TAPP Transatlantic Privacy Perceptions

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

Results from the Fifth Wave of the TAPP Panel Survey

(September 2024)

Isabela Bertolini Coelho, Anna Fuchs, Sonja Kellner and the TAPP Team

Executive Summary

This report presents findings from the fifth wave of the Transatlantic Privacy Perceptions (TAPP) panel survey, conducted from August 14 to September 11, 2024. The TAPP project, led by the University of Maryland and Ludwig-Maximilians-Universität München, tracks privacy experts' evolving perceptions on digital privacy laws, practices, and the impact of emerging technologies like artificial intelligence (AI). Wave 5 involved 66 respondents, predominantly from academia and industry, offering valuable insights into the state of digital privacy across the USA and Europe. The wave 5 questionnaire focused on the current state and effects of privacy laws, regulations, and practices.

Regional Variations in Privacy Laws: European laws are increasingly seen as favoring individual users, with 75% of respondents in 2024 highlighting this shift, compared to 43% in 2023. Conversely, in the USA, privacy laws are largely perceived as favoring businesses, with 86% of respondents maintaining this view in 2024. Additionally, concerns about the comprehensiveness of privacy laws remain prevalent. In the USA, 95% of respondents feel these laws address fewer areas than necessary, whereas this concern is shared by 43% of respondents in Europe.

Innovation and Enforcement: The perception that privacy laws encourage innovation has grown significantly in the USA, with 50% of respondents acknowledging this in 2024, up from 27% in 2023. Meanwhile, in Europe, this perception has slightly declined. Regarding enforcement, European respondents report improvements, with 27% stating that privacy practices are "mostly enforced," compared to just 9% in 2022. Meanwhile, in the USA, perceptions remain more stable with a slight increase in minimal enforcement, suggesting that privacy practices are "A little" enforced.

Future Outlook: European privacy laws continue to receive more favorable perceptions, with 59% of respondents rating them as "good" or "excellent." However, optimism about future advancements in privacy laws has declined in Europe, dropping from 48% in 2023 to 36% in 2024. In the USA, negative views on current privacy laws persist, but there is a slight increase in optimism about future improvements.

Organizational Performance: Both regions express significant dissatisfaction with organizations' privacy practices. In the USA, 95% of respondents rate organizational privacy efforts as "poor" or "fair," while 75% of European respondents share this view.

AI Regulation and Innovation: Opinions on the EU AI Act's impact on innovation vary notably by region. In Europe, 36% of respondents believe the Act will neither enable nor hinder

innovation, while 30% view it as a potential hindrance. In the USA, skepticism is more pronounced, with 41% perceiving the Act as likely to hinder innovation.

Policy Priorities: "Enforcing rules on data processing, storage, and sharing" remains the most valued approach for protecting digital privacy. However, regional differences persist. In the USA, experts prioritize giving individuals control over their data, while European respondents favor technology-based solutions.

Conclusion: Policymakers in the USA should consider adopting more comprehensive and consistent federal-level privacy regulations to address gaps and improve public confidence. In Europe, regulators should focus on balancing individual protection with fostering innovation to sustain progress. Additionally, organizations in both regions must enhance transparency and compliance with privacy laws to mitigate stakeholder dissatisfaction and strengthen trust.

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 5 of the Transatlantic Privacy Perceptions (TAPP) Panel, conducted between 14 August 2024 and 11 September 2024, 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 5 repeats 15 questions from Wave 2, conducted in 2023.

This longitudinal approach allows TAPP to track shifts in opinions and observe how the regulatory landscape and attitudes toward digital privacy may have evolved over time. Additionally, with the rapid developments in artificial intelligence, we include additional questions about the EU AI Act to gauge how stakeholders are responding to this emerging regulatory framework. As AI continues to advance, understanding reactions to the EU AI Act is critical in assessing its perceived impact on innovation and privacy protection.

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 Data collection

The target population for the TAPP Panel is privacy policy experts located on both sides of the Atlantic Ocean. The sample design includes three tiers of privacy actors: Tier 1 consists of prominent experts identified through public records such as conference programs and proceedings; Tier 2 includes individuals connected to Tier 1 experts through referrals from qualitative interviews and the survey; and Tier 3 involves contributors to privacy discussions at local or community levels. Additionally, individuals can request to join the Panel through the TAPP website or social media platforms, where they are screened for expertise before inclusion. The longitudinal nature of the Panel allows the research team to track trends over time by categorizing respondents into three groups: returning participants, previous non-respondents, and new respondents. The sample represents a convenience sample, and inferences to the entire population should not be drawn.

The Wave 5 questionnaire focused on the current state and effects of privacy laws, regulations, and practices. As part of the Panel's longitudinal design, Wave 5 repeats 15 questions from Wave 2, conducted in 2023 (see Appendix for complete questionnaire). Following approval by the University of Maryland Institutional Review Board, fielding began 4 August 2024 and continued until 11 September 2024.

Programming and survey distribution were conducted through Qualtrics, with personalized emails used to invite 799 individuals. In addition, survey links were shared via TAPP project LinkedIn posts. Invited individuals who had not yet participated in Wave 5 received a first reminder on 28 August 2024 and a final reminder on 9 September 2024. In addition to the 57 invited individuals who participated in Wave 5, 22 individuals saw and clicked on the Wave 5 survey link posted on social media (Table 1). Of these 79 individuals who started the survey, 66 (83.5%), completed the survey (AAPOR 1.1) while 13 (16.5 %) broke off, i.e., they completed less than 50% of the survey[1].

---

[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 5, we classified complete interviews as those with fewer than seven missing variables, and partials as fewer than 18 missing variables, out of a total of 35.
The American Association for Public Opinion Research (AAPOR). (2023). *Standard definitions. Final dispositions of case codes and outcome rates for surveys*.
https://aapor.org/wp-content/uploads/2024/03/Standards-Definitions-10th-edition.pdf

Table 1. Completed surveys by respondent type

	Completed surveys	Partial completes	Incompletes
Returning respondents	35 (56.5%)	3 (66.7%)	3 (23.2%)
Previous non-respondents	10 (16.1%)	1 (33.3%)	5 (38.4%)
New respondents	17 (27.4%)	0 (0%)	5 (38.4%)
Total	62 (100%)	4 (100%)	13 (100%)

3 Findings

3.1 Respondents profile

Wave 5 of the TAPP survey received responses from 66 participants. In terms of professional background, 35% are from academia, and 14 % are from the tech industry while 14 % are from the private sector, but from non-tech industry (Figure 1).
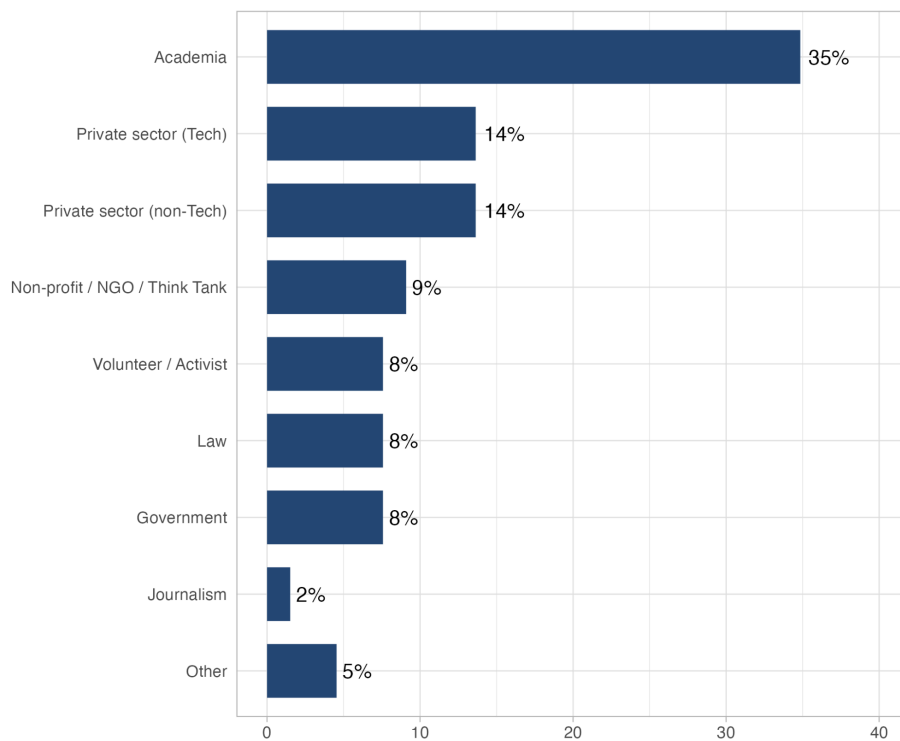

Figure 1. Respondents composition by sector

Notably, 52% of respondents have worked in the privacy field for more than 10 years (Figure 2), and only 3% less than a year. The sample includes 44 participants with more knowledge about the European privacy context and 22 of the American context.
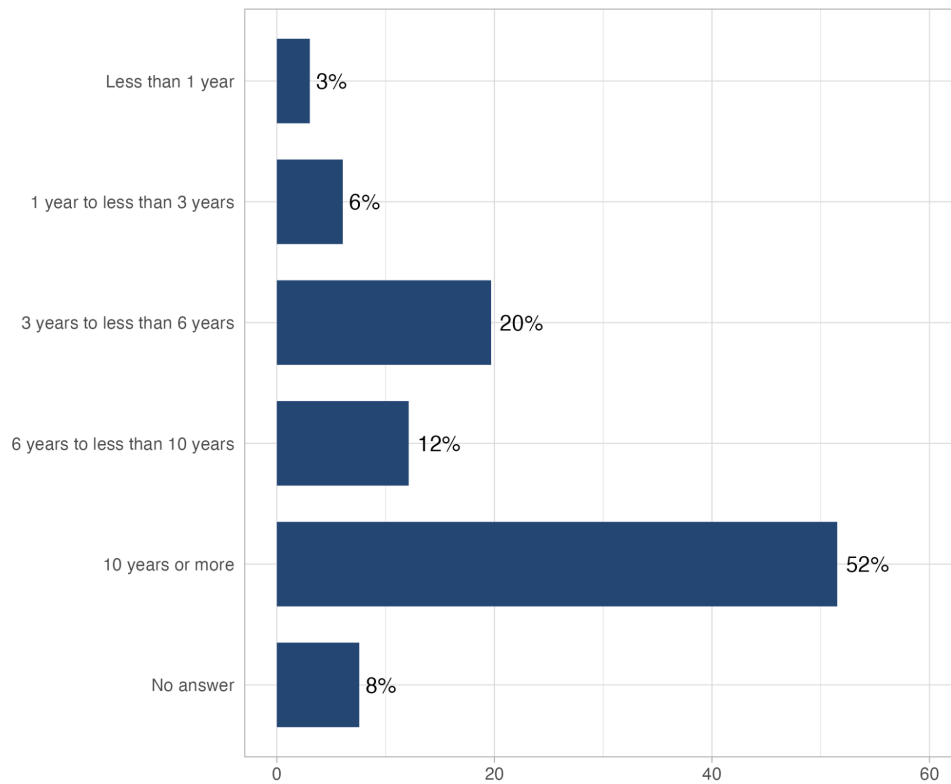
Figure 2. Respondents composition by years of experience with privacy

3.2 Balance of interest in digital privacy laws

The comparison of interest in digital privacy laws reveals relevant regional differences. In Europe, there's a notable shift towards favoring individual users over businesses. From 2023 to 2024, the percentage of respondents believing laws favor individual users rose from 44% to 75%. Conversely, in the United States (USA), the perception that laws favor businesses remains overwhelmingly high, with 92% in 2023 and 86% in 2024. This underscores the divergent approach to privacy laws on either side of the Atlantic, with Europe moving towards greater protection for individuals while the USA maintains a business-friendly stance (Figure 3).
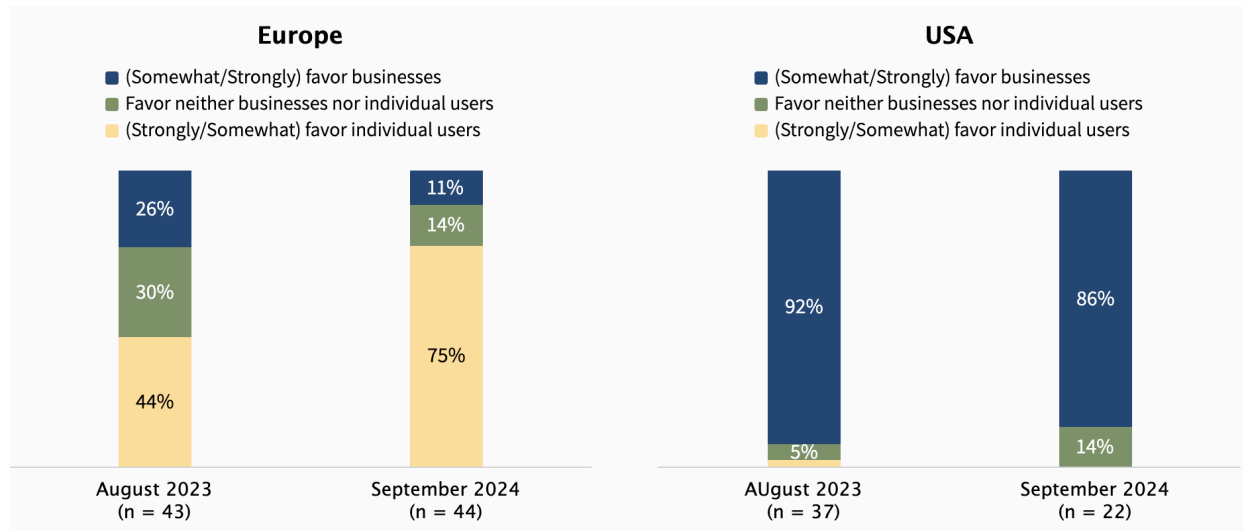
Figure 3. Balance of interest in digital privacy laws

3.3 Influence of laws on development of privacy-preserving practices and technologies

This analysis highlights a growing perception in the USA that privacy laws are encouraging innovation in privacy-preserving technologies (Figure 4). The percentage of respondents in the USA who believe laws encourage innovation almost doubled, from 27% in 2023 to 50% in 2024. On the other hand, Europe shows a slight decline in this belief, dropping from 49% in 2023 to 41% in 2024. However, this difference primarily leaned towards neutrality, increasing from 23% to 36%, rather than discouragement, which decreased from 28% to 23%. This trend indicates a positive shift in the USA towards recognizing the benefits of privacy laws in fostering technological innovation, while Europe maintains a more balanced view.
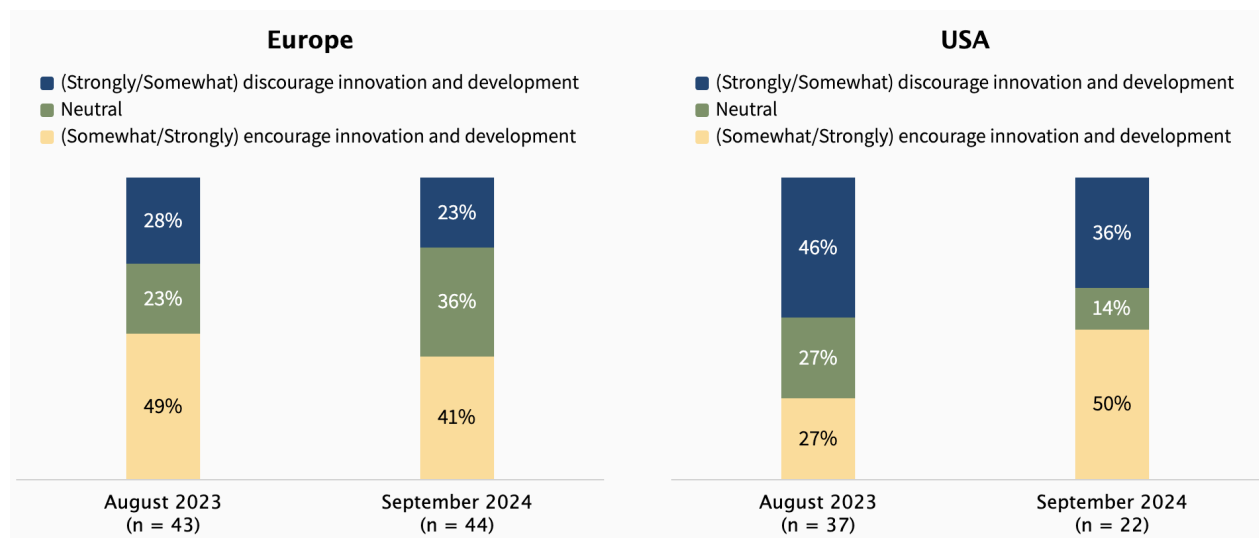
Figure 4. Influence of laws on development of privacy-preserving practices and technologies

3.4 Comprehensiveness of digital privacy laws

There is a notable difference between stakeholders in Europe and the USA regarding whether digital privacy laws cover the necessary areas (Figure 5). In Europe, 55% in 2022, 57% in 2023 and 43% in 2024 felt the laws cover fewer areas than needed. In the USA, 100% of respondents in 2022, 94% in 2023 and 95% in 2024 felt that the laws cover fewer areas than required, suggesting a broader dissatisfaction in the US about the comprehensiveness of these laws.
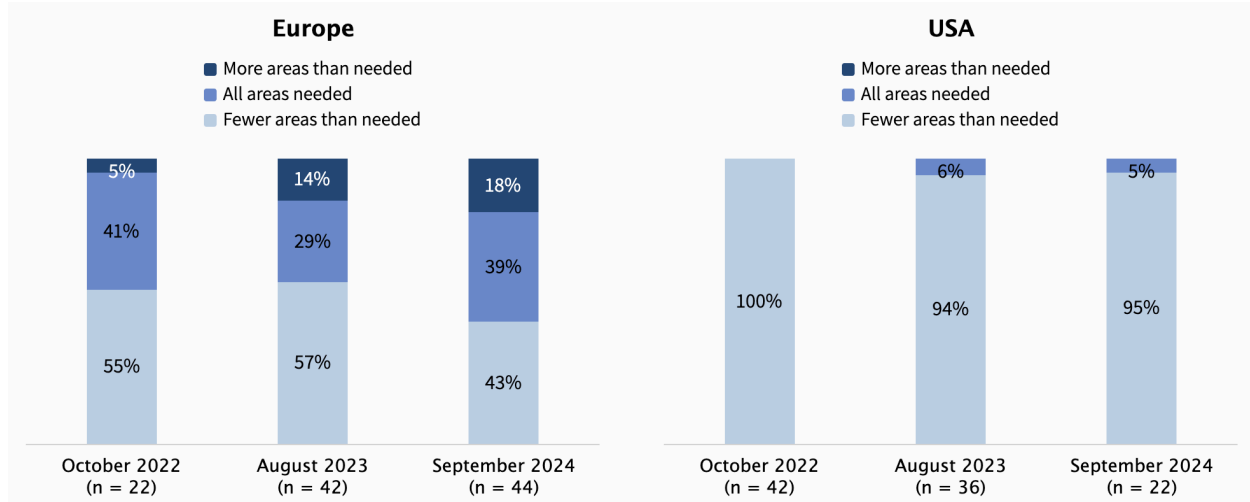

Figure 5. Comprehensiveness of digital privacy laws

3.5 Enforcement of digital privacy practices

The enforcement of digital privacy practices presents an interesting contrast between Europe and the USA (Figure 6). In Europe, there's a noticeable increase in the belief that privacy practices are "Mostly" enforced, rising from 9% in October 2022 to 27% in August 2024. Meanwhile, in the USA, perceptions remain more stable with a slight increase in minimal enforcement, suggesting that privacy practices are "A little" enforced. This contrast highlights the varying levels of regulatory enforcement and public perception, with Europe moving towards stronger enforcement and the USA showing more mixed views.
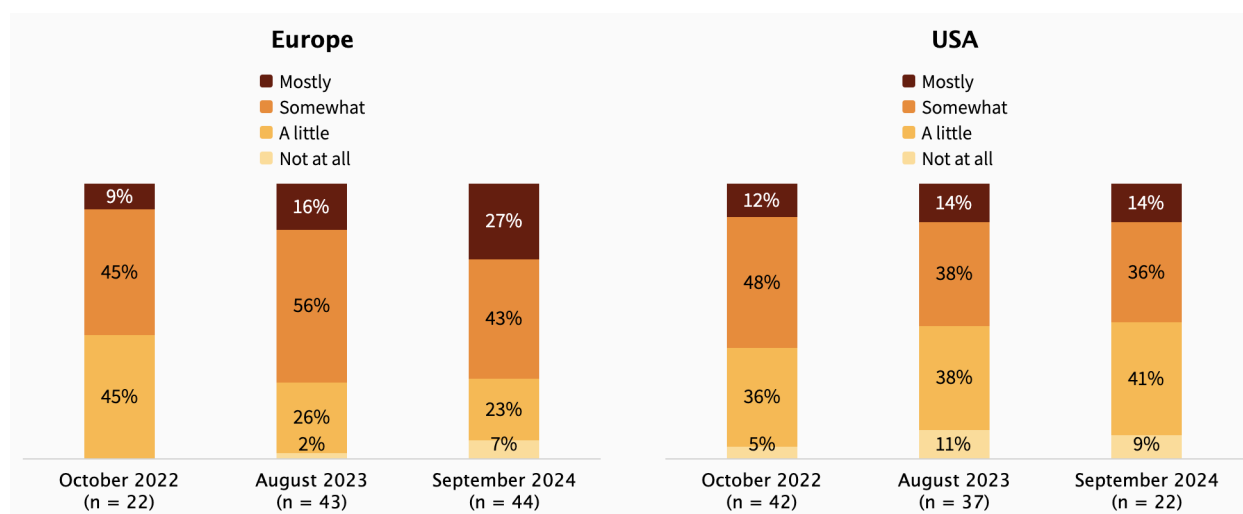
Figure 6. Enforcement of digital privacy practices

3.6 Current and future outlook of digital privacy laws

Respondents generally perceive EU digital privacy laws more favorably compared to those in the USA. Figure 7 shows that the percentage of respondents rating the current state of EU digital privacy laws as good or excellent increased from 48% to 59% over the past year. Conversely, while 100% of respondents classified the USA's digital privacy laws as poor or fair in 2023, this figure decreased to 91% in 2024, with 9% now evaluating them as good or excellent.

When considering the future, optimism about the EU's digital privacy trajectory declined, with the percentage of optimistic respondents dropping from 49% to 36%. Opinions about the USA's future regulations remain divided, with 41% of respondents still expressing pessimism and 45% expressing optimism.
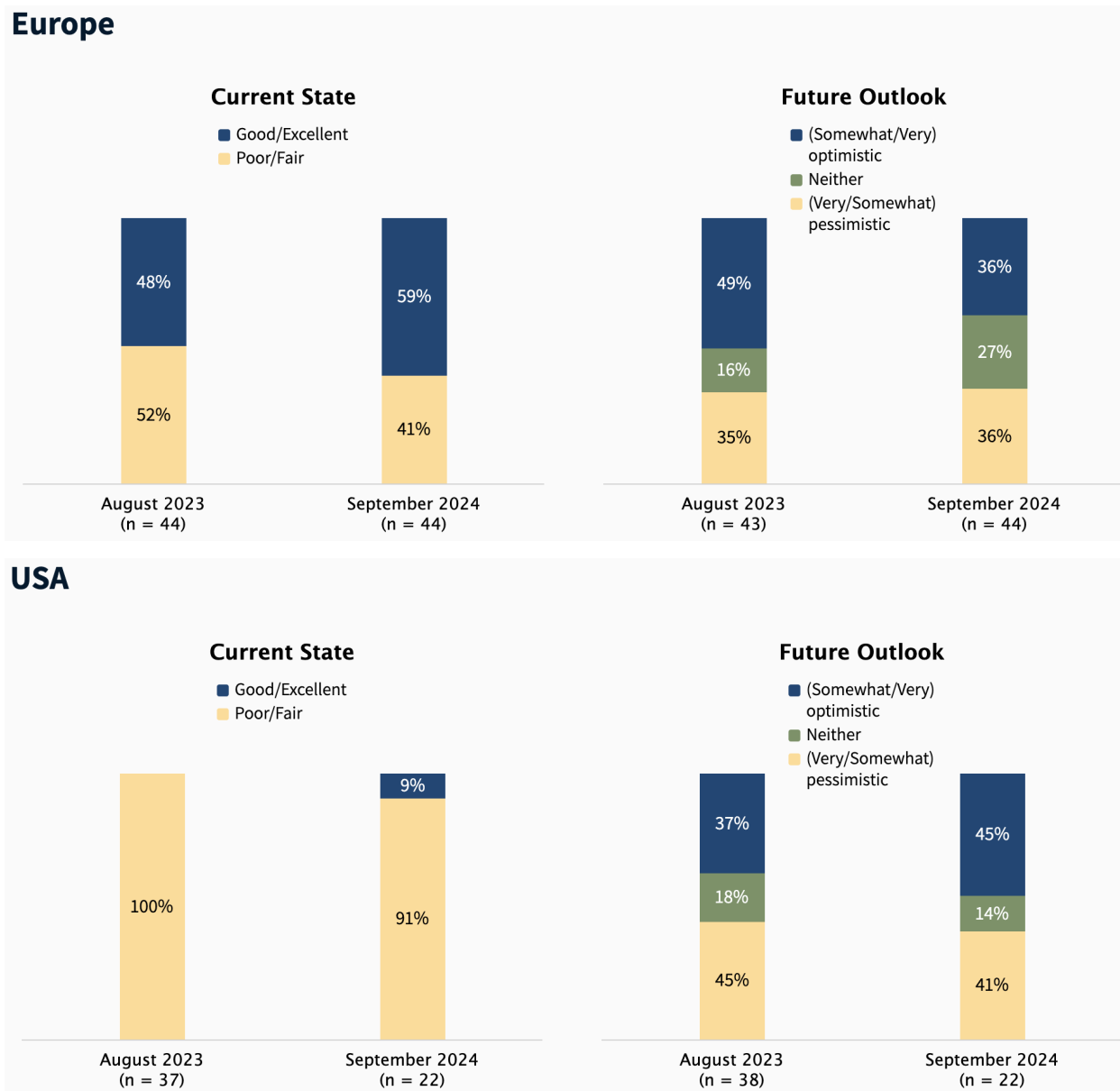
Europe

Current State	Future Outlook

Current State legend:
- ■ Good/Excellent
- ■ Poor/Fair

Future Outlook legend:
- ■ (Somewhat/Very) optimistic
- ■ Neither
- ■ (Very/Somewhat) pessimistic

Current State (Europe):
- August 2023 (n = 44): Good/Excellent 48%, Poor/Fair 52%
- September 2024 (n = 44): Good/Excellent 59%, Poor/Fair 41%

Future Outlook (Europe):
- August 2023 (n = 43): optimistic 49%, Neither 16%, pessimistic 35%
- September 2024 (n = 44): optimistic 36%, Neither 27%, pessimistic 36%

USA

Current State	Future Outlook

Current State legend:
- ■ Good/Excellent
- ■ Poor/Fair

Future Outlook legend:
- ■ (Somewhat/Very) optimistic
- ■ Neither
- ■ (Very/Somewhat) pessimistic

Current State (USA):
- August 2023 (n = 37): Poor/Fair 100%
- September 2024 (n = 22): Good/Excellent 9%, Poor/Fair 91%

Future Outlook (USA):
- August 2023 (n = 38): optimistic 37%, Neither 18%, pessimistic 45%
- September 2024 (n = 22): optimistic 45%, Neither 14%, pessimistic 41%

Figure 7. Enforcement of digital privacy practices

3.7 Policy making approaches in digital privacy protection

The pessimistic evaluation of privacy laws in the USA might be attributed to its fragmented privacy framework. As Figure 8 shows, 64% of respondents believe that 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. None of the respondents believe it should be determined solely at the state level, which reflects the current situation. In Europe, 3% of respondents think that privacy laws should be made exclusively at the EU member-state level, while 56% support an EU-level approach only and 41% favor a combination of both levels.
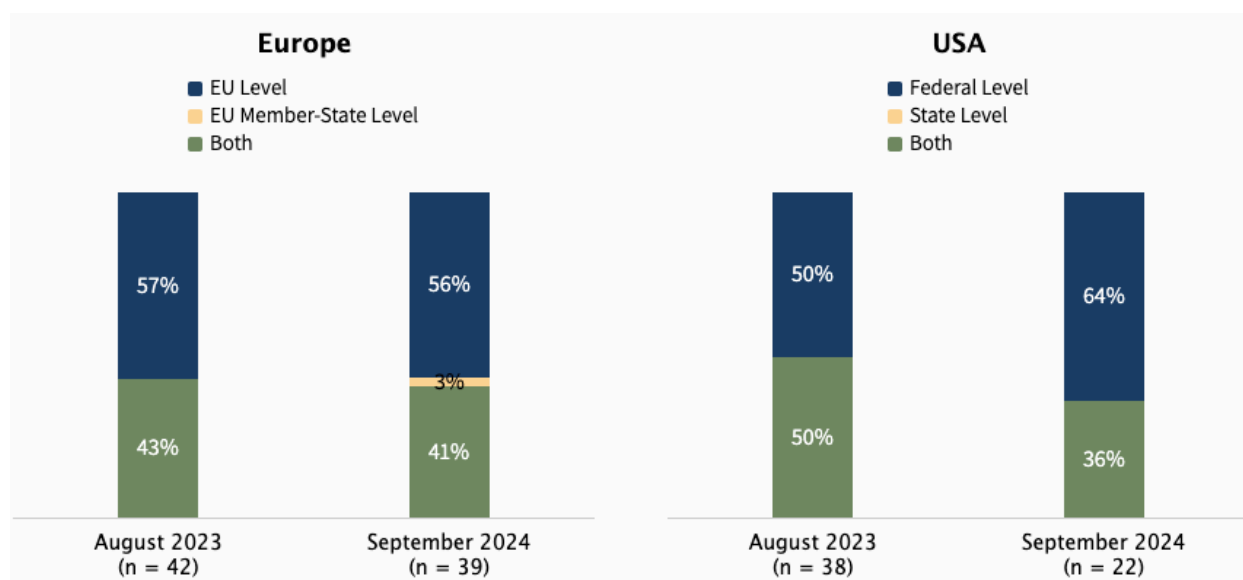
Figure 8. Policymaking approaches in digital privacy protection

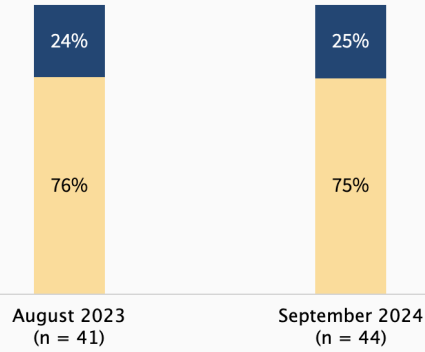## 3.8 Current and future outlook of organizational digital privacy practices

Regarding the overall assessment of organizations' digital privacy policies and practices (Figure 9), the current state remains negative, especially in the USA, where 95% of respondents rated it as poor or fair in 2024, compared to 91% in 2023. In Europe, 75% and 76% of respondents evaluated it negatively in 2024 and 2023, respectively.

The future outlook for organizational digital privacy is more optimistic in Europe than in the USA, though it declined from 2023 to 2024: in 2023, 55% of respondents viewed it as somewhat or very optimistic, but this dropped to 32% in 2024. Many respondents shifted to a neutral stance, with those indicating "neither" increasing from 17% to 41%. In the USA, the future outlook remains pessimistic, with 57% of respondents being very or somewhat pessimistic in 2023 and 55% in 2024, and those seeing it as somewhat or very optimistic decreased from 31% to 18%.
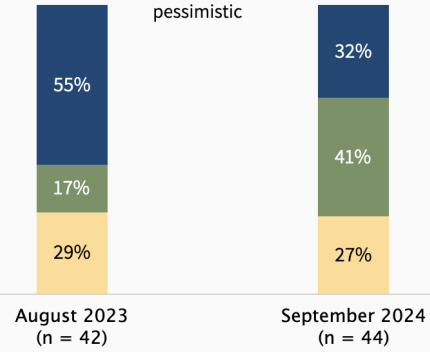
Europe

Current State
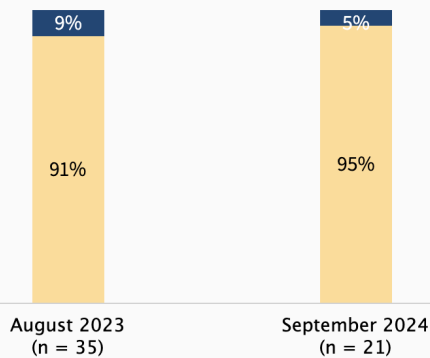
- ■ Good/Excellent
- ■ Poor/Fair

August 2023 (n = 41)	September 2024 (n = 44)
24%	25%
76%	75%

Future Outlook

- ■ (Somewhat/Very) optimistic
- ■ Neither
- ■ (Very/Somewhat) pessimistic

August 2023 (n = 42)	September 2024 (n = 44)
55%	32%
17%	41%
29%	27%

USA

Current State

- ■ Good/Excellent
- ■ Poor/Fair

August 2023 (n = 35)	September 2024 (n = 21)
9%	5%
91%	95%

Future Outlook

- ■ (Somewhat/Very) optimistic
- ■ Neither
- ■ (Very/Somewhat) pessimistic

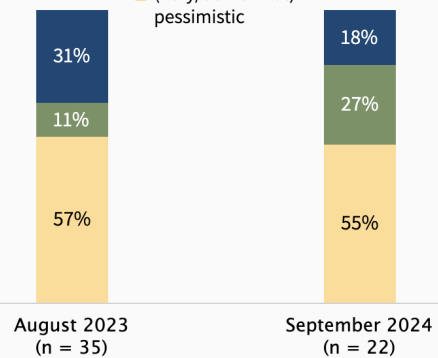| August 2023 (n = 35)	September 2024 (n = 22)
31%	18%
11%	27%
57%	55%

Figure 9. Current and future outlook of organizational digital privacy practices

3.9 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 organizations, which include Meta, Google, Amazon, Visa, Mastercard, Apple, and Microsoft. 24% of the respondents for the USA and 18% for Europe evaluate the privacy protection performance of public institutions as excellent (Figure 10). On the other hand, 45% of the respondents from Europe and 34% from the USA evaluate the privacy protection performance of private organizations as poor. For detailed analysis for specific organizations we refer to our dynamic data visualization tool at https://privacyperceptions.org/results/.
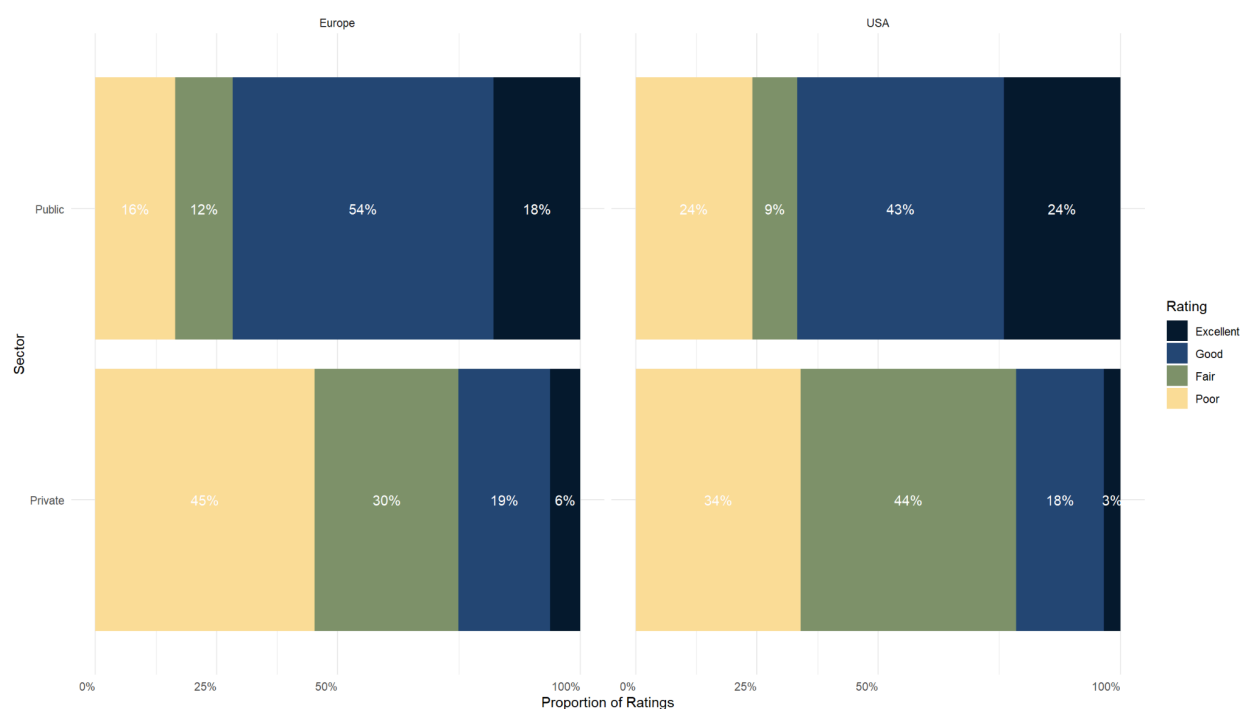

Figure 10. Organizations privacy protection performance ratings

3.10 Most important approach in protecting people's digital privacy

In Wave 5, "enforcing rules about how data is processed, stored, and shared" emerged as the most crucial approach to protecting individuals' digital privacy for Europeans(Figure 11), with the highest percentage of respondents ranking it as their top priority (30%). However, in Wave 2, this focus on enforcement dropped to fifth place (16%, Figure 13), with the emphasis shifting to "designing and deploying privacy-preserving technology" as the primary priority (27%).

In 2024, "regulating how data is processed, stored, and shared" was generally a lower priority, with 35% of respondents ranking it as least important (rank number 5) while in 2023, "giving individuals control over their data" was the least important with 34% of respondents ranking it as 5.

Interestingly, in 2024, 36% of privacy experts in the USA stated that "giving individuals control over their data" is both the most important and least important aspect (Figure 12). While "giving individuals control over their data" was the least important approach in protecting people's digital privacy in 2023 (47%, Figure 14), the most important were "designing and deploying privacy-preserving technology" and "regulating data processing, storage and sharing" with 29% of the respondents ranking them as number 1.

Regional preferences also varied: in 2024, USA experts placed a higher emphasis on data control, with 36% ranking it as their top priority compared to 12% of European experts. Conversely, European experts favored technology-based solutions, with 28% ranking it number one compared to only 9% of USA experts. Processing regulations ranked consistently low for both groups, with more European experts (35%) than USA experts (23%) designating it as the lowest priority (number 5).
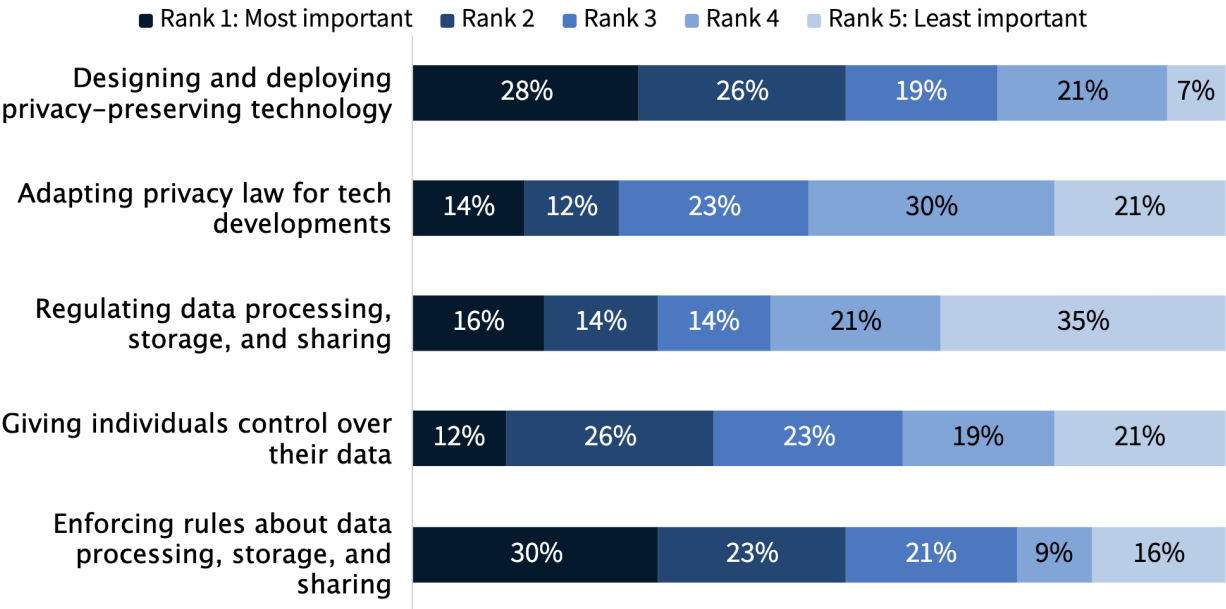
Wave 5 (September 2024): Europe

Figure 11. Wave 5 (September 2024) Ranking of Approaches to Protecting People's Digital Privacy in Europe
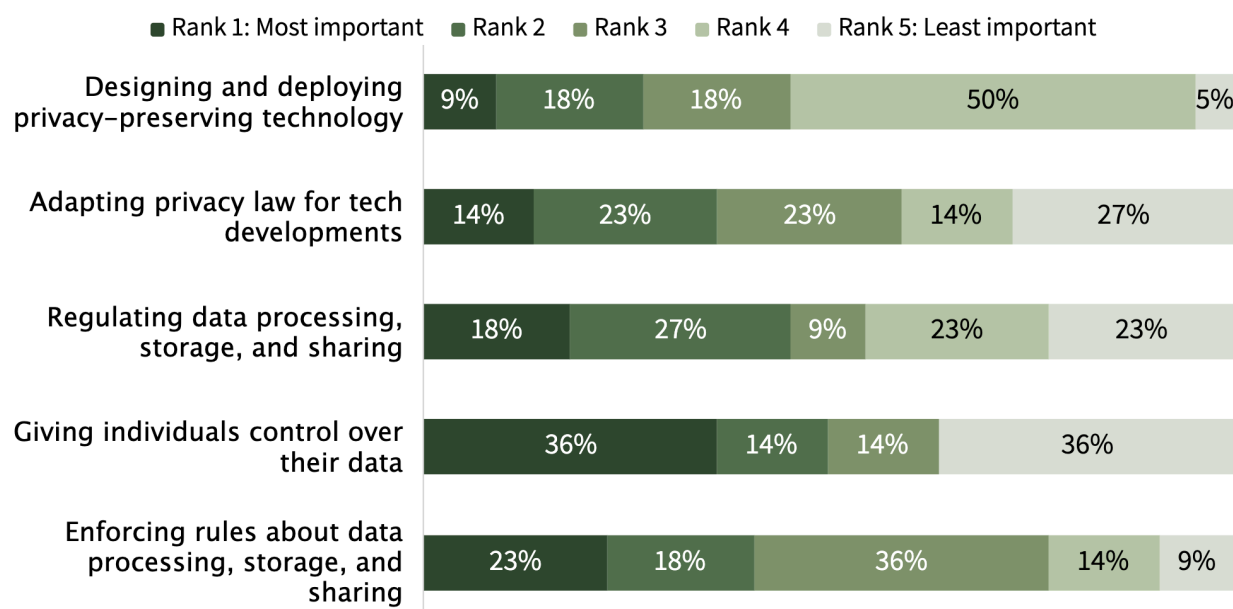
Wave 5 (September 2024): USA

Legend: ■ Rank 1: Most important ■ Rank 2 ■ Rank 3 ■ Rank 4 ■ Rank 5: Least important

Approach	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
Designing and deploying privacy-preserving technology	9%	18%	18%	50%	5%
Adapting privacy law for tech developments	14%	23%	23%	14%	27%
Regulating data processing, storage, and sharing	18%	27%	9%	23%	23%
Giving individuals control over their data	36%	14%	14%		36%
Enforcing rules about data processing, storage, and sharing	23%	18%	36%	14%	9%

Figure 12. Wave 5 (September 2024) Ranking of Approaches to Protecting People's Digital Privacy in the USA

Wave 2 (August 2023): Europe

Legend: ■ Rank 1: Most important ■ Rank 2 ■ Rank 3 ■ Rank 4 ■ Rank 5: Least important

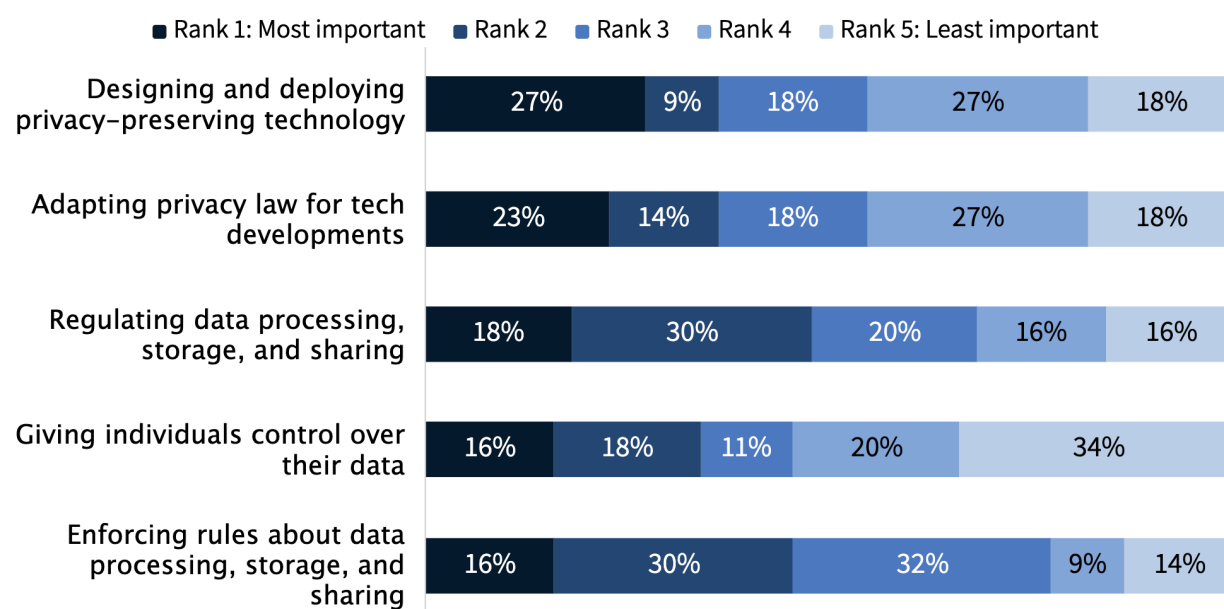| Approach	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
Designing and deploying privacy-preserving technology	27%	9%	18%	27%	18%
Adapting privacy law for tech developments	23%	14%	18%	27%	18%
Regulating data processing, storage, and sharing	18%	30%	20%	16%	16%
Giving individuals control over their data	16%	18%	11%	20%	34%
Enforcing rules about data processing, storage, and sharing	16%	30%	32%	9%	14%

Figure 13. Wave 2 (August 2023) Ranking of Approaches to Protecting People's Digital Privacy in Europe
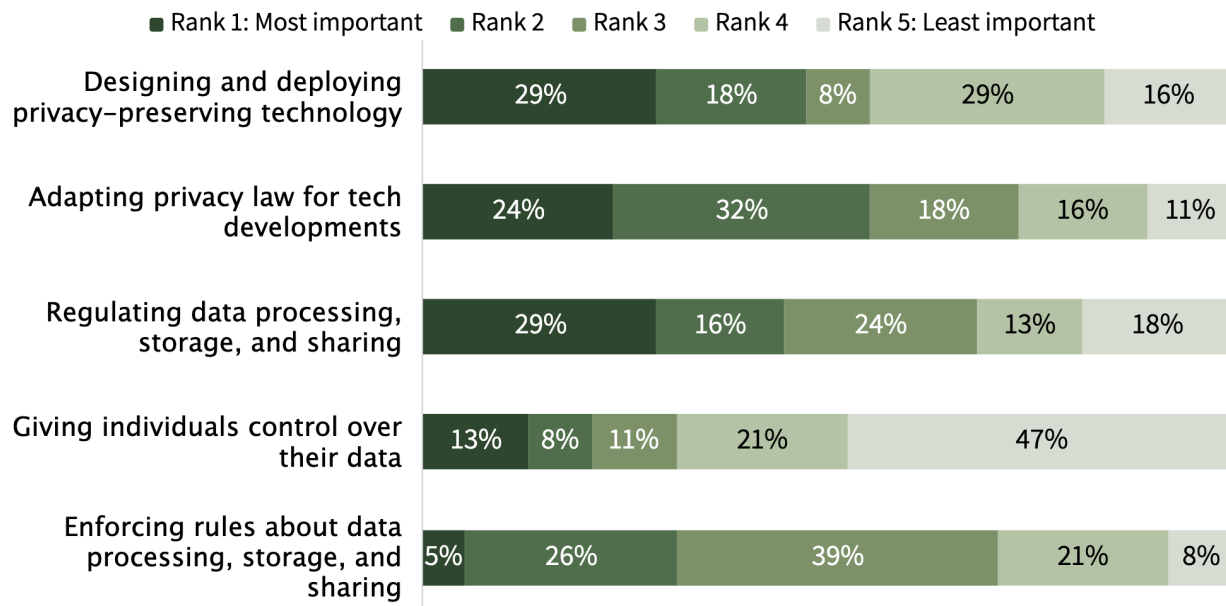
Wave 2 (August 2023): USA

Figure 14. Wave 2 (August 2023) Ranking of Approaches to Protecting People's Digital Privacy in the USA

3.11 Impact of the EU AI Act on AI innovation

Proposed by the European Unit, the EU AI Act[2] is the world's first comprehensive attempt to regulate AI at establishing guidelines and restrictions on the development, deployment, and use of artificial intelligence within the EU.

The results indicate varied perceptions between Europe and the USA on the EU AI Act's impact on innovation. In Europe, opinions are relatively balanced, with 36% believing it will neither enable nor hinder AI innovation, while 30% feel it may hinder innovation, and 18% think it will enable it. In contrast, the USA shows a stronger inclination towards skepticism, with 41% of respondents suggesting the Act is more likely to hinder innovation, and only 5% seeing it as potentially enabling. Additionally, a notable 23% in the USA and 16% in Europe responded with "don't know," reflecting some uncertainty in both regions regarding the Act's potential outcomes. This contrast highlights regional differences in attitudes towards regulatory impacts on AI progress.

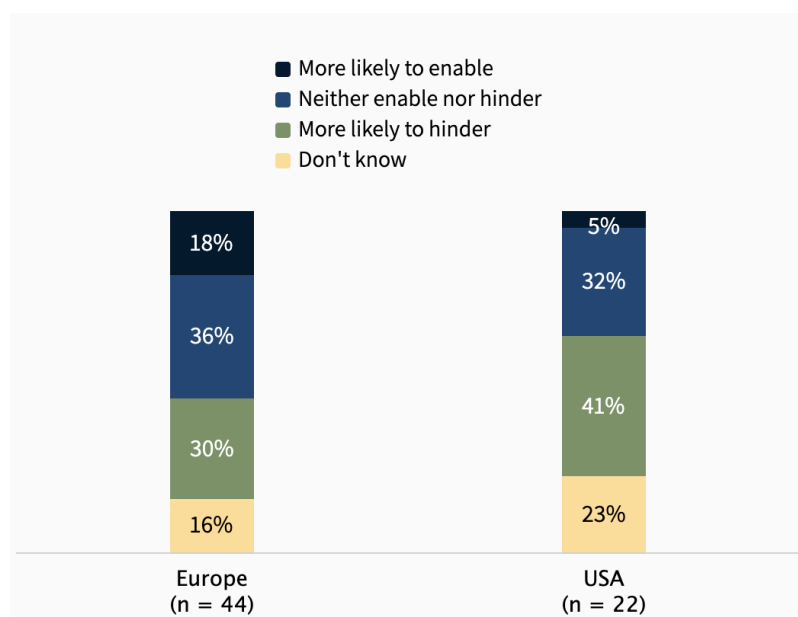[2] https://artificialintelligenceact.eu/ Retrieved on Oct 29, 2024 .

Figure 15. Impact of the European Artificial Intelligence Act on AI innovation

5 Conclusions and recommendations

The fifth wave of the Transatlantic Privacy Perceptions (TAPP) panel survey highlights significant insights into the current state of digital privacy laws and practices between the USA and Europe. According to the survey, European privacy laws are increasingly seen as favoring individual users, while in the USA, privacy laws are largely perceived as favoring businesses. This divergence underscores the differing approaches to privacy regulation on either side of the Atlantic. In the USA, there is a growing perception that privacy laws encourage innovation, reflecting a positive shift towards recognizing the benefits of privacy regulations in fostering technological advancements. In contrast, this perception has slightly declined in Europe, indicating a more balanced view. European privacy laws continue to receive more favorable perceptions from the TAPP panelists, although optimism about future advancements has declined. On the other hand, negative views on current privacy laws persist in the USA, but there is a slight increase in optimism about future improvements. This suggests a cautious yet hopeful outlook towards the evolution of privacy regulations.

The survey indicates that enforcing rules on data processing, storage, and sharing is the top priority for protecting digital privacy in Europe. By comparison, USA experts prioritize giving individuals control over their data. European experts, however, favored technology-based solutions. Processing regulations ranked consistently low for both groups, with more European experts than USA experts designating it as the lowest priority. These findings highlight regional preferences and evolving priorities to develop more effective and comprehensive digital privacy strategies.

Appendix

A.1. TAPP Panel Questionnaire Wave 5

[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.

[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

---

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?

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

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]
[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]
[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?

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

law_breadth_m_oe
What areas are covered that you feel shouldn't be? _____

law_breadth_f_oe
What areas are not covered that you feel should be? _____

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

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

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

☐ 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?

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

policymaking_US
Do you think that digital privacy policy in the US should be made at the …
- ☐ Federal level
- ☐ State level
- ☐ Both

policymaking_EU
Do you think that digital privacy policy in the EU should be made at the …
- ☐ EU-level
- ☐ EU member-state level
- ☐ Both

orgs_rating
orgs_rating_pub
b) How would you rate the performance of these government agencies in protecting people's digital privacy?
- ● [org_census] US Census Bureau
- ● [org_irs] US Internal Revenue Service
- ● [org_ssa] US Social Security Administration

- ● [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
- [org_google] Google
- [org_meta] Meta (including Facebook, Instagram, Whatsapp, Oculus)
- [org_amazon] Amazon
- [org_microsoft] Microsoft
- [org_visa] Visa
- [org_mastercard] Mastercard

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

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

state_current_pra
Overall, 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]
[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]
[PRG: Same randomization as state_outlook_law]
[PRG: Single choice]

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

☐ Very pessimistic

priorities
How would you rank the importance of the following approaches to protecting people's digital privacy?
To rank the items, drag and drop them.
[PRG: Randomize]
[PRG: Ranking question]
    ☐ [priorities_techsolutions] Designing and deploying privacy-preserving technology
    ☐ [priorities_processing] Regulating how data is processed, stored and shared
    ☐ [priorities_enforcement] Enforcing rules about how data is processed, stored and shared
    ☐ [priorities_control] Giving individuals control over their data
    ☐ [priorities_adaptlaw] Adapting privacy laws to respond to current technological developments

EU AI Act
In your opinion, will the EU AI Act be more likely to enable or hinder AI innovation? [RANDOMIZE SCALE ORDER]
    ☐ More likely to enable
    ☐ Neither enable nor hinder
    ☐ More likely to hinder
    ☐ Don't know

[PRG: Same page]
EU_AI_enable
[PRG: Ask if **EU_AI_act** is "More likely to enable"]

How do you think the EU AI Act will enable AI innovation? [PRG: Textbox]
_____.

[PRG: Same page]
EU_AI_hinder
[PRG: Ask if **EU_AI_act** is "More likely to hinder"]

How do you think the EU AI Act will hinder AI innovation? [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

sector_paid
Which of the following statements applies to you?
☐ I perform privacy-related activities as part of my paid job
☐ I perform privacy-related activities as a volunteer or activist

sector
Which sector do you currently work in?
☐ Academia
☐ Government
☐ Journalism
☐ Law
☐ Non-profit / NGO / Think tank
☐ Tech industry
☐ non-Tech industry
☐ None of the above

[Feedback]

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?
☐ Yes
☐ No

language_en
Were you comfortable completing this survey in English?
☐ Yes

☐ No

language_other
What language would you have preferred?
☐ French
☐ German
☐ Italian
☐ Spanish
☐ Other: _____ [PRG: specify]

[Email & Name]

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]

_____

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

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]

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.

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.