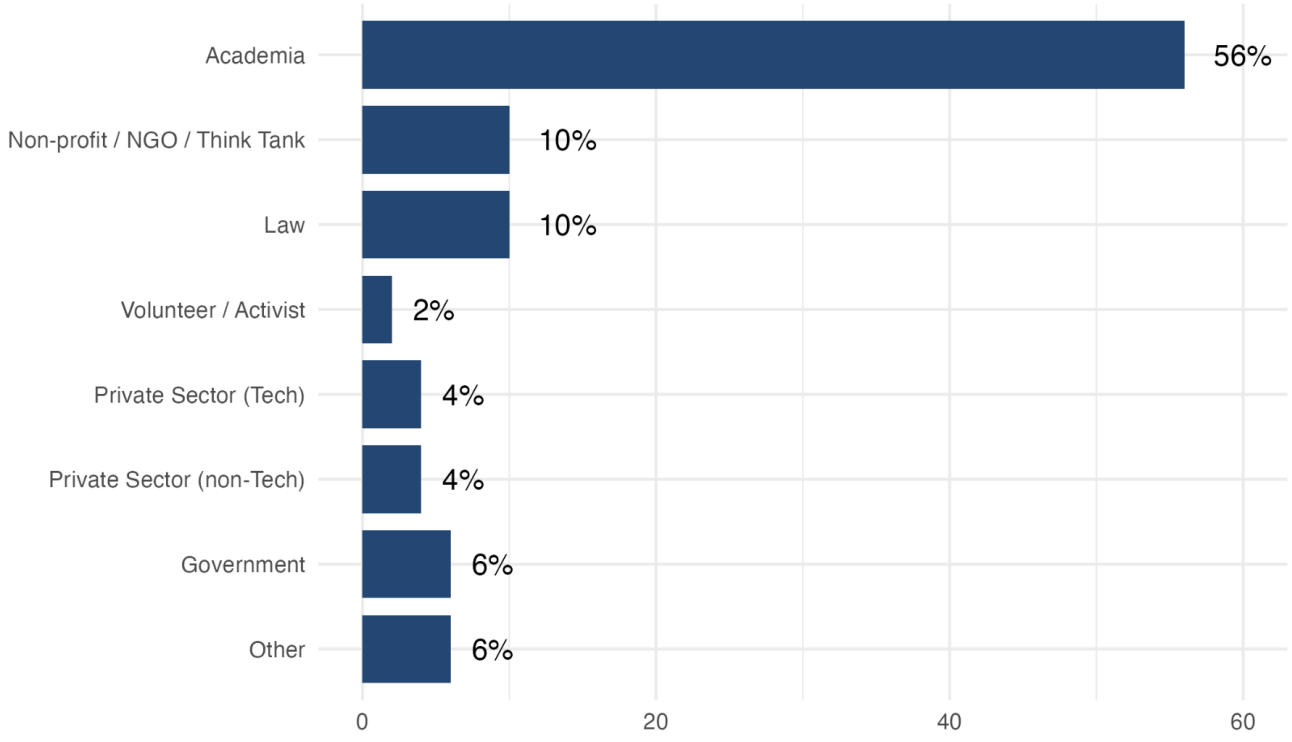

Figure 1. US and Europe respondents' composition by sector

In terms of professional background, the majority (56%) are from academia with an additional 20% evenly divided between non-profits / NGOs / Think tanks, and from law (Figure 1). This marks a shift towards more academic respondents; in the previous trend wave (Wave 5), only 35% of respondents were from academia, with an additional 28% of respondents evenly divided between the tech industry, and the private sector

[2] We include here both individuals with familiarity and knowledge of individual European countries or the EU generally.

outside the tech industry. From Figure 2, we note that 46% of respondents have worked in the privacy field for more than 10 years, and none of them have worked for less than three years. This likely reflects the experience of our respondents, as the previous trend wave (Wave 5, September 2024) included nine percent with respondents of less than three years experience.

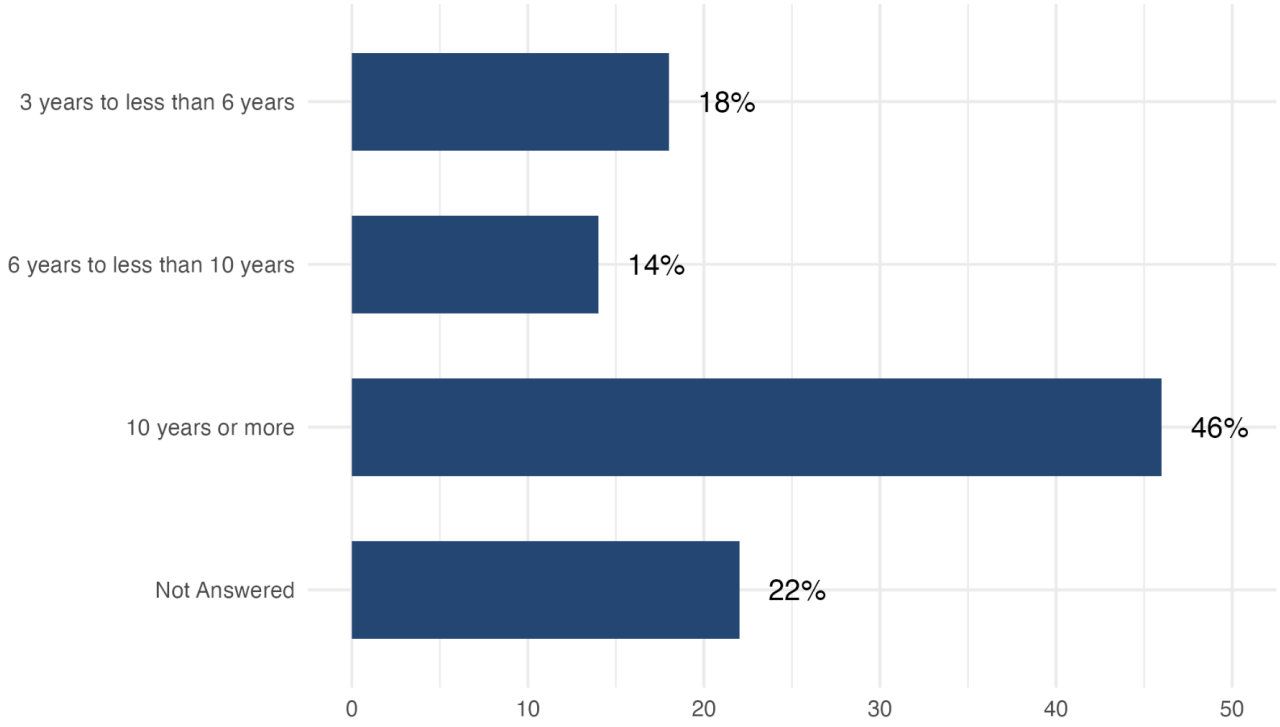

Figure 2. Respondents' composition by years of experience with privacy

3 Results

3.1 Balance of interest in digital privacy laws

The comparison of interest in digital privacy laws reveals relevant regional differences. In Europe, public perception has shown significant fluctuation (Figure 3). While the percentage of respondents believing laws favor individual users increased from 45% in 2023 to 75% in 2024, it fell again to 46% in 2025, returning to the Wave 2 (August 2023) level.

Conversely, in the US, the perception that laws favor businesses remains overwhelmingly high and consistent, at 92% in 2023, 86% in 2024, and 85% in 2025. This underscores the divergent perspectives on privacy laws on either side of the Atlantic. While sentiment in the US remains stable in its view of a business-friendly legal environment - despite the introduction of state-level consumer privacy protection - the proportion of Europeans who believe laws favor individual users has remained substantially higher than in the US across all three years (Figure 3).

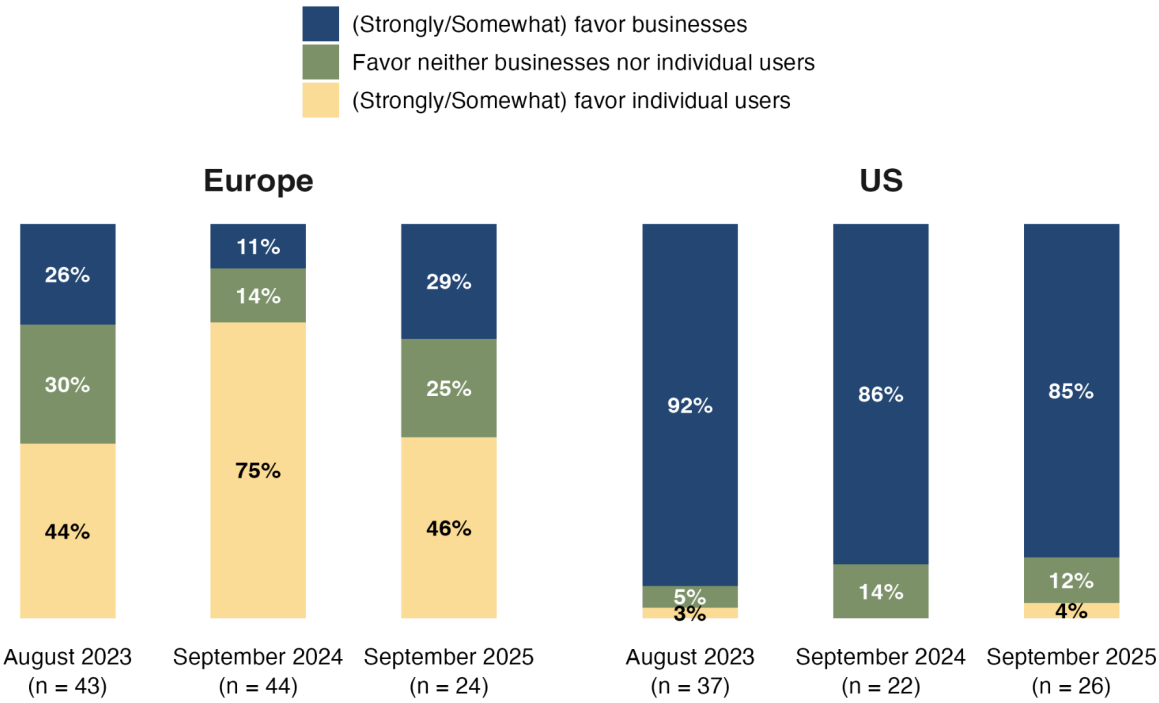

Figure 3. Balance of interest in digital privacy laws

3.2 Influence of laws on the development of privacy-preserving practices and technologies

Wave 7 data also reveals a divergence in how the impact of privacy laws on innovations is perceived in Europe versus the US, with trends observed in 2024 reversing in 2025 (Figure 4). Despite a reduction in 2024 from 50% in 2023 to 41% in 2024, in 2025, 58% of the European experts think that digital privacy laws and regulations in Europe strongly or somewhat encourage innovation and development of privacy-preserving practices and technologies in organizations. Alongside this trend, the view that these laws discourage innovation continued to steadily decline, falling to 17%.

However, in the US, the optimism seen in 2024 has dissipated. The percentage of respondents who believe privacy laws encourage innovation and development of privacy-preserving practices and technologies in organizations dropped from 50% in 2024 to 24% in 2025, returning to its 2023 level. Opinion shifted dramatically towards neutrality, with the "neither encourage nor discourage" category soaring from 28% in 2023 and 14% in 2024 to 56% in 2025. In conclusion, European experts increasingly view privacy regulations as a catalyst for innovation, while the prevailing sentiment among US experts has shifted from a mix of strong opinions to one of overwhelming neutrality (Figure 4).

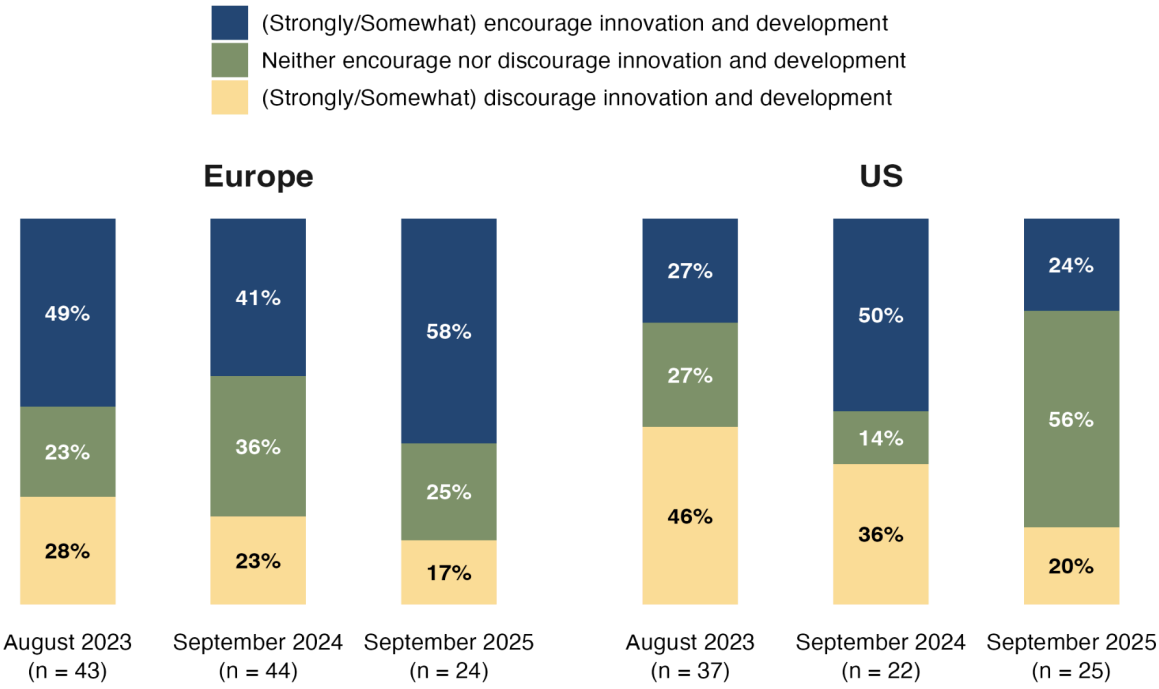

Figure 4. Influence of laws on the development of privacy-preserving practices and technologies

3.3 Comprehensiveness of digital privacy laws

There is a notable difference between stakeholders in Europe and the US regarding whether digital privacy laws cover the necessary areas (Figure 5). In Europe, while the belief that laws cover “fewer areas than needed” remains the most common response, it has decreased from a majority of 58% in 2023 to 43% in 2024 and 46% in 2025. Concurrently, there is a growing sentiment that the laws are either adequate or even excessive in areas: the perception that laws are too comprehensive (“more areas than needed”) has shown a steady increase over the period, growing from 14% in 2023 to 18% in 2024 and 21% in 2025, while the view that they cover “all areas needed” moved from 28% in 2023, 39% in 2024 and is 33% in 2025.

In the US, there is a stable consensus that current digital privacy laws are not comprehensive enough: the vast majority of respondents believe current laws cover "fewer areas than needed," with this view holding at 94% in 2023, 95% in 2024, and 92% in 2025. Similarly, very few respondents feel current laws are adequate ("all areas needed" registered between 4-6%), and the belief that the laws are too comprehensive ("more areas than needed") only registered a minimal 4% in 2025. This indicates a persistent and widespread demand for more extensive privacy legislation in the US.

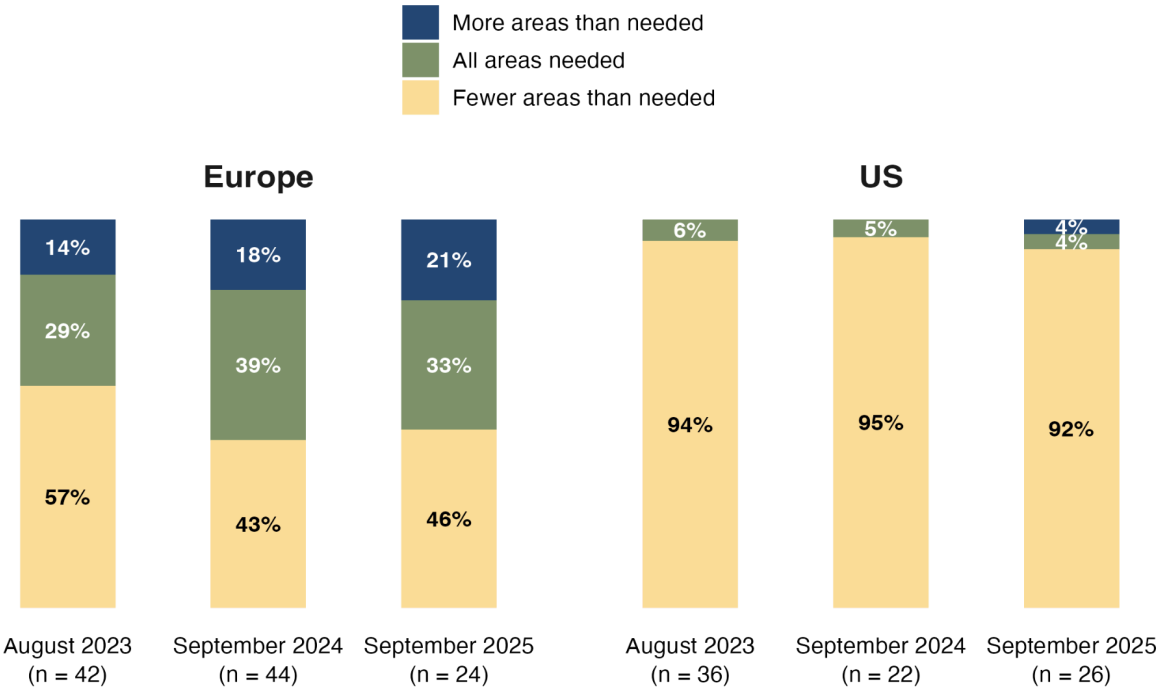

Figure 5. Comprehensiveness of digital privacy laws

3.4 Enforcement of digital privacy practices

The data on the perceived enforcement of digital privacy practices reveals a growing divergence between Europe and the United States, with European confidence remaining stable while American confidence has notably declined (Figure 6). In Europe, a strong majority of respondents consistently express confidence that digital privacy practices are being enforced. The combined percentage of those who feel practices are mostly or somewhat enforced has remained stable at approximately 70% across all three years (73% in 2023, 70% in 2024, and 70% in 2025). While the overall confidence level is steady, there was a shift in its composition; a spike in respondents feeling practices were mostly enforced in 2024 (27%) dropped in 2025 (12%).

The perception of enforcement in the US has meanwhile dropped sharply. After two years of being evenly split—with 50% expressing high confidence (mostly or somewhat) and 50% expressing low confidence (a little or not at all) in both 2023 and 2024—there is a sharp shift in 2025. In 2025, the proportion of respondents with high confidence dropped to 34% (15% mostly and 19% somewhat). Correspondingly, the view that practices are poorly enforced became the clear majority, with 66% now believing they are enforced a little (62%).

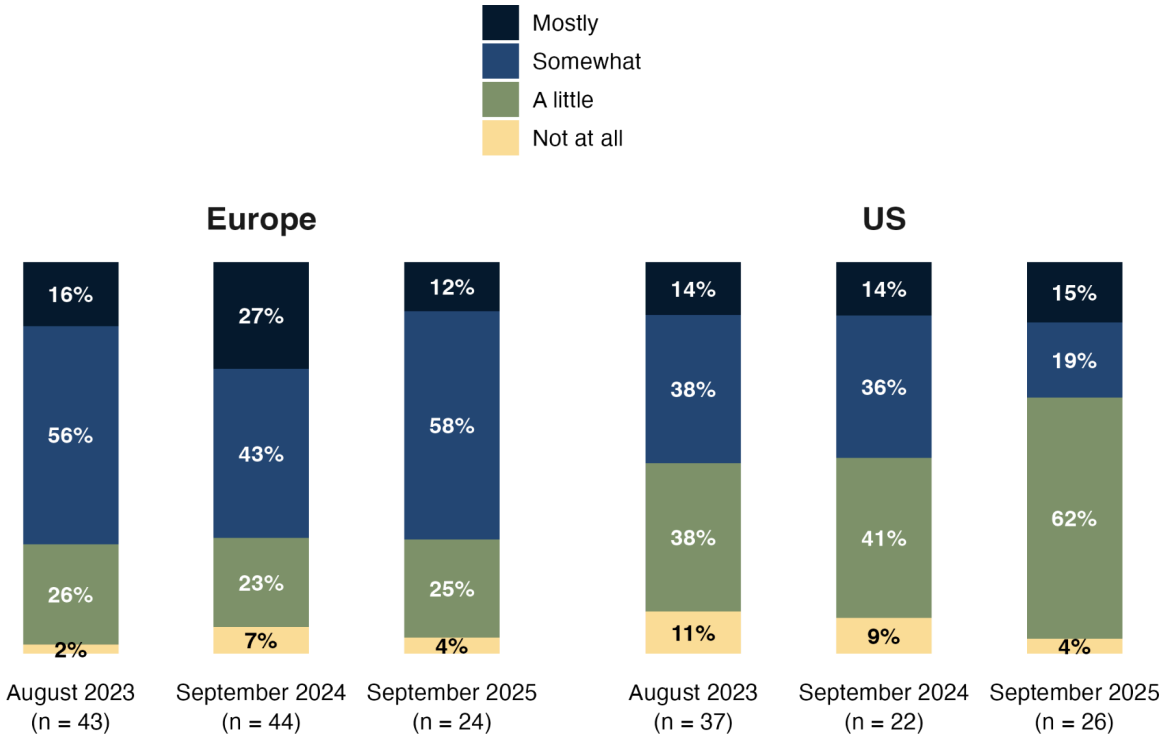

Figure 6. Enforcement of digital privacy practices

3.5 Current and future outlook of digital privacy laws

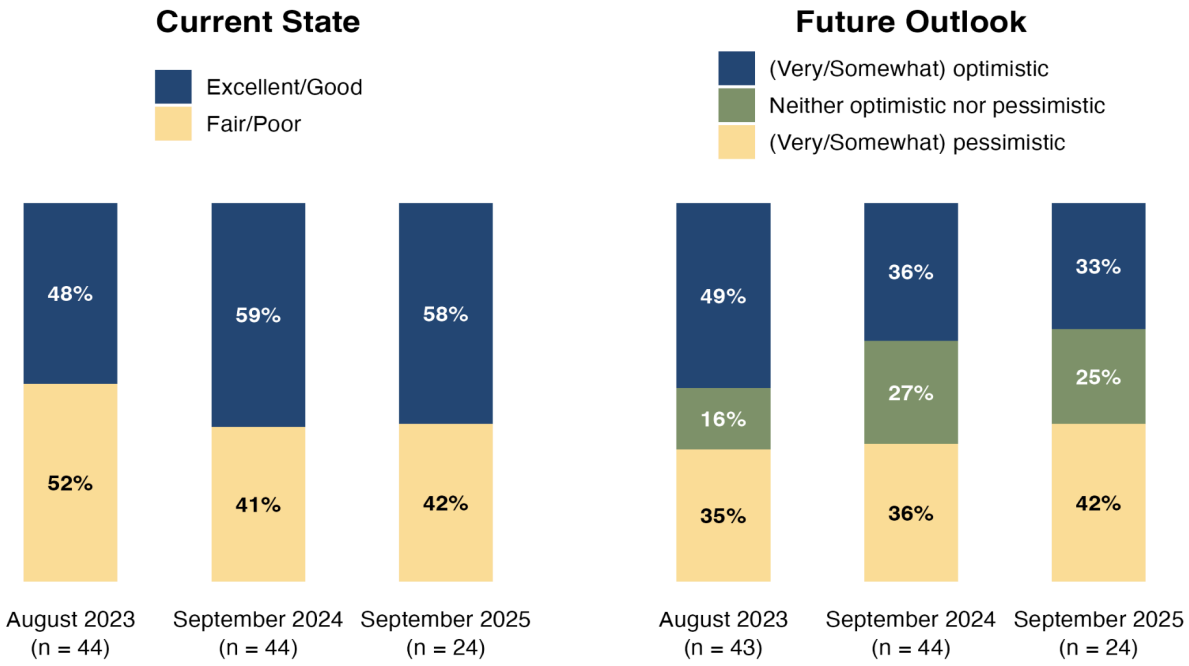

Figure 7. Current state and future outlook of digital privacy laws and regulations in Europe

The current state and future outlook of digital privacy laws and regulations reveal a stark chasm between European and American perceptions. A majority of the privacy experts in the European scenario view their current enforcement positively. The excellent/good rating had held strong at 58% in 2025, aligned with 59% in 2024 and 49% in 2023 (Figure 7). However, this satisfaction with the present state does not translate to future confidence.

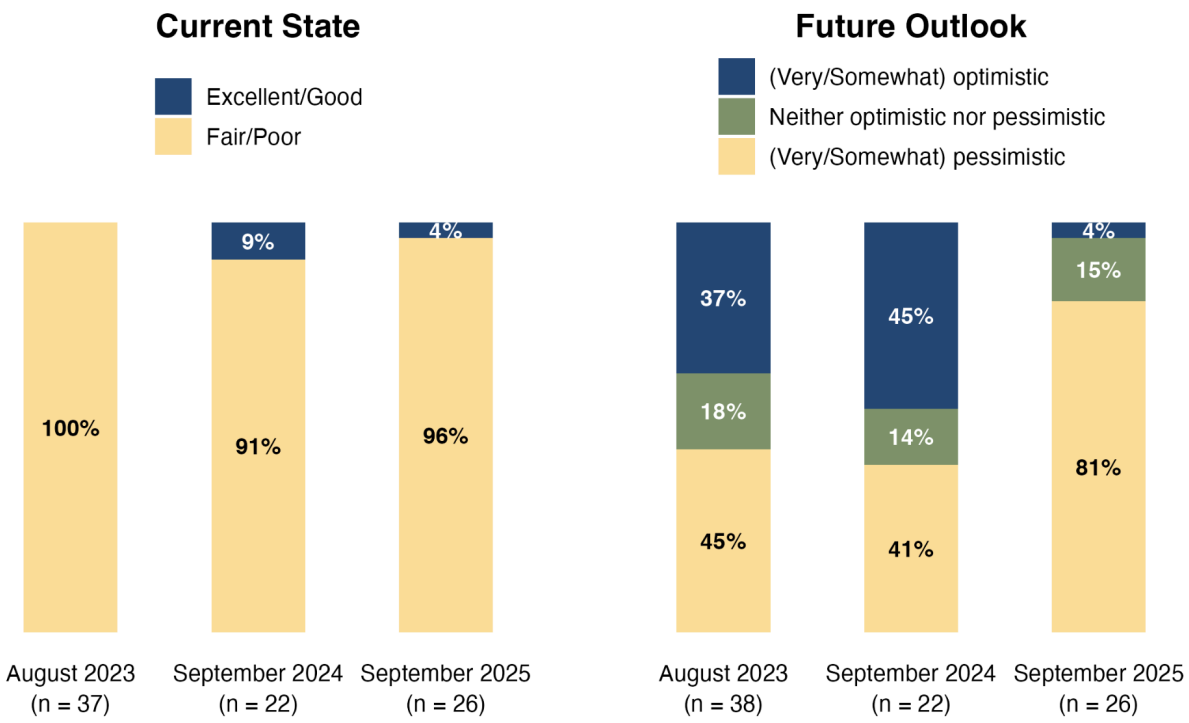

Figure 8. Current state and future outlook of digital privacy laws and regulations in US

The view from the experts in the US context is defined by near-universal dissatisfaction. Perceptions of the current state are overwhelmingly negative, with the percentage of privacy experts rating it as fair or poor holding at 96% in 2025, consistent with 91% in 2024 and 100% in 2023 (Figure 8). Effectively, almost no experts in the US context have viewed the current state of privacy laws and regulations as excellent or good over the three-year period. This negativity has now extended to the future outlook, in what is the most dramatic shift in the data. After showing some optimism in 2024 (45%) and in 2023 (38%), optimism collapsed to 4% in 2025. This sentiment was almost entirely transferred to pessimism, which surged from 41% to 81%, indicating a profound loss of confidence in the future of American privacy enforcement.

3.6 Policymaking approaches in digital privacy protection

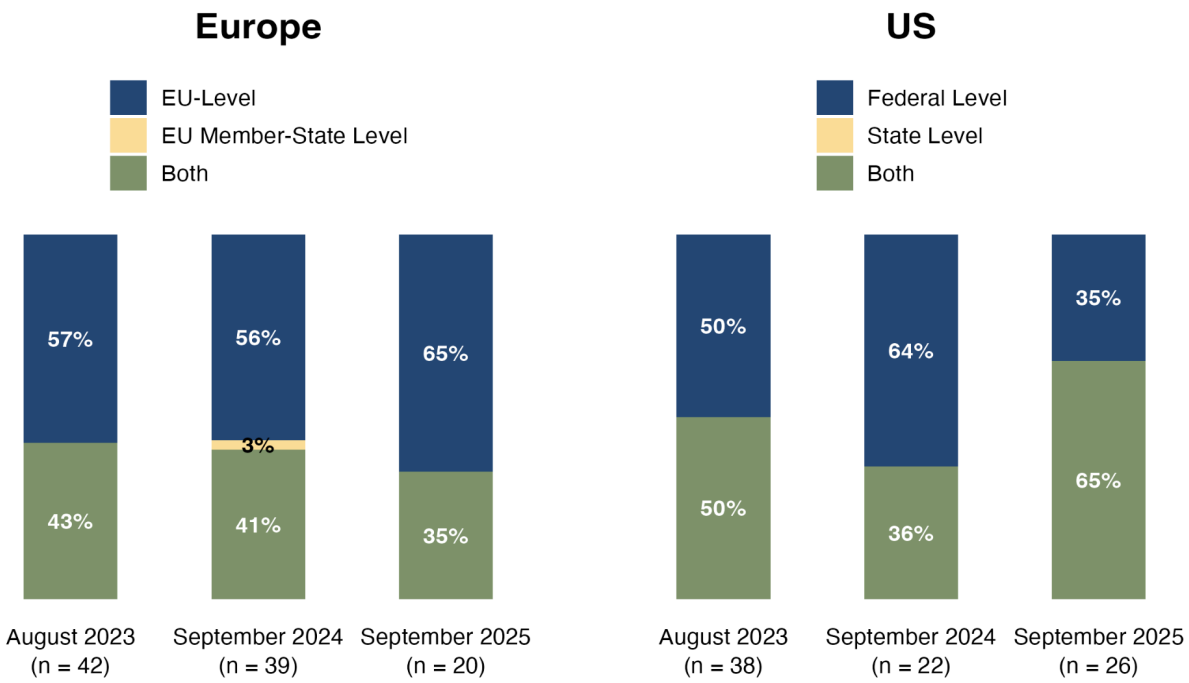

Figure 9. Policymaking approaches in digital privacy protection

The results of Wave 7 show that results from Europe remain relatively stable, with 65% of respondents supporting an EU-level approach only, and 35% favor a combination of both levels (Figure 9). However, in the US, 35% of respondents believe that a digital privacy policy should be established at the federal level, while 65% think it should be at both the state and federal levels. This is contrary to the results in 2024, where the opposite is true, where 64% of respondents believe that a digital privacy policy in the US should be established at the federal level, while 36% think it should be at both the state and federal levels. Therefore, no clear trend is visible here; however, it can be stated that no respondent from the US thinks it should be at the state level alone.

3.7 Current and future outlook of organizational digital privacy practices

Regarding the overall assessment of organizations' digital privacy policies and practices (Figure 10), the current state remains negative in Europe for 2025 at 79% for a poor or fair rating, compared to 75% for 2024 and 76% for 2023. Similarly, while there is a small increase in very or somewhat pessimistic responses with regard to the future outlook practices, the percentage of respondents reporting very or somewhat optimistic responses has dropped from 55% in Wave 2 (2023) to 21% in Wave 7.

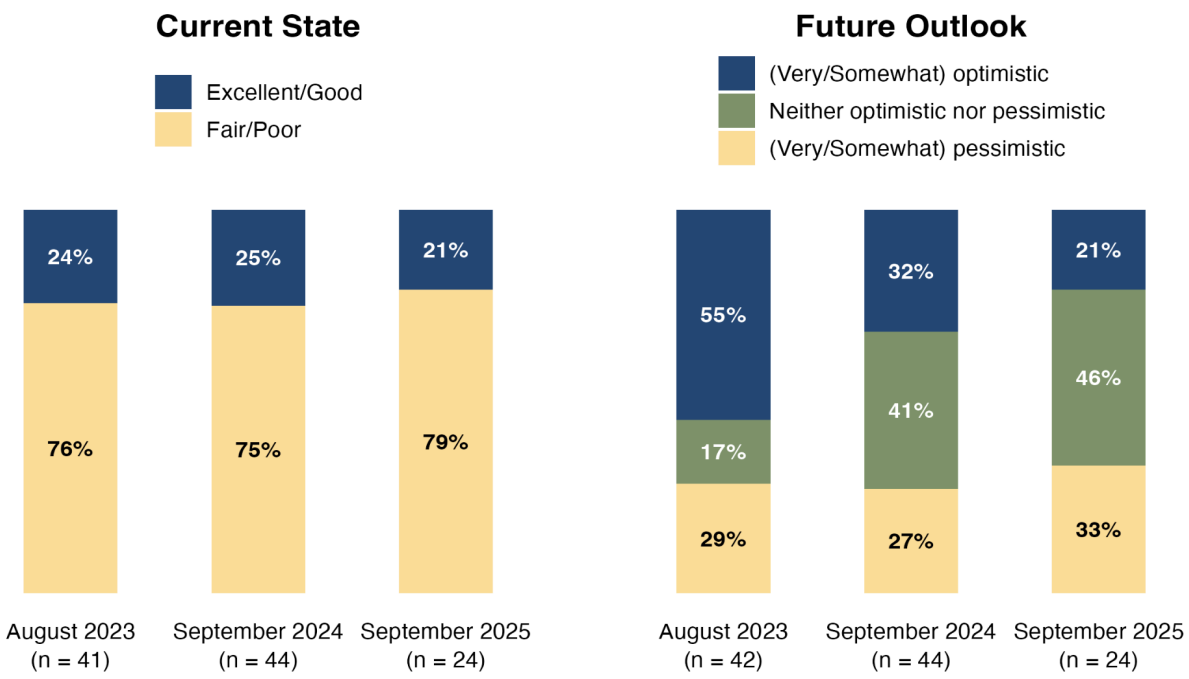

Figure 10. Current and future outlook of organizational digital privacy practices in Europe

In the US, 92% of respondents rated the current state of organizational digital privacy practices as poor or fair in 2025, remaining steady compared to 95% in 2024 and 91% in 2023 (Figure 11). However, pessimism regarding future practices has increased from 57% in Wave 2 (2023) to 73% in Wave 7 (2025).

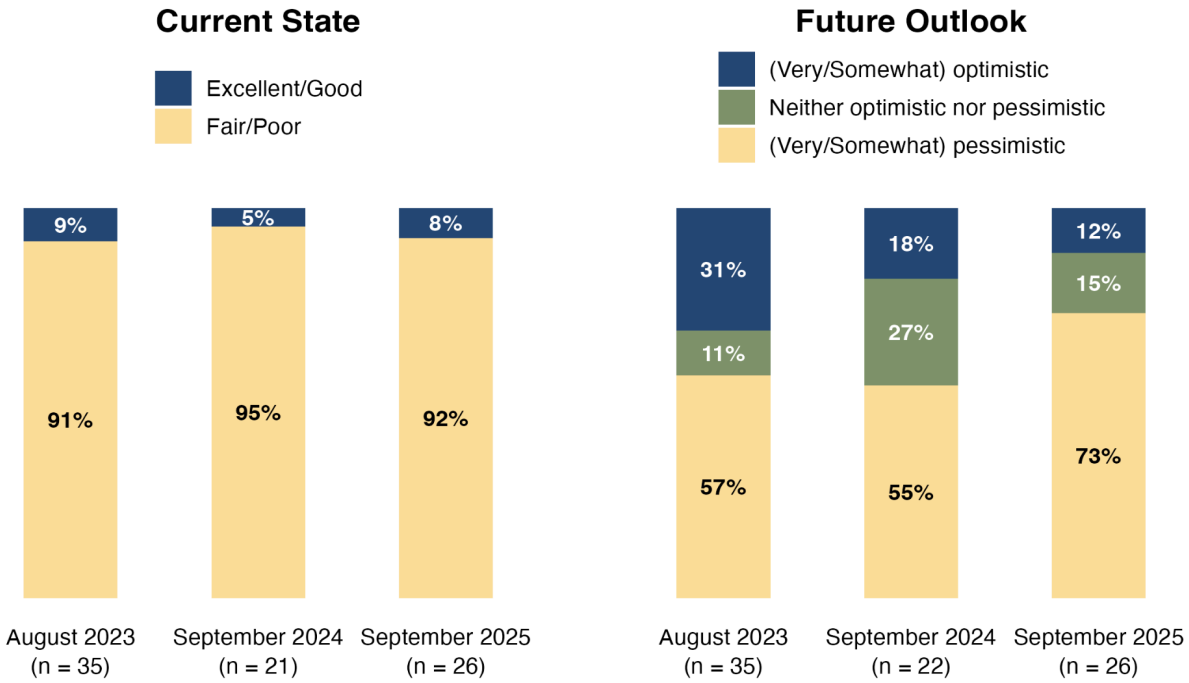

Figure 11. Current and future outlook of organizational digital privacy practices in US

3.8 Stakeholder ratings of organizations' privacy protection performance

Regardless of region, public organizations such as country statistical agencies, tax authority, and social security authority are better evaluated according to their privacy protection performance than private companies. Here, a differentiation can be made between private companies[3] and private AI companies[4], which are mainly known for their AI products.

The ratings between respondents for Europe and the US show similar results across all the depicted sectors, with higher ratings for government agencies. In Europe, 22% of the respondents evaluate the privacy protection performance of public institutions as excellent, compared to 19% for the US (Figure 12a). On the other hand, 54% of the respondents from Europe and 54% from the US evaluate the privacy protection performance of private organizations as poor. Similarly, 76% of respondents from Europe and 81% from the US evaluate the privacy performance of private AI organizations as poor.

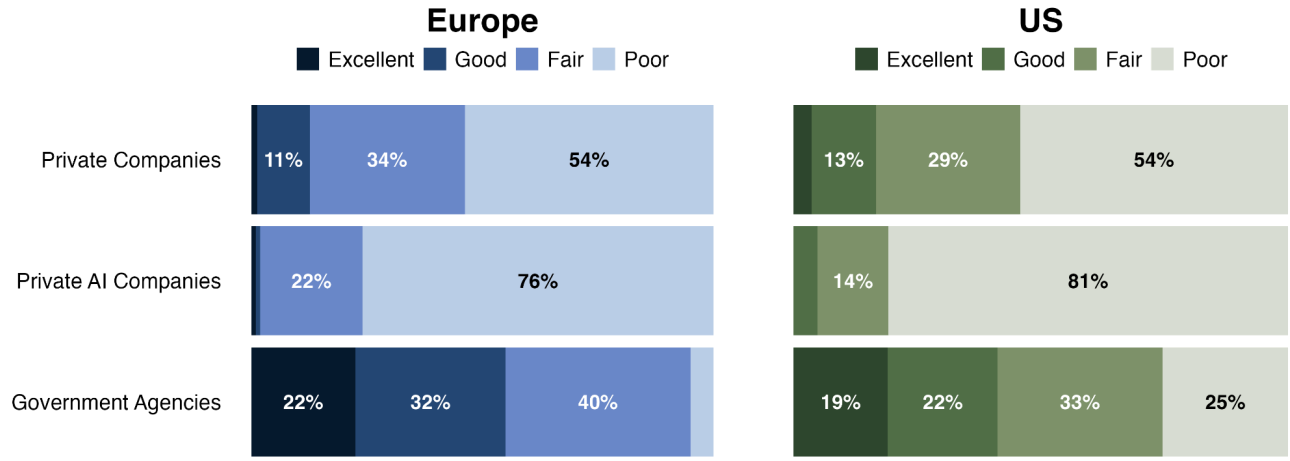

Figure 12a. Organizations' privacy protection performance ratings - September 2025

However, ratings from Wave 7 are markedly lower compared to Wave 5 results (2024; Figure 12b), for private companies and government agencies in both Europe and the US. No comparison can be made with private AI companies, as they were not part of the panel survey in 2024.

[3] Private companies include Meta, Google, Amazon, Visa, Mastercard, Apple, and Microsoft.
[4] Private AI companies include Alibaba, Anthropic, DeepSeek, Mistral AI, Open AI, Tesla, and xAI.

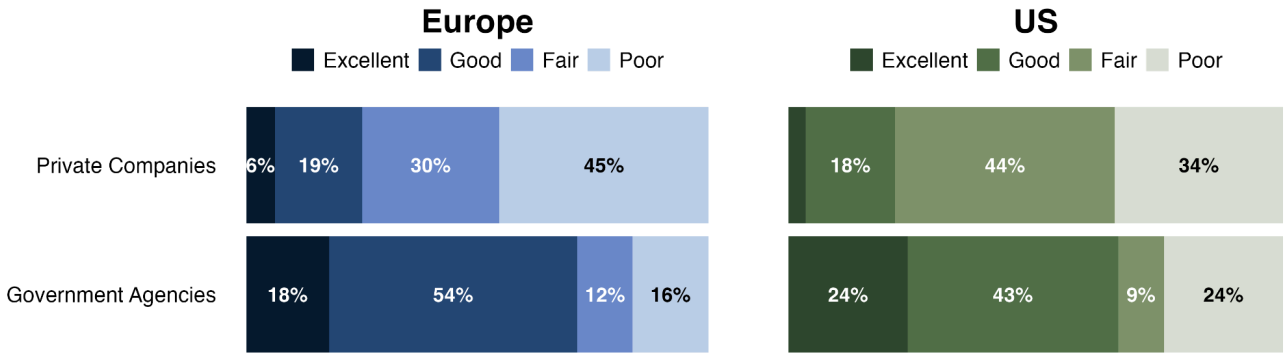

Figure 12b. Organizations privacy protection performance ratings - September 2024

For the first available comparison of private AI organizations, European respondents rate these organizations more positively overall than American respondents. Within the European context (Figure 13), Anthrophic performed better compared to its peers, with 16% of privacy experts in the European context classifying it as excellent or good, and another 50% rating it as fair. Of the other private AI organizations, only Mistral AI receives a majority positive rating, with 54% of European respondents rating it as fair compared to 46% as poor.

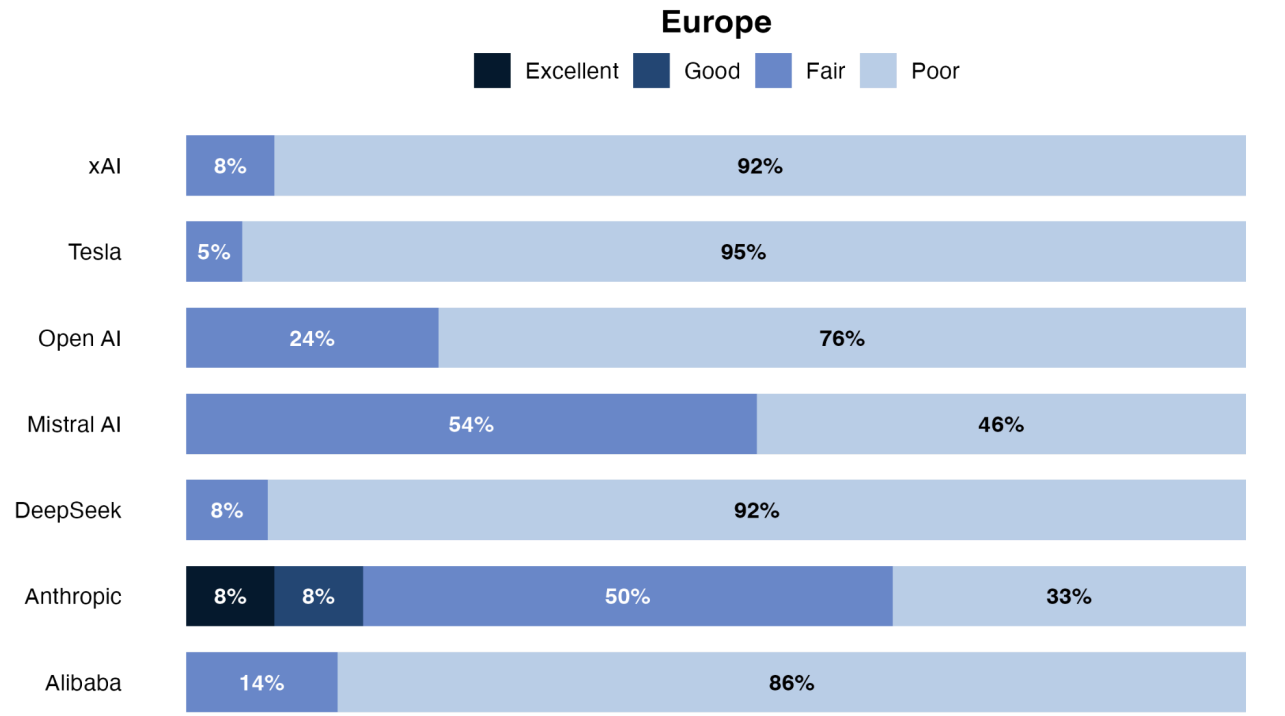

Figure 13. Private AI organizations privacy protection performance ratings in Europe - September 2025

However, in the US (Figure 14), perceptions show slightly more differentiation in their ratings, though the overall sentiment remains overwhelmingly negative, with no private AI companies rated as better than good, and no companies receiving less than a 70% poor rating (Anthropic). The detailed plots regarding other companies and government agencies are displayed in the Appendix.

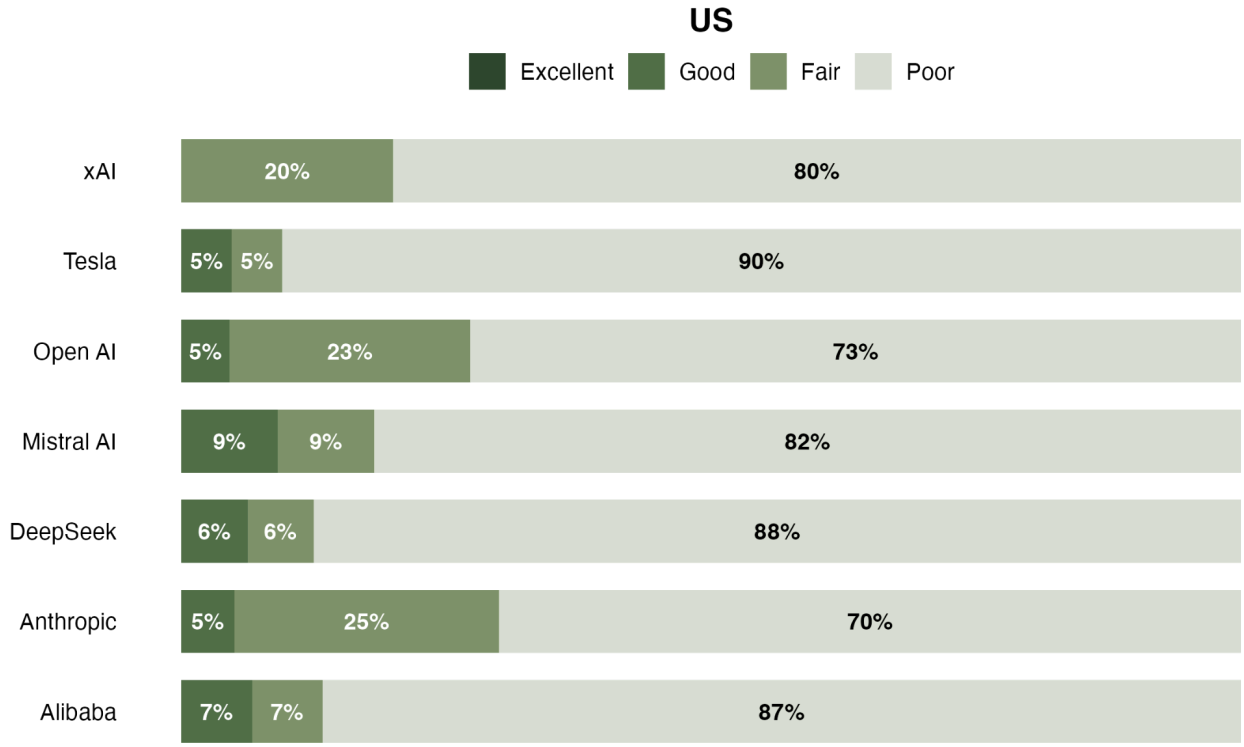

Figure 14. AI organizations privacy protection performance ratings in US - September 2025

Appendix

A.1 Detailed Plots of Stakeholder ratings of organizations' privacy protection performance

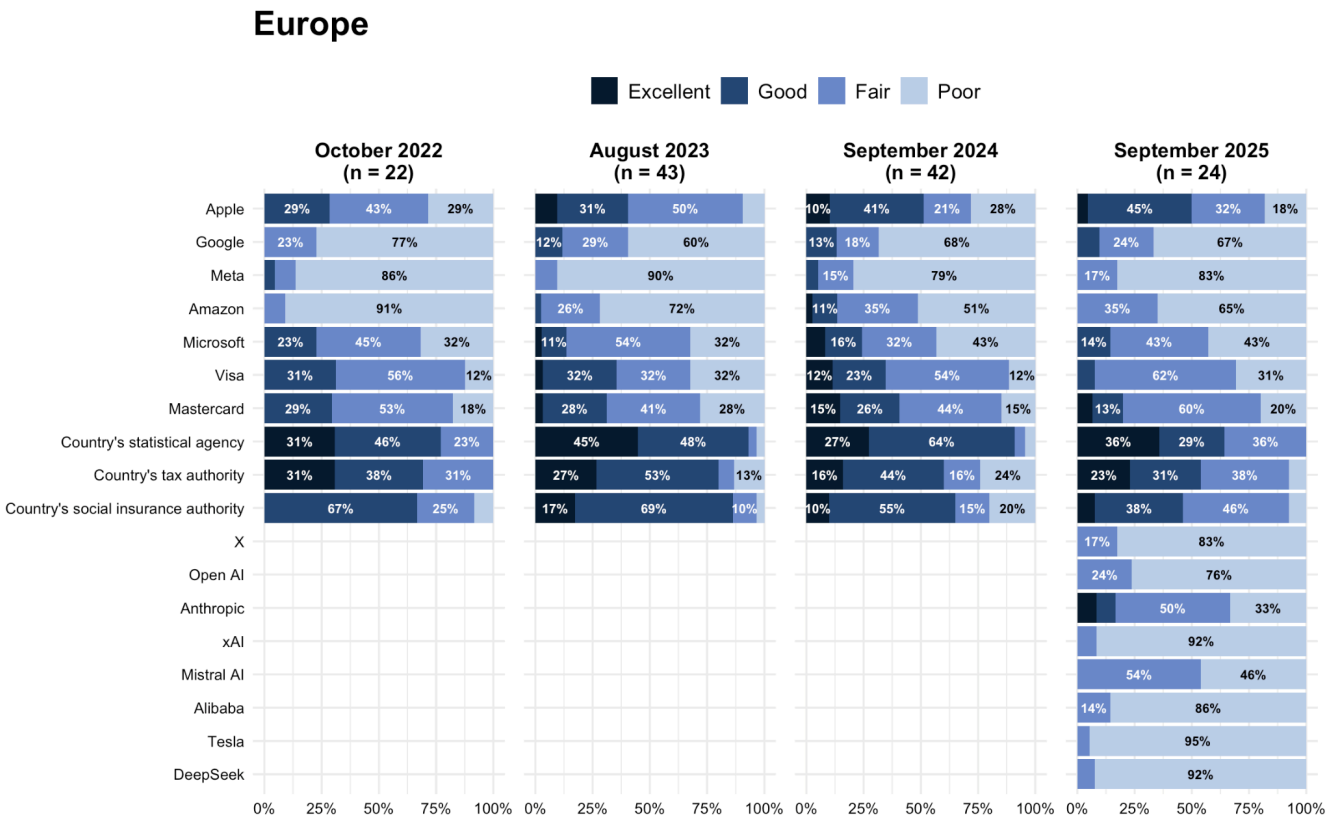

Figure A1. Privacy protection performance ratings over time - Europe

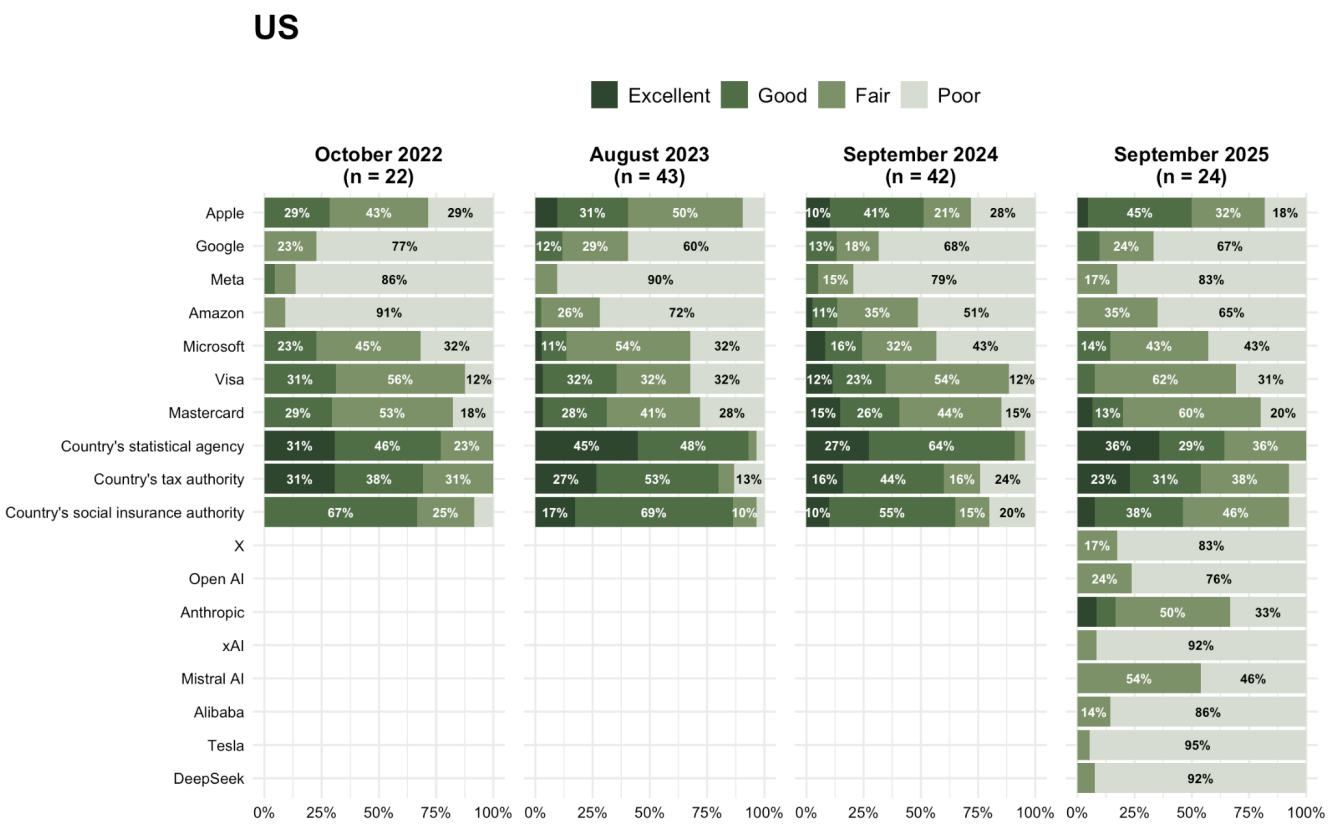

Figure A2. Privacy protection performance ratings over time - US

A.2 TAPP Panel Questionnaire Wave 7

[Introduction]

This survey is about **digital privacy**. Your answers will provide valuable **information to policymakers, companies, and the public**. (For more information about the project, see www.privacyperceptions.org.)

This survey will take about **5-7 minutes** to complete.

Your participation in this survey is entirely voluntary. You may skip any question you do not wish to answer and may stop taking the survey at any time. All of your responses are **confidential** and will be analyzed solely for the purpose of this research.

By continuing, you confirm that you are 18 years or older and understand the above, and consent to take part in this survey.

"Start Survey" button

"Data protection statement" button

[PRG: Data protection statement available as pop-up linked from "Data Protection Statement"]

in collaboration with Ludwig-Maximilians-Universität München

Data protection statement

TAPP is an interdisciplinary research project conducted at the Universities of Maryland (UMD) and Munich (LMU).

Data collected through the survey is protected in line with EU GDPR (see here for more information) and the requirements outlined by the UMD research ethics committee (IRB). Data published in reports will be aggregated and will not individually identify you or your responses. In line with the open science movement, we will make selected survey data available for research purposes. No identifying information will be contained in this dataset.

Survey Participation

You will be asked if you would like to participate in future waves of this survey. If you agree to participate in future waves of this survey, you will receive an email with a link to an equally short web survey about three times a year for the next two years.

Participant Rights

If you have any questions about the study or how you can exercise your data protection rights, please contact us at info@privacyperceptions.org and/or the Principal Investigator Frauke Kreuter, Ph.D. (University of Maryland) at fkreuter@umd.edu.

This research has been reviewed according to the University of Maryland, College Park IRB procedures for research involving human subjects.

If you have questions about your rights as a research participant or wish to report a research-related injury, please contact with reference to IRB No. 1934146-4:

University of Maryland College Park
Institutional Review Board Office
1204 Marie Mount Hall
College Park, Maryland, 20742
E-mail: irb@umd.edu
Telephone: +1 301-405-0678

For more information regarding participant rights, please visit:
https://research.umd.edu/research-resources/research-compliance/institutional-review-board-irb/research-participants

----------Page break----------

[PRG: No mandatory questions except those listed below. Instead, show warning if clicking “next” and no answer selected (except for open-ended questions and recruitment questions).
Mandatory questions: screeninterest, region, region_country, experience, sector_paid, sector, name]

[PRG: Never offer “go back” button]

[PRG: Keep scale direction randomizations consistent across questions within each individual respondent]

[PRG: One question per page unless specified otherwise]

[purple: recruitment questions, not asked to returning respondents unless specified otherwise]

RespondentID [PRG: Embedded data field: Respondent ID (from Contact List)]

[Screener]
[PRG: Ask only Tier 2 and Tier 3 (from Contact List), and only first time. Mandatory question]
screen_interest
Which of the following statements best applies to you?
[PRG: Single choice]

- ☐ I have only a **personal** interest in privacy-related topics.
- ☐ I have only a **professional** interest in privacy-related topics.
- ☐ I have **both a personal and a professional** interest in privacy-related topics.
- ☐ None of the above

screen_privacy

[PRG: Ask if screen_interest is “I have only a personal interest” or “None of the above”

Do you take privacy into consideration as part of your work?

- ☐ Yes
- ☐ No

[PRG: SCREEN OUT if screen_interest is “I have a personal interest” or “None of the above” AND screen_privacy is “No”. Display text as specified in [End] and END survey]

[Demographics: Regional Expertise]

[PRG: Ask all, but only first time. Mandatory question]

region

When it comes to privacy issues, with which of the following policy contexts are you most familiar?

[PRG: Single choice]

- ☐ [region_europe] Europe
- ☐ [region_us] United States
- ☐ [region_both] Both Europe and the United States
- ☐ [region_other] Another country or region: _____ [PRG: Specify]

[PRG: Same page]

[PRG: Ask if region is “Both”]

[PRG: Ask only first time. Mandatory question]

region_both

In which of the two regions do you think you have more influence?

[PRG: Single choice]

- ☐ [europe] Europe
- ☐ [us] United States

[PRG: Same page]

[PRG: Ask if region is “Europe” or region_both is “Europe”]

[PRG: Ask only first time. Mandatory question]

region_country

And which European country in particular?

[Alphabetic drop-down of all countries in Europe, add “EU-level” at top of list]
[PRG: Single choice]
[PRG: Same page]
[PRG: Embedded field]
EU
[PRG: EU = “Yes” if region_country is one of the following: EU-level, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden; “No” otherwise]

[Main Questionnaire]

[Laws & Regulations / Public Policy]
[PRG: New page]
[PRG: Ask all]
law_favor_tech
Do you think digital privacy laws and regulations in [the US / the EU / country] more strongly favor the rights and needs of businesses or of individual users?
[PRG: Insert “the US” if region is “United States”, “the EU” if EU is “Yes”, else: insert country from region_country or region_other]
[PRG: Randomize scale direction]
[PRG: Single choice]

- ☐ Strongly favor businesses
- ☐ Somewhat favor businesses
- ☐ Favor neither businesses nor individual users
- ☐ Somewhat favor individual users
- ☐ Strongly favor individual users

law_innovation
Do you think digital privacy laws and regulations in [the US / the EU / country] encourage or discourage innovation and development of privacy-preserving practices and technologies in organizations?
[PRG: Insert “the US” if region is “United States”, “the EU” if EU is “Yes”, else: insert country from region_country or region_other]
[PRG: Randomize scale direction]
[PRG: Single choice]

- ☐ Strongly encourage innovation and development
- ☐ Somewhat encourage innovation and development
- ☐ Neither encourage nor discourage innovation and development

- ☐ Somewhat discourage innovation and development
- ☐ Strongly discourage innovation and development

law_breadth

Do you think digital privacy laws in [the US / the EU / country] cover more areas than needed, fewer areas than needed, or all areas needed?

[PRG: Insert “the US” if region is “United States”, “the EU” if EU is “Yes”, else: insert country from region_country or region_other]

[PRG: Randomize scale direction]

[PRG: Single choice]

- ☐ More areas than needed
- ☐ All areas needed
- ☐ Fewer areas than needed

[PRG: Ask if law_breadth is “More areas than needed”]

law_breadth_m_oe

What areas are covered that you feel shouldn’t be? [PRG: Textbox]

_____

[PRG: Same page]

[PRG: Ask if law_breadth is “Fewer areas than needed’]

law_breadth_f_oe

What areas are not covered that you feel should be? [PRG: Textbox]

_____

[PRG: Ask all]

law_enforcement

Would you say the digital privacy practices required by [US / EU / country’s] law are enforced …

[PRG: Insert “US” if region is “United States”, “EU” if EU is “Yes”, else: insert country from region_country or region_other]

[PRG: Randomize scale direction]

[PRG: Single choice]

- ☐ Completely
- ☐ Mostly
- ☐ Somewhat
- ☐ A little
- ☐ Not at all

state_current_law

Overall, how would you rate digital privacy laws and regulations **i**n [the US / the EU / country] today?

[PRG: Insert “the US” if region is “United States”, “the EU” if EU is “Yes”, else: insert country from region_country or region_other]
[PRG: Same randomization as law_depth]
[PRG: Single choice]

- ☐ Excellent
- ☐ Good
- ☐ Fair
- ☐ Poor

state_outlook_law
In the next few years, how optimistic or pessimistic are you that digital privacy laws and regulations in [the US / the EU / country] will move in the direction you prefer?
[PRG: Insert “the US” if region is “United States”, “ the EU” if EU is “Yes”, else: insert country from region_country or region_other]
[PRG: Randomize scale direction]
[PRG: Single choice]

- ☐ Very optimistic
- ☐ Somewhat optimistic
- ☐ Neither optimistic nor pessimistic
- ☐ Somewhat pessimistic
- ☐ Very pessimistic

[PRG: Ask if region is “United States”]
policymaking_US
Do you think that digital privacy policy in the US should be made at the …
[PRG: Randomize “Federal level” and “State level”]
[PRG: Single choice]

- ☐ Federal level
- ☐ State level
- ☐ Both [PRG: Anchor]

[PRG: Ask if EU is “Yes”]
policymaking_EU
Do you think that digital privacy policy in the EU should be made at the …
[PRG: Randomize “EU-level” and “EU member-state level”]
[PRG: Single choice]

- ☐ EU-level
- ☐ EU member-state level

☐ Both [PRG: Anchor]

[Organizational Policy]
[PRG: Ask all]
orgs_rating
[PRG: Random half list a first, other half list b first. Randomize list items within the two groups]
[PRG: Single-choice grid]
orgs_rating_pub
How would you rate the performance of these government agencies in protecting people's digital privacy?
[PRG: if region is "United States"]
[Rows]

- [org_census] US Census Bureau
- [org_irs] US Internal Revenue Service
- [org_ssa] US Social Security Administration

[PRG: if region is "Europe" or region is "Other". Do NOT display if region_country is "EU-level"]
[PRG: insert country from region_country or region_other]
[Rows]

- [org_cstatistics] [country]'s statistical agency
- [org_ctaxes] [country]'s tax authority
- [org_csocial] [country]'s social insurance authority

Orgs_rating_priv
How would you rate the performance of these firms in protecting people's digital privacy?
[Rows]

- [org_apple] Apple (including Apple Intelligence)
- [org_google] Google (including Gemini)
- [org_meta] Meta (including Facebook, Instagram, Whatsapp, Oculus, LLaMa)
- [org_twitter] X, formerly Twitter
- [org_amazon] Amazon
- [org_microsoft] Microsoft (including Copilot)
- [org_visa] Visa
- [org_mastercard] Mastercard

[Columns]
[PRG: Same randomization as law_depth]
[PRG: Single choice]

☐ Excellent
☐ Good

- ☐ Fair
- ☐ Poor
- ☐ Don't know

AI_orgs_r_priv

How would you rate the performance of these firms in protecting people's digital privacy?

[Rows]

- [org_openai] Open AI (including ChatGPT and DALL-E)
- [org_anthropic] Anthropic (including Claude)
- [org_xai] xAI (including Grok)
- [org_mistral] Mistral AI
- [org_alibaba] Alibaba (including Qwen)
- [org_tesla] Tesla
- [org_highflyer] DeepSeek

[Columns]

[PRG: Same randomization as law_depth]

[PRG: Single choice]

- ☐ Excellent
- ☐ Good
- ☐ Fair
- ☐ Poor
- ☐ Don't know

[PRG: New page]

[PRG: Ask all]

state_current_pra

Generally speaking, how would you rate organizations' digital privacy policies and practices in [the US / the EU / country] today?

[PRG: Insert "the US" if region is "United States", "the EU" if EU is "Yes", else: insert country from region_country or region_other]

[PRG: Same randomization as law_depth]

[PRG: Single choice]

- ☐ Excellent
- ☐ Good
- ☐ Fair
- ☐ Poor

state_outlook_pra

In the next few years, how optimistic or pessimistic are you that organizations' digital privacy policies and practices in [the US / the EU / country] will move in the direction you prefer?
[PRG: Insert "the US" if region is "United States", "the EU" if EU is "Yes", else: insert country from region_country or region_other]
[PRG: Same randomization as state_outlook_law]
[PRG: Single choice]

- ☐ Very optimistic
- ☐ Somewhat optimistic
- ☐ Neither optimistic nor pessimistic
- ☐ Somewhat pessimistic
- ☐ Very pessimistic

[Chatbot PII]
sensitive_1
When using AI chatbots like ChatGPT or Gemini, users may share their [Mental health information / Physical health information / Relationship/sexual information /Ideological beliefs] which could be used by the chatbots' provider to deliver targeted services (e.g., offering personalized resources, suggesting tailored educational content, adjusting chatbot tone or responses, showing location-based offers). Under what conditions do you think this would be **inappropriate**?
[PRG: Randomize fill options]
[PRG: Textbox]

_____

sensitive_2
Under what conditions do you think would it be **appropriate** for an AI chatbots' provider to share a user's [Mental health information / Physical health information / Relationship/sexual information /Ideological beliefs] with law enforcement?
[PRG: Randomize fill options; exclude fill option used in sensitive_1]
[PRG: Textbox]

_____

[Demographics]
[PRG: Ask only first time. Mandatory question]
experience
About how many years have you been working on privacy issues?
[PRG: Single choice]

- ☐ Less than 1 year
- ☐ 1 year to less than 3 years
- ☐ 3 years to less than 6 years

- ☐ 6 years to less than 10 years
- ☐ 10 years or more

[PRG: Ask only first time. Mandatory question]

sector_paid

Which of the following statements applies to you?

[PRG: Single choice]

- ☐ I perform privacy-related activities as part of my paid job
- ☐ I perform privacy-related activities as a volunteer or activist

[PRG: Ask only first time. Mandatory question]

[PRG: Ask if sector_paid is “I perform privacy-related activities as part of my paid job”]

sector

Which sector do you currently work in?

[PRG: Multiple choice]

- ☐ Academia
- ☐ Government
- ☐ Journalism
- ☐ Law
- ☐ Non-profit / NGO / Think tank
- ☐ Tech industry
- ☐ non-Tech industry
- ☐ None of the above

[Feedback]

[PRG: Ask only first time]

panel_intro Thank you for taking the time to respond to this survey. We are particularly interested in what may change over time as privacy stakeholders like you evaluate ongoing debates and events, so we would like to contact you again in four to six months to complete another short questionnaire.

[PRG: same page]

panel

Would you be willing to participate in future rounds of the TAPP Panel?

[PRG: Single choice]

- ☐ Yes
- ☐ No

[Email & Name]

[PRG: Ask if not invited via email and panel is “Yes”. Ask only first time]

email

Thank you for your response! We would like to invite you to future rounds of this survey via email. Please enter your email address here: [PRG: Validation: email format]

_____

[PRG: Ask if email is empty and panel = “Yes”]

If you don't share your email, we will not be able to include you in the panel.

[PRG: Ask if recruited through pilot or RDS and panel is “Yes” and email_entry is not empty. Ask only first time. Mandatory question]

name

We would like to address you by name when inviting you to future rounds of this survey. Your name will not be associated with your answers. Please enter your name here: [PRG: Textbox]

_____

[End]

[PRG: Display for all completes]

Thank you! Your responses have been submitted.

If you know other privacy thought leaders who would contribute meaningful insights on the questions posed in this survey, please contact us or encourage them to reach out at info@privacyperceptions.org.

For more information about TAPP, please visit www.privacyperceptions.org.

For regular survey updates and analysis of the results, check out our LinkedIn page.

If you have any questions, you can contact us at info@privacyperceptions.org.

You can now close this window.

[PRG: Display if screened out]

Thank you for your interest in TAPP! We have no more questions for you at this time.

If you know other privacy thought leaders who would contribute meaningful insights on the questions posed in this survey, please contact us or encourage them to reach out at info@privacyperceptions.org.

For more information about TAPP, please visit www.privacyperceptions.org.

For regular survey updates and analysis of the results, check out our LinkedIn page.

If you have any questions, you can contact us at info@privacyperceptions.org.

You can now close this window.