



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

Results from the Fourth Wave of the TAPP Panel Survey

(May 2024)

Isabela Bertolini Coelho, Olga Kononykhina, Sonja Kellner, Mariel McKone Leonard, and the TAPP
Team

Citation:

Coelho, I. B., Kononykhina, O., Kellner, S., Leonard, M.M., & TAPP Team. (2024). Policies, practices, and priorities: Transatlantic experts' perceptions on privacy: Results from the Fourth Wave of the TAPP panel survey. [September 2024].

Executive Summary

This report presents the findings from the fourth wave of the Transatlantic Privacy Perception (TAPP) panel survey, conducted in May 2024. The survey focused on privacy experts' views on the use of Artificial Intelligence (AI) tools, the presence of governance frameworks, and the impact of privacy concerns on AI adoption across the United States and Europe. A total of 82 participants from academia, the tech industry, and other sectors answered the survey, providing valuable perspectives on the state of AI governance and privacy in their organizations.

AI Usage and Governance: The results show that 71% of respondents use AI tools in their work, yet only 41% of their organizations have governance frameworks for AI. Among those with frameworks, 91% were developed internally. This indicates that while AI usage is widespread, formal governance remains limited, with a significant portion of organizations still lacking the necessary structures to ensure responsible AI usage. Notably, 44% of organizations without frameworks plan to adopt them in the near future.

Compliance and AI-Specific Roles: 41,5% of organizations are uncertain about their organization's approach to AI compliance. Additionally, 17,5% see external consultants as a solution and 12,5% anticipate the creation of new roles or teams focused on AI governance. This reflects a growing need for raising awareness of implemented AI governance into business processes and sharing best practices.

Privacy Concerns and Responsible AI: Privacy concerns are a major influence on AI adoption, with 52% of respondents exercising caution due to these concerns, and 33% reporting moderate concern. While 87% of respondents are familiar with Responsible AI principles, only 41% feel confident in their organization's ability to address AI-related privacy challenges. This highlights a gap between awareness of Responsible AI and actual preparedness, suggesting a need for more comprehensive frameworks and training.

Regional Differences: There is a noticeable difference between Europe and the US in AI adoption. In Europe, 79% of privacy experts report using AI, compared to 59% in the US. However, fewer organizations in both regions have established AI frameworks, with only 46% in Europe and 38% in the US having such structures in place. Future planning for AI frameworks is evident, as 44% of organizations in both regions without current guidelines are working towards implementing them.

Conclusion: The findings underscore the critical need for organizations to establish robust AI governance frameworks to address privacy concerns and ensure responsible AI use. Organizations must focus on enhancing governance structures, expanding the involvement of privacy experts in the development of AI guidelines, and increasing education on Responsible AI to bridge the gap between awareness and effective governance.

Table of Contents

1 Introduction.....	4
2 Data collection.....	5
3 Findings.....	6
3.1 Respondents profile.....	6
3.2 Organizational adoption and integration of AI systems.....	7
3.3 Future plans for organizational adoption of AI frameworks and guidelines.....	9
3.4 Privacy concerns in the implementation of AI systems.....	11
3.5 Organizational team structure for AI compliance.....	12
3.6 Awareness of Responsible AI principles.....	13
4 Conclusions and recommendations.....	14
5 Appendix.....	16
5.1 Questionnaire.....	16
5.2 Sampling design.....	23

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 AI on privacy policies. During the fourth wave conducted in May 2024, 82 participants responded to questions about the adoption and integration of frameworks and guidelines of AI systems in their work.

The latest findings from the Transatlantic Privacy Perception panel highlight that while AI is widely used in professional settings, many organizations still lack formal frameworks to govern its use. Most AI governance frameworks that do exist are developed internally. Although there is a growing familiarity with responsible AI principles, there remains a noticeable divide in confidence regarding organizations' ability to address AI-related privacy challenges, emphasizing the need for stronger governance and privacy protections.

2 Data collection

The Wave 4 questionnaire focused on organizational adoption and integration of AI systems (see Appendix for complete questionnaire). Following approval by the University of Maryland Institutional Review Board, fielding began 17 April 2024 and continued until 15 May 2024.

Programming and survey distribution were conducted through Qualtrics, with personalized emails used to invite 895 individuals. In addition, survey links were shared via TAPP project LinkedIn posts. Invited individuals who had not yet participated in Wave 4 received a first reminder on 1 May 2024 and a final reminder on 13 May 2024.

A total of 895 individuals received email invitations. Of these, 39 returning respondents (who responded to at least one of the previous TAPP waves) provided complete (AAPOR 1.1) responses¹. In addition, 38 new individuals participated, for a total of 77 participants. No individuals provided partially complete (AAPOR 1.2) responses. Table 1 shows the breakdown of respondents.

Table 1. Completed surveys by respondent type

	Completed surveys (AAPOR 1.1)	Partial completes (AAPOR 1.2)
Returning respondents	39 (50.7%)	0
New respondents	38 (49.3%)	0
Total	77 (100%)	0

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) defined as 50-80% of all applicable questions answered and/or 50-99% of all crucial questions answered. Incomplete or break-off interviews are those which do not meet the definition of either partial or complete interviews. For the Wave 4, we classified complete interviews as those with fewer than six missing variables, and partials as fewer than 16 missing variables, out of a total of 32.

3 Findings

3.1 Respondents profile

Wave 4 of the TAPP survey received responses from 77 participants. In terms of professional background, 43% are from academia, and 17% are from the tech industry while 12% are from the private sector, but from non-tech industry (Figure 1).

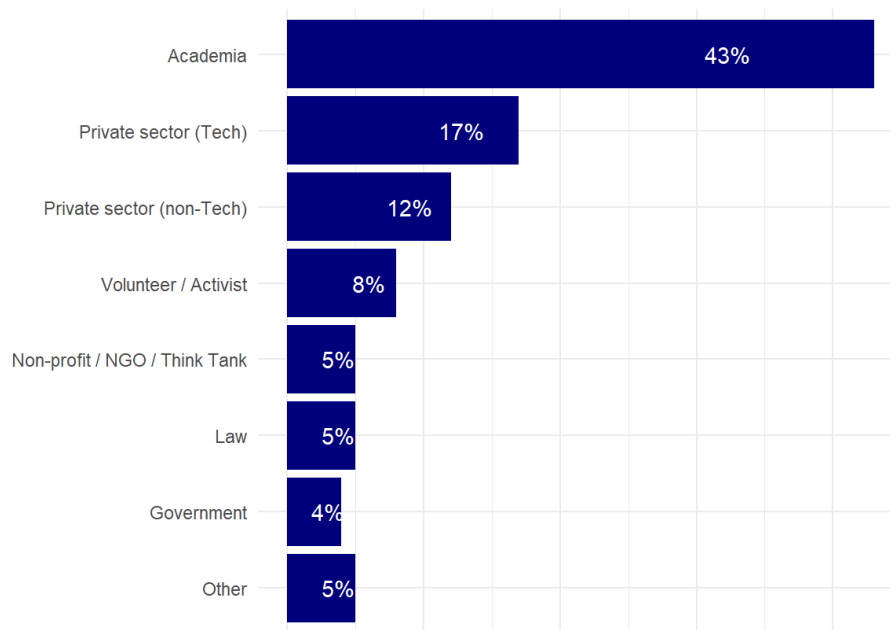


Figure 1. Respondents composition by sector

Notably, 45% of respondents have worked in the privacy field for more than 10 years (Figure 2), and only 5% less than a year. The sample includes 48 participants with more knowledge about the European privacy context and 28 of the American context.

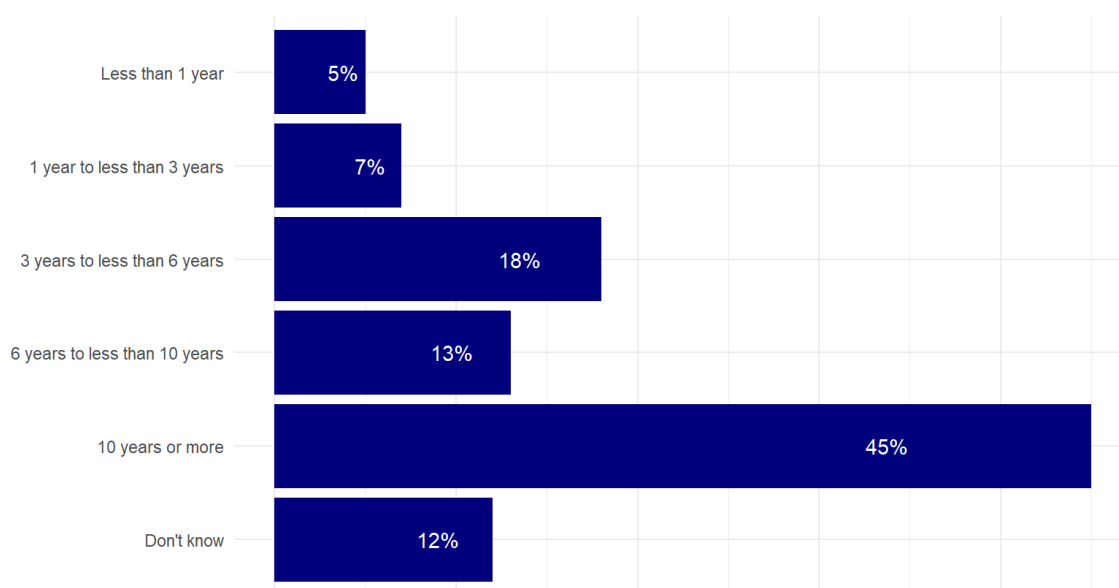


Figure 2. Respondents composition by years of experience with privacy

3.2 Organizational adoption and integration of AI systems

Significant majority of respondents are integrating AI tools or systems into their work. However, this trend is not consistent across all regions. There is also a critical gap in governance, with less than half of European and US organizations having established frameworks to guide responsible AI implementation.

The fourth wave of the TAPP survey revealed that a large majority (72%) of respondents reported using AI tools or systems in their work. However, this adoption is not uniform across all regions. 79% of experts about privacy in Europe use AI tools or systems in their work and 19% of them do not, whereas 2% do not know how to answer this question (Figure 3). Following a similar trend but lagging behind, 61% of the experts about privacy in the United States use AI tools or systems in their work while 39% do not, reflecting the importance of AI in modern business operations.

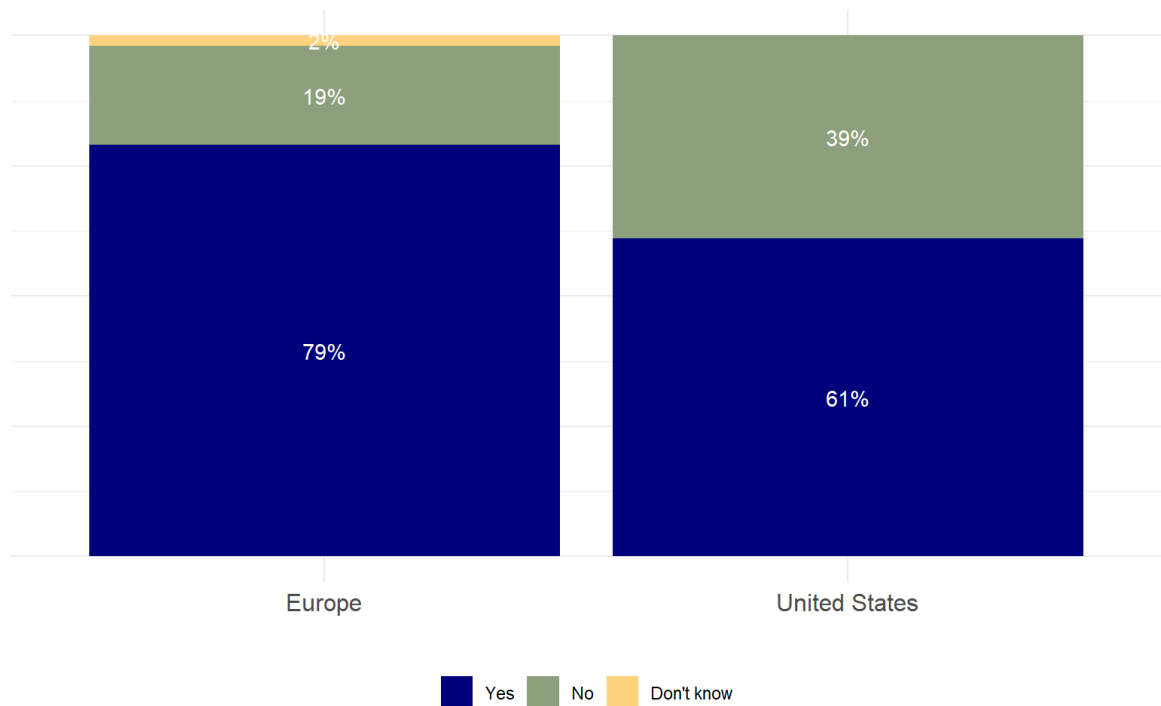


Figure 3. Use of AI tools and systems for work

However, only 46% in Europe and 39% in US work for organizations that have established specific frameworks or guidelines to govern how AI is implemented and used in the workplace (Figure 4). These frameworks are crucial for ensuring that AI is employed responsibly, ethically, and effectively, addressing issues such as data privacy, fairness, and the impact on employees (Haipeter et al., 2024). Unfortunately, a large portion of experts —17% in Europe and 7% in the US— do not know whether such frameworks or guidelines exist within their organizations.

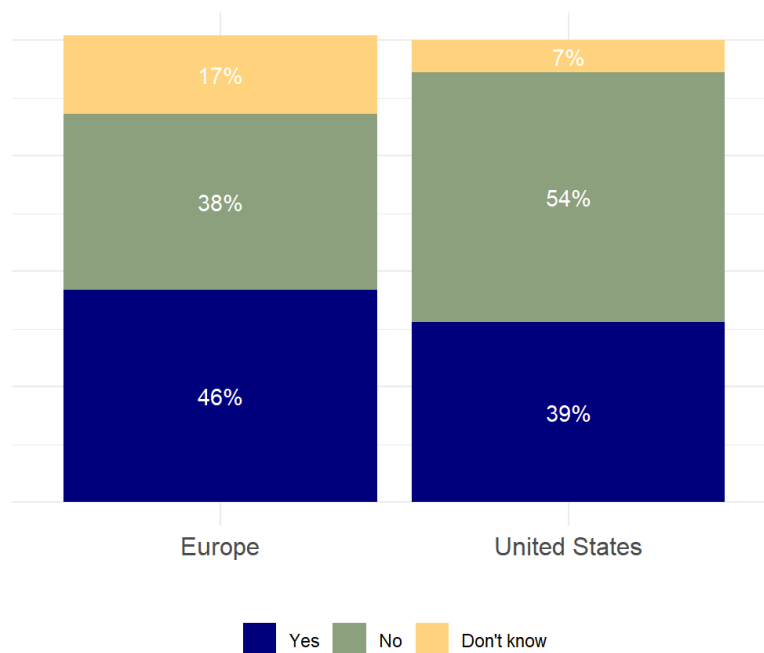


Figure 4. Organizational adoption of AI frameworks and guidelines

Among those with guidelines, 91% were developed internally in both regions. The choice between internal and external AI frameworks presents distinct advantages and challenges. Internal frameworks offer customization and collaboration benefits, as they are tailored to the organization's specific needs and context. However, they may suffer from limited expertise, resource constraints, and scalability issues.

In contrast, external frameworks promote standardization and provide updated guidelines with expert insights, though they may not perfectly align with an organization's specific needs and may create dependencies on external updates. Recognized external AI frameworks include those from OECD.AI, NIST, ISO, and major companies like Google and Microsoft (Burle and Cortiz, 2020).

A hybrid approach that combines internal and external guidelines may offer the best of both worlds, helping organizations strategically navigate the evolving AI landscape to maximize the technology's potential. Therefore, the decision to adopt internal, external or hybrid AI frameworks is a strategic one, influenced by an organization's unique context and goals.

3.3 Future plans for organizational adoption of Responsible AI frameworks and guidelines

The majority of organizations in Europe and the US without current guidelines intend to implement a framework or guidelines for future Responsible AI use in their work.

Among those without guidelines, future planning for Responsible AI frameworks is evident, as 45% of experts in Europe and US indicated their organizations plan to implement those frameworks in the future. On average, 30% are still undecided (28% in Europe and 33% in US), and 24% will not implement guidelines (28% in Europe and 20% in US).

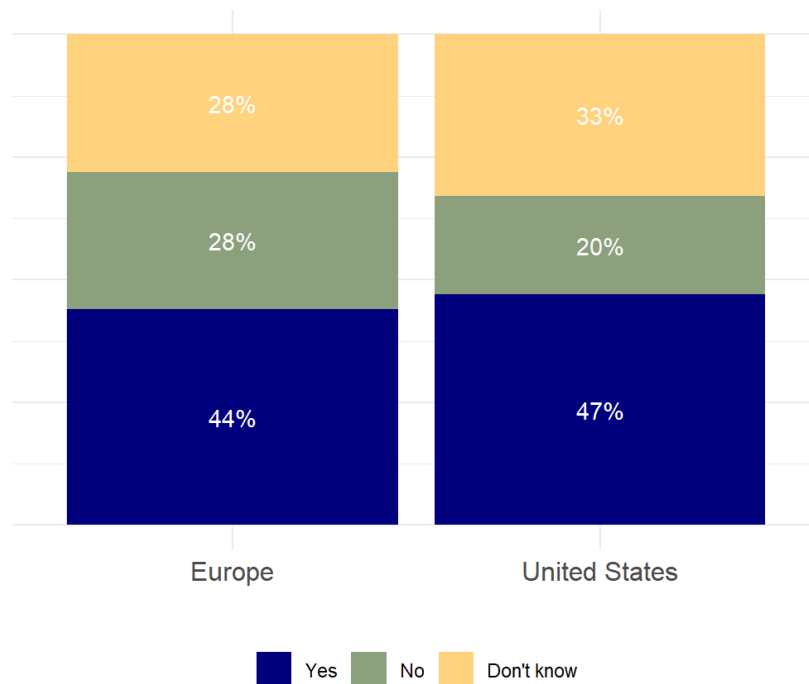


Figure 5. Intentions for organizational adoption of Responsible AI frameworks and guidelines

Creating effective Responsible AI frameworks requires the input of those who will use and enforce them. Employee participation in creating those frameworks ensures that diverse perspectives are considered, leading to more comprehensive and effective guidelines. Encouraging broader involvement in the drafting process can also foster a culture of ethical AI use and accountability within organizations (Haipeter et al, 2024). TAPP provides insights into the involvement of privacy experts in drafting Responsible AI frameworks. Specifically, 50% of respondents are or will be involved in drafting their organization's Responsible AI guidelines, while 7% will not be involved, and 43% are unsure about their involvement.

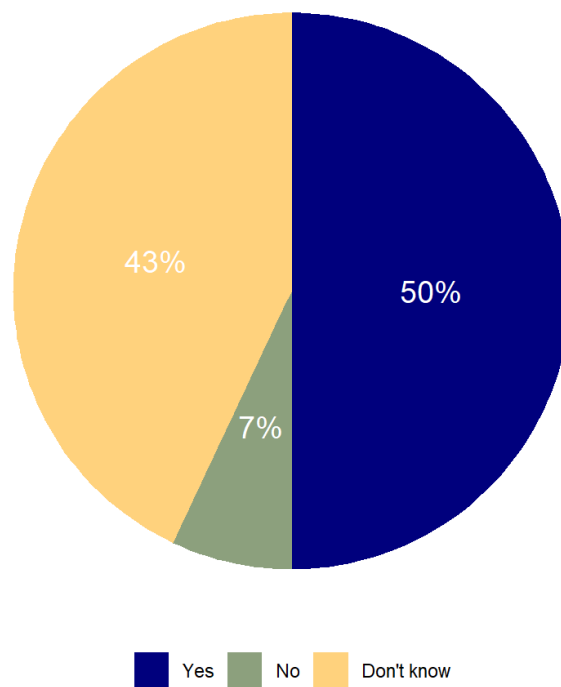


Figure 6. Stakeholder involvement in organizational AI framework and guidelines development

3.4 Privacy concerns in the implementation of AI systems

Privacy concerns strongly influence AI adoption, with over half of respondents in Europe and the US reporting that these concerns greatly affect their use of AI tools, highlighting the urgent need for robust regulations, transparency, and human oversight to ensure safe and trusted AI use.

According to the survey (Figure 7), privacy concerns affect the use of AI tools or systems, with 52% of respondents in Europe and 57% in the USA reporting that these concerns greatly influence their use. Additionally, 33% and 29% of respondents indicated that privacy concerns somewhat influence their use of AI, suggesting that while they may use AI tools, they do so with certain reservations and safeguards in place. This underscores the urgent need for robust regulation, guidelines, frameworks, and best practices to ensure the safe development, adoption, procurement, and sale of AI technologies. Public and private organizations must be equipped with clear standards to navigate the complex landscape of AI deployment while safeguarding privacy. Moreover, providers of AI technologies should prioritize transparency about the privacy of the data collected through AI tools. Transparent data practices will build trust and allow users to understand how their data is being used and protected (Morey et al., 2015). Conversely, 12% of respondents in Europe and 14% in the US reported that privacy concerns do not affect their use of AI tools at all, indicating that a smaller segment of users either have robust privacy measures already in place or do not view privacy issues as a significant barrier to AI adoption.

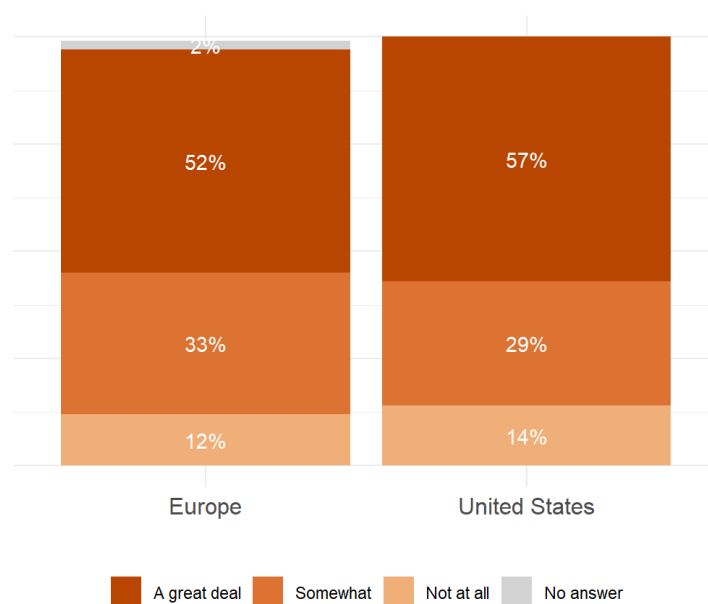


Figure 7. Privacy concerns for the use of AI tools or systems in their work

In 2024, the survey also explored which practices centered around AI privacy are considered most important. The ability to control one’s own data, including accessing, correcting, and deleting personal data, was the top priority, chosen by 37 respondents. Privacy by design, involving default privacy settings, followed closely with 36 selections. Human involvement and oversight of AI decision-making were emphasized by 32 respondents, highlighting the need for human judgment in AI processes. Documentation and traceability of data sources were deemed crucial by 31 participants, while data minimization and technical privacy safeguards were each chosen by 21 and 19 respondents respectively. Human-centered design, focusing on usability and explainability, was selected by 16 respondents. Copyright protections were important to 11 participants. These insights highlight the critical elements that experts believe should be prioritized to ensure rigorous AI privacy protections. Emphasizing control over own data, privacy by design, and human oversight can significantly enhance AI adoption.

3.5 Organizational team structure for AI compliance

American privacy experts are more likely to be responsible to address AI guidelines, while European experts foresee that privacy work has to expand to include AI.

Regarding how organizations ensure compliance with AI frameworks and guidelines, wave 4 results show that a notable percentage of privacy experts in both regions (40% in Europe and 67% in the US) believe that individuals or teams will be responsible for ensuring compliance within the organization. Interestingly, 22% of US experts think their existing privacy work will expand to include AI, a perspective shared by 27% of their European counterparts. Additionally, 20% of

European experts anticipate the creation of new roles or teams focused on AI, compared to only 11% of US experts. In the US, 11% of experts see external consultants as a solution, whereas none of the European experts share this view. Finally, wave 4 results show that a larger proportion of US privacy experts (39%) are uncertain about their organization's approach to AI compliance, compared to 27% in Europe.

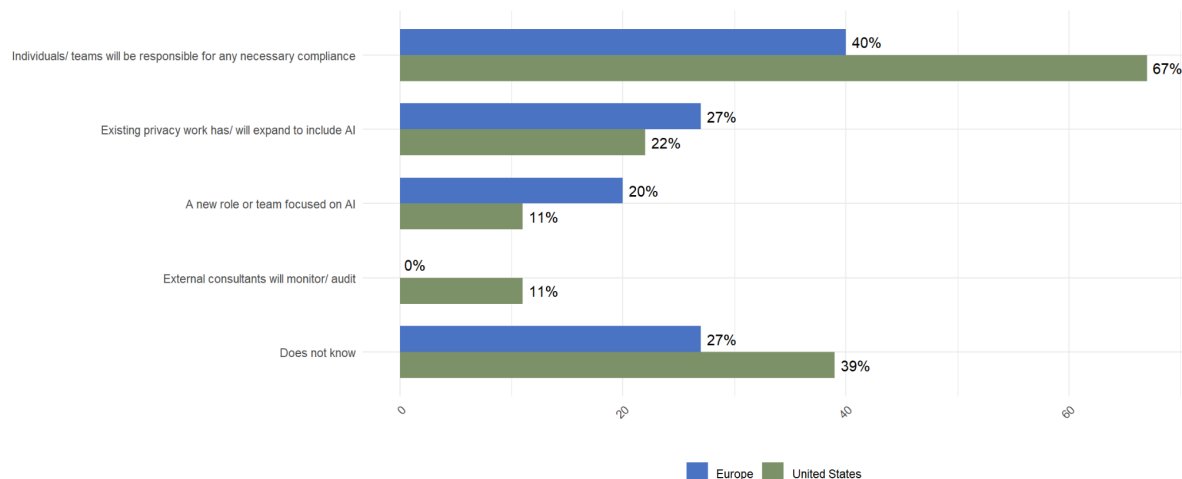


Figure 8. Organizational compliance with AI framework and guidelines

3.6 Awareness of Responsible AI principles

Only 37% of privacy experts are highly familiar with Responsible AI principles, indicating a need for greater education in the field.

The TAPP survey reveals varying levels of familiarity with Responsible AI principles among privacy experts. Specifically, 37% of respondents (33% in Europe and 43% in the US) are highly familiar with these principles, 53% (54% in Europe and 50% in the US) are somewhat familiar, and 9% (10% in Europe and 7% in the US) are not familiar at all. These results highlight an area for growth and education within the field, emphasizing the need for privacy experts to have a common foundational framework. Responsible AI principles, which stress fairness, transparency, accountability, and ethical considerations in AI development, are crucial for ensuring that these technologies benefit society while minimizing potential harms. As AI continues to advance, aligning privacy expertise with these principles is essential for developing ethical and effective AI systems (Stryker, 2024).

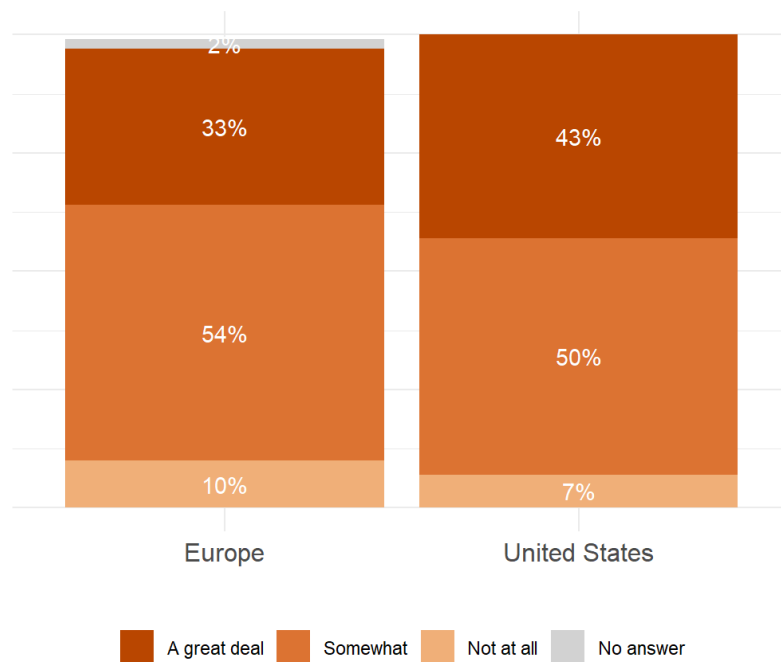


Figure 9. Awareness of Responsible AI principles

4 Conclusions and recommendations

The fourth wave of the Transatlantic Privacy Perception (TAPP) panel survey highlights significant insights into the current state of AI usage and governance among privacy experts in the United States and Europe. The survey reveals that while AI tools are widely adopted, the presence of specific frameworks to govern AI use remains limited. Creating effective Responsible AI frameworks requires the input of those who will use and enforce them. Employee participation in creating those frameworks ensures that diverse perspectives are considered, leading to more comprehensive and effective guidelines. Encouraging broader involvement in the drafting process can also foster a culture of ethical AI use and accountability within organizations (Haipeter et al, 2024). It is promising to see that many experts without current guidelines plan to establish them for future Responsible AI practices. As seen in the results, privacy concerns significantly impact AI adoption. The recommendations from the panelists to tackle those concerns include the importance of controlling one's own data, implementing Privacy by Design, and ensuring human involvement and oversight in AI decision-making. Despite the growing importance of AI, relatively few privacy experts are aware of general Responsible AI principles. There is also a considerable amount of varying opinions and uncertainties on how organizations should structure their teams to ensure AI compliance according to our results. In future TAPP surveys, we aim to identify best practices of different Responsible AI approaches by examining which strategies for increasing education on Responsible AI to bridge the gap between awareness and effective governance are most widely regarded as effective.

References

Burle, Caroline, and Diogo Cortiz. "Mapping Principles of Artificial Intelligence." São Paulo: Núcleo de Informação e Coordenação do Ponto BR (2020).

Haipeter, Thomas, Manfred Wannöffle, Jan-Torge Daus, and Sandra Schaffarczyk. "Human-Centered AI through Employee Participation." *Frontiers in Artificial Intelligence* 7 (2024).

<https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1272102>.

Morey, Tim, Theodore Forbath, and Allison Schoop. "Customer Data: Designing for Transparency and Trust." *Harvard Business Review* 93, no. 5 (2015): 96-105.

Stryker, Cole. "What is responsible AI?". IBM. Last modified February 6, 2024.

<https://www.ibm.com/topics/responsible-ai> Accessed August 10, 2024.

The American Association for Public Opinion Research. 2023 Standard Definitions: Final Dispositions of Case Codes and Outcome Rates for Surveys. 10th edition. AAPOR

5 Appendix

5.1 Questionnaire

[\[Introduction\]](#)



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 **2-5 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.

[\[PRG: "Start Survey" button\]](#)



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>

[Screener]

[PRG: Ask first time only. 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

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

screen_privacy

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]

[Main Questionnaire]

ai_work

Do you use AI tools or systems in your work?

[PRG: Single choice]

- ☐ Yes
- ☐ No
- ☐ Don't know

ai_concern

How much do privacy concerns affect your use of AI tools or systems in your work?

[PRG: Randomize scale direction]

- ☐ Not at all

- ☐ Somewhat
- ☐ A great deal

ai_org_framework

Does your organization have a framework or guidelines in place for using AI in the workplace?

[PRG: Single choice]

- ☐ Yes
- ☐ No
- ☐ Don't know

[PRG: Ask if ai_org_framework is "Yes"]

ai_org_develop

Was the framework or guidelines developed by your organization or by another organization?

[PRG: Single choice]

- ☐ My organization
- ☐ Another organization
- ☐ Don't know

[PRG: Ask if ai_org_develop is "My organization" OR "Another organization"]

ai_framework_use

Which frameworks and guidelines does your organization have for AI use? (e.g., OECD, IEEE, internal) _____

[PRG: Ask if ai_org_develop is "My organization" OR "Another organization"]

ai_framework_link

We'd like to report on the characteristics of the frameworks or guidelines organizations are using within the privacy community for AI use. If possible, please share a link to the framework or guidelines your organization uses. _____

[PRG: Ask if ai_org_framework is "No"]

ai_framework_future

Does your organization plan to implement a framework or guidelines for future AI use?

[PRG: Single choice]

- ☐ Yes
- ☐ No
- ☐ Don't know

[PRG: Ask if ai_framework_future is "Yes"]

ai_framework_draft

Are you/ will you be involved in drafting the framework or guidelines?

[PRG: Single choice]

- ☐ Yes
- ☐ No
- ☐ Don't know

[PRG: Ask if ai_framework_draft is "Yes"]

ai_interview

Would you be willing to participate in an interview with TAPP researchers about your experience drafting the framework or guidelines?

[PRG: Single choice]

- ☐ Yes
- ☐ No

[PRG: Ask if ai_org_framework is "Yes" OR ai_framework_future is "Yes"]

ai_compliance_frame/future

How does/ will your organization ensure that everyone complies with the framework or guidelines?

[PRG: Randomize]

[PRG: Multiple choice]

- ☐ Individuals/ teams will be responsible for any necessary compliance
- ☐ Existing privacy work has/ will expand to include AI
- ☐ A new role or team focused on AI
- ☐ External consultants will monitor/ audit
- ☐ Don't know

ai_challenge

Do you feel confident that you/ your organization will be able to address privacy challenges that may arise when using AI tools or systems in your work?

[PRG: Single choice]

- ☐ Yes
- ☐ No
- ☐ Don't know

[PRG: Ask if ai_challenges is "Yes"]

ai_challenge_plan

How do you/ does your organization plan to address such challenges? _____

ai_privacy

Below, we have listed key aspects of practices centered around AI privacy often included in AI frameworks and guidance. Which of these do you think are the most important aspects to include for privacy purposes? *Choose up to three.*

[PRG: Randomize]

[PRG: Multiple choice]

- ☐ [ai_privacy_document] Documentation and traceability of data sources
- ☐ [ai_privacy_oversight] Human involvement and/or oversight of AI decision-making
- ☐ [ai_privacy_hcd] Human-centered design (e.g., usability, explainability)
- ☐ [ai_privacy_safeguards] Technical privacy safeguards (e.g., encryption)
- ☐ [ai_privacy_pbd] Privacy by design (e.g., default settings)
- ☐ [ai_privacy_dm] Data minimization
- ☐ [ai_privacy_userrights] Control over own data (e.g., access, correct, delete data)
- ☐ [ai_principle_copyright] Copyright protections
- ☐ [ai_privacy_other] Other: _____
- ☐ [ai_privacy_none] Prefer not to answer

ai_responsible

How familiar are you with "Responsible AI" principles?

[PRG: Single choice]

- ☐ Not at all
- ☐ Somewhat
- ☐ A great deal

[Demographics: Regional Expertise]

[PRG: Ask first time only. Mandatory questions]

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 United States
- ☐ [region_other] Another country or region: _____

[PRG: Ask if region is "Both"]

region_both

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

[PRG: Single choice]

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

[PRG: Ask if region is "Europe" or region_both is "Europe"]

region_country

And which European country in particular?

[Demographics]

[PRG: Ask first time only. Mandatory questions]

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

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 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 first time only]

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.

panel

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

[PRG: Single choice]

- ☐ Yes
- ☐ No

language_en

Were you comfortable completing this survey in English?

[PRG: Single choice]

- ☐ Yes
- ☐ No

[PRG: Ask if language_en is “No”]

language_other

What language would you have preferred?

[PRG: Single choice]

- ☐ French
- ☐ German
- ☐ Italian
- ☐ Spanish
- ☐ Other: _____

aspects_future_oe

What aspects of digital privacy would you like to see asked about in future surveys?

[Email & Name]

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

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: 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 email is not empty.]

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: _____

[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.

5.2 Sampling design

The target population for the TAPP Panel is privacy policy experts. Members of the research team initially identified several groups of key stakeholders:

- **Tier 1:** Key privacy actors and experts identified by the research team via publicly available records. The research team screened conference announcements, schedules, programs, and proceedings for experts in privacy.
- **Tier 2:** People associated with Tier 1 through offline referrals via qualitative interviews and the quantitative survey.
- **Tier 3:** "Conversants" in privacy who contribute to the spread of Tier 1-2 influence or influence privacy at a local or community level.

Each tier contains stakeholders of different sectors, and each sector contains stakeholders of different tiers. Electronic invitations to participate were sent to privacy experts and influential voices identified by the researchers through systematic screening of academic journals, conference programs, government documents, NGO whitepapers, policy briefs, media articles, and press releases. The non-random sample were selected based on their visibility, recognizability, and influence in the field. Contact details were researched manually.

Additionally, individuals are able to request to join the Panel through the TAPP website, LinkedIn posts, and TAPP events; these individuals are screened for expertise before inclusion. Once invited to the Panel, respondents receive the questions regardless of tier membership.