How Experts Think About Digital Privacy - Interview Report

July 2025

IEEE Digital Privacy

IEEE
Advancing Technology
for Humanity

Disclaimer

The opinions and statements voiced by the experts in the interviews do not necessarily reflect the opinion of IEEE Digital Privacy. This report is provided to further the global discussion of digital privacy.

Capsule Summary

In an effort to understand digital privacy and to refine the IEEE Digital Privacy Model, a project was undertaken involving in-depth interviews with 23 global experts in digital privacy, law, technology, and policy. The primary objectives were to understand each expert's definition of digital privacy, explore individual expectations of privacy and the forces that shape those expectations, understand global variations in privacy expectations, and gather insights on achieving digital privacy.

Key Findings

1. **Privacy Means Control, Not Just Secrecy** - Experts overwhelmingly defined digital privacy as the ability to control one's data—what is collected, how it's used, and who can access it.
2. **Transparency Is Essential—but Often Absent** - Many users are unaware of how their data is collected or used. Experts said transparency is the foundation of meaningful consent but is frequently lacking in real-world systems.
3. **Consent Is Broken** - Consent mechanisms today—like cookie banners and privacy policies—are largely performative. True informed consent is rarely achieved.
4. **Trust in Systems Is Eroding** - Widespread surveillance, data breaches, and manipulative data use have diminished public trust in digital platforms and institutions.
5. **Privacy Is a Global, Contextual Concept** - Expectations vary dramatically across regions. In Europe, privacy is viewed as a human right; in the U.S., more as a consumer issue; in China, privacy often yields to state control.
6. **Information Asymmetry Undermines Privacy** - Users face a profound knowledge gap compared to companies and platforms. This imbalance makes meaningful privacy decisions nearly impossible.
7. **AI Is Reshaping the Privacy Landscape** - Artificial intelligence introduces new privacy risks, especially through inference—deducing sensitive traits from indirect data without consent.
8. **Not All Data Is Equally Sensitive** - Financial, health, biometric, and children's data are seen as especially sensitive. But even low-sensitivity data can become harmful when aggregated or inferred.
9. **Privacy Is About Power** - Experts repeatedly emphasized that privacy is a matter of power dynamics. Individuals often lack meaningful choices or alternatives to invasive systems.
10. **The Privacy Paradox Is Real** - People say they care about privacy but routinely accept risks for convenience—often due to lack of viable alternatives or resignation.
11. **Younger and Older Generations View Privacy Differently** - Older users see privacy as secrecy; younger users see it as control over context. Both groups express frustration with current systems.
12. **Compliance Isn't Enough** - Experts said legal compliance is often treated as a checkbox. True privacy protection requires a shift toward ethical responsibility and proactive risk mitigation.
13. **Public Education Alone Won't Fix It** - While digital literacy helps, experts argued that users shouldn't bear the burden of understanding complex systems. Systemic changes are needed.
14. **Privacy by Design Is Essential—but Rarely Practiced** - Experts called for privacy to be embedded into system architecture from the start, rather than added as an afterthought.
15. **Stronger Enforcement Is Needed** - Even with strong laws like GDPR, lack of enforcement and corporate resistance limit their effectiveness. Clear consequences and consistent oversight are required.

Table of Contents

Navigating this report:
This report includes hyperlinks.
Control/Click on "Table of Contents" pages or "Detailed Findings" to jump to that section in the report.

Purpose, Methodology & Experts Interviewed

Purpose, Methodology and Experts Interviewed

Purpose

To further the discussion of digital privacy, this project engaged 23 global experts in digital privacy, law, technology, and policy. Through in-depth interviews, the goal was to explore how digital privacy is understood, implemented, and challenged across different regions and disciplines.

Experts shared their definitions of digital privacy, offering perspectives shaped by their professional backgrounds and cultural contexts. The discussions sought to identify commonalities and differences in privacy expectations worldwide, examining how regulatory frameworks, societal norms, and technological landscapes influence individuals' rights and protections.

Participant Diversity & Expertise

The participants in this study were selected to ensure a diverse range of expertise and perspectives on digital privacy. The IEEE team leading this project played a key role in identifying potential interviewees, drawing from their professional networks and research.

Many participants were handpicked by the IEEE team based on their expertise in privacy law, cybersecurity, AI ethics, and digital governance. Some interviewees were recommended by other IEEE members or colleagues familiar with their work in digital privacy. A few experts were identified through independent research, ensuring a broad, global representation of privacy professionals.

Initial outreach was conducted by IEEE, introducing the project and inviting experts to participate. Scheduling and interviewing were handled by the lead researcher (Robin Wedewer), who conducted each interview via Zoom. Interviews lasted approximately one hour. All participants were offered a $100 International VISA gift card as a token of appreciation for their time and expertise.

The participants include lawyers, academic researchers, policymakers, regulatory authorities, engineers, and technology consultants, providing a multidisciplinary view of privacy challenges and solutions.

A significant number of the interviewees are legal professionals, including privacy lawyers, regulatory advisors, and legal scholars specializing in data protection laws such as GDPR, CCPA, and emerging national privacy frameworks. Their expertise provides a deep understanding of privacy legislation, enforcement challenges, and legal loopholes that shape global privacy policies.

Purpose, Methodology and Experts Interviewed

Academia is well-represented, with five computer science and engineering professors who specialize in areas such as cryptography, artificial intelligence, cybersecurity, and privacy-enhancing technologies. Their contributions highlight the technical dimensions of privacy, including the risks posed by AI inference, biometric surveillance, and metadata tracking.

Several privacy and cybersecurity consultants (3 participants) contributed practical insights on organizational compliance, corporate privacy strategies, and risk mitigation in both public and private sectors.

Privacy researchers (5 participants) brought an investigative lens to the discussions, exploring privacy vulnerabilities in digital systems, AI-driven data profiling, and the role of emerging technologies in reshaping digital identity management.

Additionally, regulatory and policy experts (5 participants) provided perspectives from government agencies, advocacy groups, and regulatory bodies.

Geographic Representation

The participants represent 11 countries, including experts from Europe (Italy, France, Germany, Spain, Portugal, Greece, Belgium, UK), North America (Canada, USA), and Australia/New Zealand.

Note About Quotes in this Report

Quotes used in this report may have been edited for clarity and conciseness.

Experts Interviewed

Country	Area of Expertise	Years Experience in Digital Privacy
Australia	Cybersecurity & Ethics Expert	25 years
Germany	Privacy Researcher and Medical Faculty Member	6 years
Portugal	Professor of Engineering	20+ years
Italy	Regulatory Authority	20+ years
Canada	Digital Privacy Consultant	7 years
United States	Digital Privacy Consultant	15 years
United Kingdom	Privacy Policy Lawyer	4 years
Belgium	Policy & Communications Expert	20 years
United States	Privacy Policy Lawyer	several years
Greece	Computer Science Professor	15 years
Scotland	Professor of Computer Science and Engineering	2 years
Spain	Surgeon and Medical Privacy Researcher	10 years
United Kingdom	Professor and Cybersecurity Expert	7 years
United States	Digital Privacy Expert	7 years

Country	Area of Expertise	Years Experience in Digital Privacy
United Kingdom	Privacy Policy Lawyer	8 years
United Kingdom	Professor and AI/Privacy Researcher	17 years
Australia	Privacy & Security Expert	7 years
Canada	Privacy & National Security Researcher	15-20 years
United States	Privacy Lawyer & AI/Human Rights Expert	9 years
Australia	Cryptography & Privacy Researcher	20 years
Australia	Cybersecurity Consultant	25 years
New Zealand	Digital Identity Specialist	20 years
Australia	Digital Privacy Expert	20 years

Executive Summary

What is Digital Privacy?

Ask ten experts what digital privacy means, and you'll get ten variations—but common themes emerge. Privacy isn't just about secrecy; it's about control, transparency, consent, and trust. It's the ability to decide who has access to your data and how it's used.

One digital privacy consultant described privacy as "the ability to control one's data and decide who has access to it." But control is meaningless without transparency—if people don't know how their data is collected and shared, they can't make informed choices. A privacy policy lawyer puts it plainly: "Privacy is about transparency—people should know what data is collected and how it's used."

Yet, they said that today's privacy policies rarely provide clarity. People trade privacy for convenience without realizing it, navigating (or ignoring) legal jargon that obscures the reality of data collection. True informed consent is often a myth.

Privacy requires trust—in governments, corporations, and digital platforms. But that trust is eroding, fueled by data breaches, hidden tracking, and government surveillance.

While definitions of digital privacy vary, certain principles remain fundamental:

- **Control** – Individuals should determine what happens to their data.
- **Transparency** – Users must understand how data is collected and used.
- **Consent** – Choices about privacy should be real, not forced.
- **Trust** – Without confidence in privacy protections, they lose meaning.

Privacy is not a fixed concept. It evolves as technology, law, and cultural expectations shift. But at its heart, privacy is about power: who has it, who doesn't, and what can be done to protect individuals in a data-driven world. Detailed Findings

Frameworks for Thinking About Digital Privacy

How these experts think about digital privacy is shaped by the work they do. A privacy lawyer, for instance, is likely to focus on legal compliance—ensuring companies follow the rules, avoid liability, and navigate regulatory frameworks like GDPR or HIPAA. A healthcare professional, on the other hand, sees privacy as a duty of care, a responsibility to protect sensitive patient information from misuse or exposure. Meanwhile, cybersecurity professionals and engineers often approach privacy through the lens of risk management, asking what threats exist, how likely they are, and what steps can be taken to mitigate them.

Continued next page

Despite these differences, no single framework fully defines privacy. Instead, privacy is an intersection of law, ethics, security, and personal autonomy, viewed differently depending on the priorities of those involved.

Through the expert interviews, several dominant frameworks for thinking about privacy emerged:

Privacy as Regulatory Compliance

For many of these experts, privacy is a matter of following the law. Organizations operating in multiple jurisdictions must comply with an evolving patchwork of privacy laws—GDPR in Europe, CCPA in California, China’s PIPL, and others. But while legal frameworks provide structure, they don’t always guarantee meaningful privacy protection. As a privacy lawyer and AI/human rights expert, put it: “Compliance is the minimum. But without enforcement, regulations are just paper laws.” A regulatory authority in Italy agreed, arguing that “Privacy needs clear accountability. Without strong legal frameworks, it’s just a vague ethical idea.”

The compliance model of digital privacy ensures organizations meet legal requirements, but it often prioritizes avoiding penalties over truly respecting privacy.

Privacy as a Duty of Care

In fields like healthcare and finance, privacy is about more than compliance—it’s about preventing harm. A privacy breach isn’t just an administrative failure; it can have devastating consequences. A surgeon and medical privacy researcher put it plainly: “Privacy in healthcare is not just about compliance; it’s about protecting patients from harm. A breach isn’t just a legal issue—it can be life-altering.” One expert likened data protection to handling sensitive medical material: “Data should be handled as carefully as any other sensitive material—like medication. Mishandling it can be dangerous.”

This duty-of-care framework acknowledges that privacy violations can have far-reaching, real-world impacts—from identity theft to medical discrimination.

Privacy as Human Dignity

Some experts took a more philosophical view, seeing privacy as a fundamental component of human dignity and autonomy. A policy and communications expert argued that “The ability to control your digital identity is as important as controlling your real-world identity. Privacy is about dignity.” Similarly, a cybersecurity consultant warned about the dangers of a surveillance society, stating: “People deserve to exist without being constantly watched.”

This perspective aligns privacy with broader human rights concerns, emphasizing that privacy violations aren’t just technical failures—they can lead to oppression and loss of freedom.

Privacy as Trust

For many engineers and technologists, privacy is fundamentally about trust in digital systems. If people don’t trust platforms, they stop using them—or they share less information, limiting innovation. A privacy policy lawyer summed it up: “It really just comes down to trust. It's not just about following the rules, following the laws, it's about making sure that people genuinely feel that their personal information is safe.”

Continued next page

A privacy and security expert warned of the consequences when that trust is broken: “When privacy is broken, trust collapses. And when trust collapses, people disengage from digital systems altogether.”

This framework suggests that privacy protections are not just a matter of individual rights—they are critical to the long-term viability of digital ecosystems.

Privacy as a Human Right

For privacy advocates, the strongest case for privacy is its status as a fundamental human right. This perspective is especially prominent in Europe, where historical events—particularly surveillance and data misuse during and after World War II—shaped modern privacy laws. A digital identity specialist emphasized this connection: “Privacy is not a privilege—it’s a fundamental right that must be protected, like freedom of speech.” A privacy and AI/privacy researcher reinforced this idea, noting that “Privacy is essential to protecting other freedoms, like freedom from discrimination or political repression.”

Europe’s GDPR is rooted in this human rights-based approach, in contrast to the market-driven privacy models found in the United States.

Privacy as Risk Management

In cybersecurity and business, privacy is often framed as a risk to be managed, not just a legal or ethical concern. Organizations assess likelihood and impact, then apply safeguards accordingly. A cybersecurity consultant described it this way: “Privacy isn’t just about following rules—it’s about assessing risks, minimizing exposure, and preventing harm before it happens.”

One expert emphasized the need for a structured, proactive approach, stating “Organizations need to think of privacy breaches like financial risks—you calculate likelihood and severity, then put controls in place to reduce exposure.”

This framework is especially relevant for AI and algorithmic decision-making, where risks often emerge in unpredictable ways. A computer science professor warned that “Privacy risk isn’t just about the data you give—it’s about what AI can infer from the data you don’t even know you’re sharing.”

Corporate vs. Consumer Views on Privacy

Finally, a significant gap exists between how companies and individuals think about privacy. While consumers often assume they have more rights than they actually do, businesses tend to treat privacy as a compliance issue rather than a fundamental right.

A privacy policy lawyer explained that “Consumers believe they have more privacy rights than they actually do. They assume companies are required to protect their data in ways that aren’t legally mandated.” Most people assume companies can’t track them across services—but they can, unless explicitly prohibited by law.

For many companies, privacy compliance is just about avoiding legal trouble. One expert pointed out that for many companies, privacy compliance is just about avoiding penalties. If they can get away with collecting and using more data, they will. Monetization of data is a significant motivator to abuse. Many companies see privacy as a legal obligation rather than an ethical one. Consumers assume privacy protections exist, but companies only provide the bare minimum required by law. [Detailed Findings]

Continued next page

Expectations like access, notice, correction, and deletion are widely shared, yet not always legally guaranteed.

But should expectations be based on what average people assume or what a well-informed person knows is necessary? As one privacy policy lawyer put it, “We shouldn’t think about a lay person’s expectations. An informed person may have a different set of expectations that better safeguard an individual’s rights.”

The Information and Power Asymmetry

Experts emphasized that privacy is not a level playing field:

- **Information Asymmetry** – Privacy policies are lengthy and highly legalistic, making informed decision-making nearly impossible.
- **Time Asymmetry** – People interact with hundreds of digital services, making it unrealistic to understand and manage privacy settings for each one.
- **Power Asymmetry** – Many services provide no real opt-out, forcing users into choices that benefit companies, not individuals.

Privacy is Contextual

People care more about privacy in certain areas. For example, they are highly protective of medical and financial data but more relaxed about social media activity. Yet experts warned that even seemingly minor data, when combined, can reveal deeply personal insights.

Misconceptions That Shape Privacy Expectations

One of the most important—but often invisible—factors shaping digital privacy is how people misunderstand it. Interviews revealed that many users operate under comforting illusions: that data marked “private” stays that way, that consent through cookie banners is meaningful, or that anonymized data is safe. These misconceptions don’t just lead to poor individual decisions—they widen the gap between what people think is happening with their data and what actually is. That gap has consequences: it undermines trust, weakens regulatory protections, and allows bad actors to exploit user behavior in ways that are largely invisible. As privacy systems become more complex, so too must efforts to educate, simplify, and design around how people really think—not how we wish they did.

(Interview participants identified seven common misperceptions about privacy.)

Detailed Findings

Continued next page

Sensitivity of Information: What People Consider Most and Least Private

What people consider sensitive varies based on personal experience, cultural norms, and context. As a digital identity specialist put it, “Privacy is not one-size-fits-all. People react more strongly to certain types of data collection, but even those reactions depend on the situation.”

That said, some categories of information are almost universally regarded as highly private, while others are seen as lower risk or even public by default.

What People Consider Most Sensitive

Certain types of data consistently rank as highly sensitive due to the risk of fraud, identity theft, discrimination, or manipulation if exposed. All of the interview participants agreed that this information is considered most sensitive:

- **Financial Information** – Bank details, credit card numbers, and transaction history are seen as prime targets for criminals. People worry about identity theft more than almost any other privacy risk. However, individuals often overlook how their purchasing behavior is tracked and monetized beyond traditional financial fraud.
- **Health Data** – Medical records, prescriptions, and mental health histories are among the most tightly regulated data categories, yet breaches are common. People assume their medical records are safe—but they aren’t. Growing concerns around genetic data from consumer DNA testing services highlight new risks people don’t fully understand.
- **Biometric Data** – Fingerprints, facial recognition, and iris scans are particularly sensitive because they are permanent identifiers. Unlike passwords, they cannot be changed if compromised. Once biometric data is compromised, it’s compromised forever.
- **Location and Behavioral Data** – While many people voluntarily share their location for convenience, they often fail to consider the implications of constant tracking, surveillance, and profiling. People don’t mind sharing their location—until they realize how much is being tracked.
- **Information About Children** – Parents and guardians are particularly concerned about protecting children’s identities online, fearing exploitation, data theft, and long-term profiling.

Continued next page

Reputation, Identity, and Political Sensitivity

Some experts emphasized that people underestimate the risks of exposing identity-related information.

- **Political Affiliation** – Individuals don't always realize that liking a tweet or signing a petition can be used to infer political views, which may have consequences depending on their country's political climate.
- **Gender and Sexual Orientation** – In some regions, digital traces of someone's identity can put them at risk of discrimination or violence.
- **Deepfake and Image Manipulation** – The rise of AI-generated content means people can lose control over their own likeness.

What People Consider Less Sensitive

While financial and biometric data trigger strong privacy concerns, other types of information are often seen as lower risk—even when they may not be.

- **Aggregated or De-Identified Data** – Many people assume that data stripped of personally identifiable information (PII) is safe. However, experts warned that AI models can reconstruct identities with frightening accuracy from supposedly anonymous data.
- **Publicly Available Information** – Users freely share details about their lives online, assuming that anything posted publicly is fair game. Many people don't realize how easily public data can be collected, analyzed, and used against them.

Detailed Findings

Continued next page

Factors Influencing Expectations of Privacy

What people expect when it comes to privacy is shaped by personal experiences, cultural norms, education, and trust in institutions. Some assume their data is safe by default, while others view privacy as a constant battle. Across interviews, experts described how these influences shape privacy expectations—highlighting why they vary so dramatically from person to person.

Privacy Becomes Real When It’s Personal

For many, privacy is an abstract concern—until something goes wrong. Several experts noted that firsthand experiences, such as identity theft, financial fraud, or a data breach, often serve as wake-up calls. A privacy and national security researcher pointed out that “Most individuals only take privacy seriously after they’ve suffered a personal violation—whether that’s having their bank account hacked or seeing eerily accurate targeted ads.”

Social influence also plays a role. People learn from others. If friends or family start taking privacy seriously, you’re more likely to do the same.

Education and Digital Literacy: Knowing the Risks

People with greater digital literacy tend to be more skeptical about how their data is collected and used. Yet many lack the technical knowledge to grasp the scale of modern digital tracking.

A common misconception is that people assume privacy laws automatically protect them. But privacy protections vary widely depending on jurisdiction and enforcement. Those who understand these gaps tend to use encrypted messaging apps, VPNs, and privacy-focused browsers, but even among informed users, myths persist—like the false belief that anonymized data is truly anonymous.

A privacy and national security researcher pushed back on the idea that privacy literacy should fall on individuals: “We don’t expect people to understand how their cars work. Why should they be responsible for fully understanding digital privacy?”

Trust in Institutions

These experts said that how much people trust governments, corporations, and regulators shapes their privacy expectations.

- In countries with trusted governments, individuals are more willing to share personal data.
- In nations with corruption or mass surveillance, people assume data sharing is inherently risky.

Continued next page

Technology companies face a similar trust divide. After the Facebook–Cambridge Analytica scandal, trust in Big Tech plummeted, yet most people continue using their services anyway—a contradiction known as the privacy paradox.

One expert put it bluntly: “People don’t trust Big Tech, but they don’t see a way to opt out, either. Digital life is structured in a way that makes privacy difficult to maintain.”

Generational Shifts

These experts generally agree that younger and older generations think about privacy differently.

- **Older generations** (50+) tend to see privacy as not sharing information at all, prioritizing identity theft and financial security.
- **Younger generations** define privacy as controlling what they share and with whom. For them, privacy isn’t about secrecy—it’s about control. Despite sharing more online, younger users expect greater control over their data—and are frustrated when companies don’t provide it.

Cultural and Regional Differences: Privacy is Not Universal

Privacy expectations differ dramatically by region, shaped by historical and political factors.

- **Europe** – Privacy is viewed as a human right, heavily influenced by past government surveillance, such as the Stasi in East Germany.
- **United States** – Privacy is often framed as a consumer right rather than a human right, leading to fragmented laws based on industry rather than a unified framework. As a result, Americans expect to trade privacy for convenience far more than Europeans.
- **China** – Privacy concerns take a back seat to state security. Citizens expect extensive government surveillance and structure their online behavior accordingly.
- **Developing Nations** – In countries like Papua New Guinea, efforts to implement a national digital identity system faced resistance because Western-style privacy models didn’t align with local governance structures.

How individuals actually think about privacy has been measured. See next pages.

Detailed Findings

Continued next page

Global Data & Marketing Alliance's Privacy Segments

The Global Data & Marketing Alliance (GDMA) has surveyed citizens in 16 markets and reported its findings about privacy attitudes in the comprehensive report "Global Data Privacy: The Consumer Perspective 2022 report (Link)."

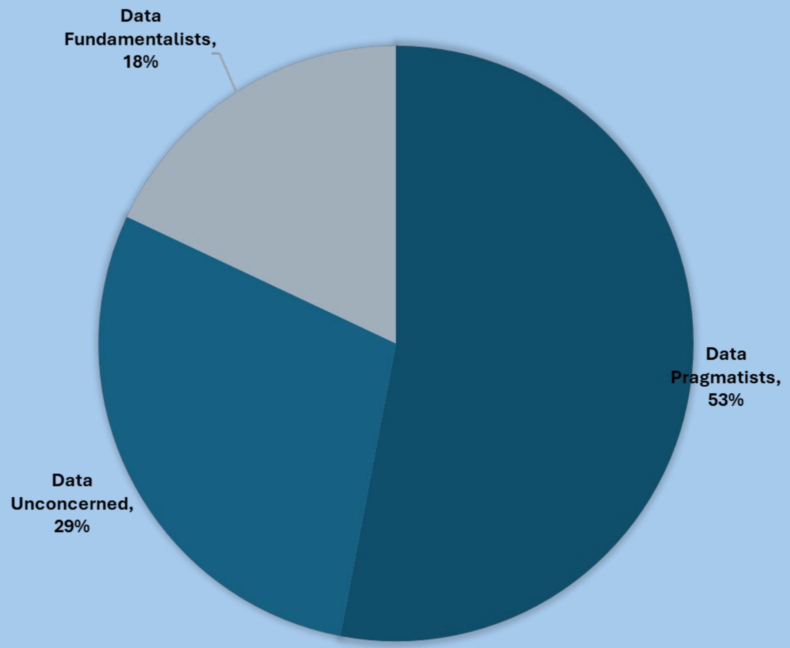
The GDMA describes three segments as follows:

- "**Data Pragmatists (53%)**: Those who are concerned about online privacy but will make tradeoffs on a case-by-case basis as to whether the service or enhancement of service offered is worth the information requested
- **Data Unconcerned (29%)**: Those who are unconcerned about online privacy in general and characterized by lower levels of concern about the sharing of personal data
- **Data Fundamentalists (18%)**: Those who are concerned about online privacy and are unwilling to provide personal information even in return for service enhancement."

Their findings for individual countries:

"Looking across all global markets in 2022, it is interesting to note that the pragmatist mindset is the most prevalent across almost all markets, with the unconcerned segment being the second largest and the fundamentalist third. This pattern is consistent across all markets other than France, where the unconcerned segment is the largest at 38%; slightly ahead of the pragmatist segment at 36%.

However, the level of dominance of the pragmatist mindset does vary considerably across global markets. For example, in China and India, over 3 in 4 consumers fall within the pragmatist mindset. Across the majority of other markets, the pragmatist segment falls below half, at the expense of the unconcerned who make up a more significant part of society. Indeed, in markets such as Belgium, Germany, Japan and the Netherlands the proportion of the unconcerned rises above 1 in 3 (not far behind the proportion of the pragmatists in these markets)."



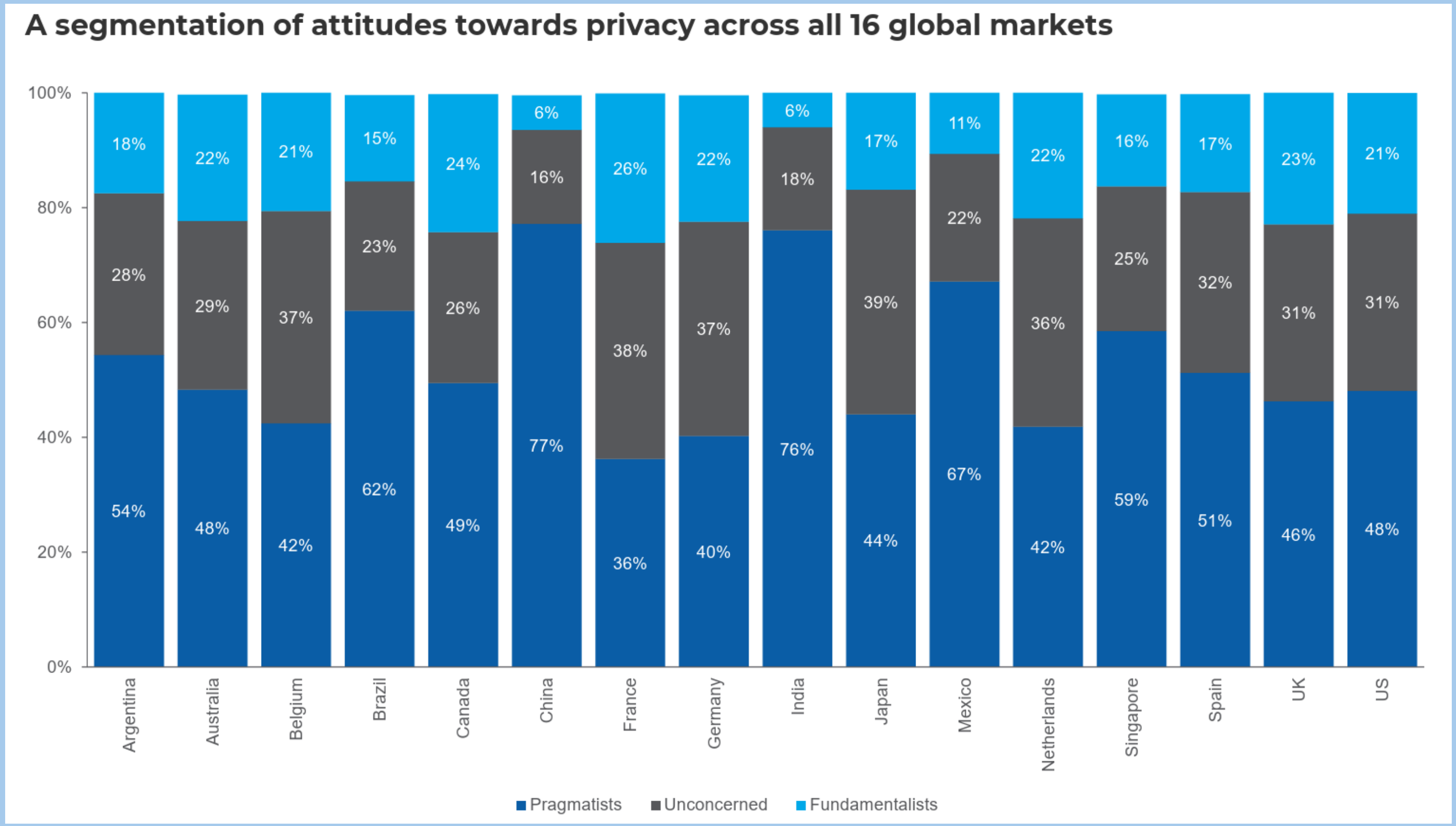
Source: Global Data & Marketing Alliance (GDMA) Global Data Privacy: The Consumer Perspective 2022 report

Continued next page

Global Data & Marketing Alliance’s Privacy Segments (cont.)

“It should be noted that the fundamentalist mindset remains as a relatively high proportion of society across a range of markets, with over 1 in 5 falling within this segment in Australia, Belgium, Canada, France, Germany, the Netherlands, the UK and the USA.”

Source: Global Data & Marketing Alliance (GDMA) Global Data Privacy: The Consumer Perspective 2022 report


A segmentation of attitudes towards privacy across all 16 global markets

Source: Global Data & Marketing Alliance (GDMA) Global Data Privacy: The Consumer Perspective 2022 report

Continued next page

Why Do Privacy Laws Fall Short?

Regulations struggle to keep up with technology, enforcement is inconsistent, and companies find legal loopholes. Privacy policies are often intentionally dense and misleading, relying on user "consent" that is more about compliance than meaningful choice. As one privacy policy lawyer put it, “Technology waits for no one. Privacy advocates are always playing catch-up.”

Public pressure matters, but it must be sustained. Scandals like Cambridge Analytica sparked new privacy laws and pushed users toward more secure platforms, but momentum fades quickly. Without continued advocacy, corporations and governments return to their old habits.

Detailed Findings

How AI Will Impact Digital Privacy

Artificial intelligence is transforming privacy challenges at an unprecedented scale. AI doesn't just collect data—it infers, predicts, and reconstructs personal information in ways users never explicitly consented to. Nearly every expert in this study agreed: AI will make protecting privacy significantly harder.

AI-Driven Profiling

AI analyzes browsing habits, purchases, social media activity, and even typing speed to build detailed behavioral profiles. These insights power hyper-targeted advertising, political manipulation, and even predictive policing. As one expert described, AI doesn’t just track what you do. It predicts what you’re going to do next—and that’s often more invasive than direct data collection.

One of AI’s greatest privacy risks is its ability to deduce personal details users never explicitly shared. As a professor and AI/privacy researcher warned, “AI can figure out things about you that even you don’t consciously know yet.”

- **Health status** – AI can predict pregnancy, mental health conditions, or financial distress from spending patterns and search history.
- **Political affiliation** – A study conducted by a computer science professor found that AI could determine users’ political leanings based solely on the images they engaged with on Twitter—without analyzing text.
- **Social credit systems** – AI-powered scoring models, like those used in China, evaluate individuals based on online and offline behaviors, affecting access to jobs, loans, or travel.

Continued next page

Facial Recognition and Biometric Risks

AI-driven facial recognition, iris scans, and voiceprints are being collected without consent. Unlike passwords, biometric data is permanent—if compromised, it cannot be reset. One expert raised a critical question: “A world where every person is automatically recognized wherever they go—do we really want that?”

AI in Law Enforcement

Governments worldwide are deploying AI for predictive policing, automated fraud detection, and mass surveillance. These experts agreed that once AI-powered surveillance is deployed, rolling it back becomes nearly impossible. Governments will always justify keeping it.

Can AI Be Privacy-Preserving?

Some experts argue that AI could be designed to protect privacy rather than erode it:

- **Federated Learning** – AI models train on user devices rather than collecting raw data.
- **Differential Privacy** – Algorithms introduce noise to data to prevent individual identification.
- **Transparency & User Control** – Companies should disclose how AI makes decisions and allow individuals to inspect or delete AI-generated profiles.

More than one expert asserted that privacy-preserving AI is possible—but only if regulators and the public demand it. Without oversight, AI will be used to maximize surveillance, not privacy.

Detailed Findings

Best Practices for Achieving Digital Privacy

Strong security practices and privacy-enhancing technologies are essential, but true privacy protection requires a fundamental shift in how businesses, policymakers, and individuals approach data. But there are many forces working against digital privacy, not least of which is what many of these experts call “surveillance capitalism.” A privacy researcher and medical faculty member said, “We will never have privacy as long as it’s a trade-off against convenience.”

Privacy by Design

Experts overwhelmingly emphasized Privacy by Design—embedding privacy into systems from the start rather than adding it as an afterthought. This includes:

- **Data Minimization** – Collecting only what is necessary and deleting data when it’s no longer needed.

Continued next page

- **Transparency and User Control** – Clear, accessible privacy settings, not buried in fine print.
- **Encryption and Security** – Strong encryption and strict access controls to protect personal data.

One expert asserted that “We shouldn’t be asking, ‘Are we compliant?’ We should be asking, ‘Are we respecting user privacy in a meaningful way?’”

How Users Can Protect Themselves

While privacy shouldn’t fall entirely on individuals, these experts also advocated for increased consumer education and information. They said users can take steps to reduce their exposure:

- **Use privacy-focused tools** – Encrypted messaging apps, VPNs, and browsers that block tracking.
- **Practice good information hygiene** – Be mindful of what data is shared and with whom.
- **Opt for services that respect privacy** – Companies that prioritize privacy-first design are gaining traction.

But many experts warned that placing too much responsibility on individuals is unfair. Most people lack the time or technical knowledge to fully protect themselves—and they shouldn’t have to. These experts all agree that the real solution is stronger systemic protections.

The Role of Policymakers

Regulations like GDPR and CCPA set important foundations, but all of the experts interviewed argued that privacy laws must focus on the spirit of the law, not just the letter. Many companies treat compliance as a box-ticking exercise, doing the minimum required rather than genuinely improving privacy protections. Several experts agreed that privacy should be seen as part of human dignity, not just a legal requirement.

The Future of Digital Privacy

Experts were divided on where privacy is headed:

- **The Optimistic View** – Stronger privacy laws, greater consumer awareness, and privacy-enhancing technologies (e.g., federated learning, differential privacy) could shift the balance in favor of users.
- **The Pessimistic View** – AI-driven surveillance, biometric data collection, consumer apathy, and/or ignorance and corporate resistance to regulation could erode privacy even further.

Privacy protection is at a crossroads. Businesses, policymakers, and individuals must move beyond compliance toward meaningful privacy protections. Whether privacy improves or continues to decline depends on how seriously regulators, companies, and the public treat it in the coming years.

Continued next page

A Final Word

Is Privacy Just About Data?

Most privacy discussions focus on data protection—who collects personal data, how it's used, and whether it's secure. But many of the experts we interviewed argued that privacy is **more than just information stored in ones and zeros**—it's a **fundamental issue of human rights, ethics, and autonomy.**

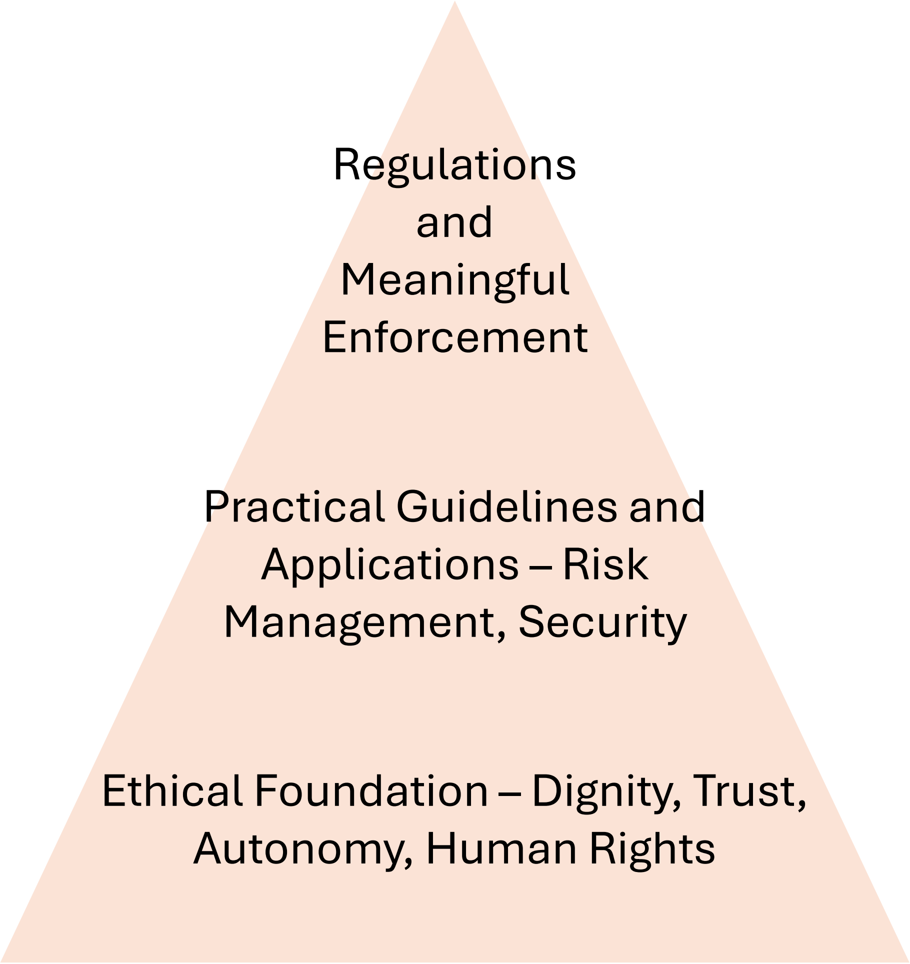
One digital privacy expert challenged the idea that privacy can be reduced to just "information privacy": "When you talk about privacy and having multiple dimensions of privacy, that's what they're talking about. They're talking about that much broader suite of rights, not just information privacy. And information privacy is the thing that governments have been concerned about legislating."

This perspective raises a difficult question: **If privacy is more than just data protection, how do we regulate it?**

He cautions that **broad ethical frameworks alone** aren't enough: "You can say dignity, but how do you regulate dignity? You've got to do better than that. It's like AI ethics—people talk about it as a regulatory solution, but what ethics are they? Deontological? Consequentialist? Feminist ethics? Are they the ethics chosen by some bunch of invariably white blokes in Palo Alto sitting in a basement with gravy stains on their T-shirts?"

The challenge, then, is to **bridge the gap between abstract concepts like dignity, trust, and autonomy, and real-world privacy regulations**. A privacy framework that only protects digital information may be too narrow, but one based only on philosophical principles may be too vague to enforce.

This debate highlights the ongoing struggle in privacy policy: **How do we move beyond simply protecting data to safeguarding privacy as a lived experience?**

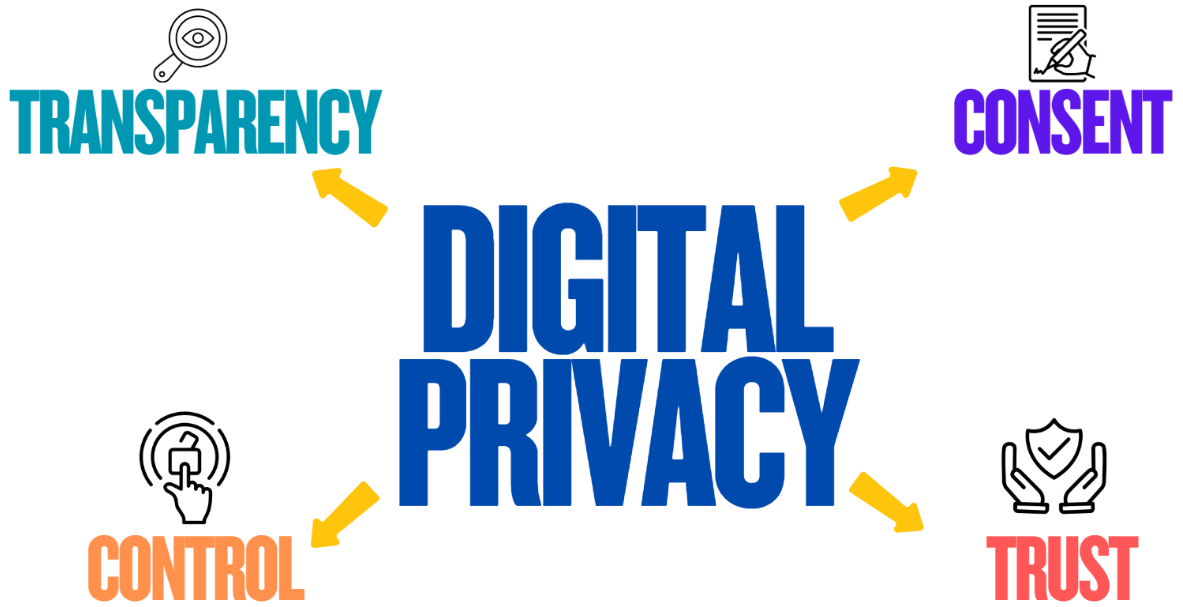

Regulations and Meaningful Enforcement
Practical Guidelines and Applications – Risk Management, Security
Ethical Foundation – Dignity, Trust, Autonomy, Human Rights

Detailed Findings

Detailed Findings:
What is Digital Privacy?

What is Digital Privacy?

When asked to define digital privacy, the experts interviewed provided a range of perspectives, reflecting their education and work in law, engineering, policy, and cybersecurity. While their wording varied, several key themes emerged, including control, transparency, consent, and trust.



Privacy as Control Over Personal Data

Many of the experts we talked to emphasized control—who has access to personal data and how it is used.

- *Digital privacy is the ability to control one's data and decide who has access to it.*
- *Privacy is about maintaining control, not just about keeping things secret.*
- *Digital privacy includes the right to be forgotten—the ability to remove personal data when desired.*

This idea of control extends beyond just who can see the data—it also includes the right to modify, delete, or manage one's digital presence.

Privacy Requires Transparency

Several experts pointed out that privacy protections don't mean much if people don't understand what's happening with their data. They emphasized that transparency is essential—people should be able to see what data is being collected, why, and how it will be used.

- *Privacy is about transparency—people should know what data is collected and how it's used.*
- *People trade privacy for convenience all the time, usually without realizing it. We need more visibility into what we're actually giving up.*

A common concern among experts was that privacy agreements and consent forms are deliberately vague and complex, making it difficult for users to make informed decisions.

Continued next page

What is Digital Privacy? (cont.)

Privacy as Consent and Autonomy

Another major theme during the course of the interviews was consent—the idea that individuals should have a real choice about how their data is shared. These experts argued that true privacy means being able to opt out of tracking, data collection, and algorithmic profiling.

- *The right to autonomy over digital identity and the ability to opt out of tracking.*
- *A matter of consent—people should never be forced to share personal data without explicit approval.*
- *A legal and ethical obligation for companies and governments to protect individual data.*

However, many interview participants noted that informed consent, as practiced today, is often an illusion—people feel forced to accept invasive privacy policies just to access everyday services.

Privacy and Trust

Several experts emphasized that digital privacy is ultimately about trust—trust in companies, governments, and digital platforms—but also trust that all of these will do what they say they will do.

- *Privacy is about trust—people need to trust that their data is safe and used ethically.*

Many interviewees warned that trust in privacy protections is being eroded by high-profile data breaches, hidden tracking, and government surveillance.

What These Definitions Have in Common

Despite differences in wording, nearly all participants agreed that digital privacy is not just about secrecy—it’s about control, transparency, and informed choices.

- **Control**—People want to decide what happens to their personal data.
- **Transparency**—Users should know how their data is collected and used.
- **Consent**—No one should be forced into data-sharing without real options.
- **Trust**—Without confidence in institutions, companies, and laws, privacy protections are meaningless.

Detailed Findings: Frameworks for Thinking About Privacy

Frameworks for Thinking About Privacy

How these experts think about digital privacy is deeply influenced by their professional education, industries, experience, and roles. While lawyers focus on compliance and regulations, healthcare professionals emphasize duty of care, and technologists often approach privacy through the lens of trust and human rights.

There is no single "correct" way to think about privacy. Instead, privacy is a multifaceted concept that intersects with ethics, law, security, and societal expectations.

Through these interviews, seven dominant frameworks emerged:

- Regulatory compliance
- Duty of care
- Human dignity
- Trust
- Human rights
- Risk management
- Corporate vs. consumer views

Privacy as Regulatory Compliance

Lawyers, policymakers, and regulatory experts primarily think and talk about privacy as it relates to legal compliance—ensuring that organizations follow existing laws and avoid liability. Privacy laws like GDPR (Europe), CCPA (California), HIPAA (U.S. healthcare), and China's PIPL provide structured guidelines that organizations must follow.

- *Privacy needs clear accountability. Without strong legal frameworks, it's just a vague ethical idea.*
- *Compliance is the minimum. But without enforcement, regulations are just paper laws.*

This approach frames privacy as a legal obligation—something that must be followed but is subject to interpretation and enforcement gaps.

Continued next page

Frameworks for Thinking About Privacy (cont.)

Privacy as a Duty of Care

For healthcare professionals, medical researchers, and certain corporate leaders, privacy is framed as a moral obligation to prevent harm. This “duty of care” perspective focuses on protecting individuals from privacy breaches that could impact their safety, well-being, or rights. Privacy in healthcare is not just about compliance; it's about protecting patients from harm. A breach isn’t just a legal issue—it can be life-altering.

This perspective acknowledges that privacy breaches in certain fields—like healthcare or finance—have more severe consequences than in others.

Privacy as Human Dignity

Some experts argued that privacy should not be seen as just a legal requirement or security feature, but as an intrinsic part of human dignity and autonomy. This approach is aligned with ethics, philosophy, and digital rights advocacy. These experts asserted:

- *The ability to control your digital identity is as important as controlling your real-world identity. Privacy is about dignity.*
- *Surveillance isn’t just a security issue—it’s a human dignity issue. People deserve to exist without being constantly watched.*

This framework sees privacy as an enabler of personal freedom, rather than just a matter of compliance or harm reduction.

Privacy as Trust

Some technologists and engineers approach privacy through the lens of trust—they see privacy as a way to maintain confidence in digital systems, technology platforms, and institutions.

- *Privacy is fundamentally about trust—people need to believe that their data is handled responsibly.*
- *When privacy is broken, trust collapses. And when trust collapses, people disengage from digital systems altogether.*

From this perspective, privacy is not just about secrecy or control—it’s about creating a relationship of trust between individuals and organizations.

Continued next page

Frameworks for Thinking About Privacy (cont.)

Privacy as a Human Rights

For privacy advocates and international legal scholars, privacy is viewed as a fundamental human right, rather than just a matter of corporate policy or national law. This perspective is strongly shaped by history, particularly the harms caused by surveillance, tracking, and data misuse in the 20th century.

- *Privacy is not a privilege—it's a fundamental right that must be protected, like freedom of speech.*
- *Privacy is essential to protecting other freedoms, like freedom from discrimination or political repression.*

Much of Europe's modern privacy philosophy is influenced by the atrocities of World War II, when data collection was weaponized against marginalized populations. During Nazi occupation, census data, religious records, and personal registries were used to identify and target individuals. The lesson was clear: when governments have unchecked access to personal data, that data can be used for oppression.

These historical experiences helped shape the strong privacy protections in Europe today, most notably the General Data Protection Regulation (GDPR), which treats privacy as an inalienable right. This contrasts with other parts of the world, such as the United States, where privacy is often framed as a consumer protection issue rather than a fundamental right.

Privacy as Risk Management

Several experts framed privacy as a risk management challenge, distinct from compliance, trust, or human rights perspectives. This approach, common among cybersecurity professionals, engineers, and policymakers, emphasizes assessing and mitigating risks rather than adhering to rigid legal frameworks.

Risk-based privacy management starts with the recognition that not all privacy threats are equal. Some violations may result in minor inconveniences, while others can lead to identity theft, reputational harm, or even state surveillance. Organizations using this model assess threats based on likelihood and severity, applying safeguards accordingly.

Privacy isn't just about following rules—it's about assessing the risks, minimizing exposure, and preventing harm before it happens.

Unlike compliance-driven models, which focus on legal obligations, risk management frameworks prioritize understanding vulnerabilities and consequences in a systematic way. This means treating privacy like any other major business risk, including cybersecurity threats, operational failures, and financial liabilities. Organizations need to think of privacy breaches like financial risks—you calculate likelihood and severity, then put controls in place to reduce exposure.

Continued next page

Frameworks for Thinking About Privacy (cont.)

A major focus of risk-based privacy management is proactive harm reduction. Instead of responding after a privacy violation occurs, this approach encourages organizations to identify vulnerabilities in advance and implement preventative measures. One of the most effective methods is data minimization—storing and collecting only the personal data that is strictly necessary. Some industries, particularly healthcare, already operate within a risk-based privacy framework. In medical settings, privacy breaches can have life-altering consequences, making risk mitigation strategies essential. As one expert noted, privacy risks are assessed differently in medical settings. A data breach isn't just an inconvenience—it can cost lives.

Emerging technologies like AI-driven profiling introduce new, harder-to-predict privacy risks. AI can infer sensitive personal traits—such as political beliefs or sexual orientation—without individuals explicitly disclosing them. This creates privacy exposures that individuals don't even realize exist. With AI, privacy risk isn't just about the data you give—it's about what AI can infer from the data you don't even know you're sharing.

Many experts also highlighted the gap between corporate privacy strategies and consumer expectations. While individuals often assume their data is being protected, organizations tend to treat privacy as a legal requirement rather than a real-world risk factor affecting users. Several of the lawyers interviewed said they routinely encounter clients who treat privacy policies and protections as an add-on after product development, rather than embracing privacy-by-design. But, they say, privacy isn't just about avoiding lawsuits—it's about avoiding harm. The best companies understand that before regulators force them to.

Adopting a risk-based privacy model offers a structured way to evaluate and mitigate threats across different industries. Instead of treating privacy as a legal formality, companies that take this approach prioritize protections based on real-world risk exposure.

Corporate vs. Consumer Views on Privacy: Where Perspectives Diverge

The tension between corporate and consumer perspectives on privacy was a recurring theme across several interviews. While individuals often assume they have more privacy protections than they do, corporations tend to view privacy as a compliance issue rather than a fundamental right.

Many interviewees noted that consumers expect their data to be protected but rarely read or understand the fine print in privacy policies. They believe they have more privacy rights than they actually do. They assume companies are required to protect their data in ways that aren't legally mandated. What's more, most people assume that companies aren't allowed to track them across different services—but they are, unless laws explicitly prohibit it.

Continued next page

Detailed Findings: Expectations of Privacy

Rights of access, notice, correction and deletion seem to be pretty ubiquitously shared across different global regions and data privacy. – Digital Privacy Expert

When we talk about individual expectations of privacy, we shouldn't actually think about a lay person. We should think about the individual expectations of an informed person, because a lay person probably has very low expectations. But that doesn't mean it's right. An informed person may have a different set of expectations that would better safeguard an individual's personal rights, just because they have a better understanding of what's at stake. – Privacy Policy Lawyer

Expectations of Privacy

Across cultures and industries, individuals have strong yet inconsistent expectations about privacy—but those expectations do not always align with reality. While many assume their data is being handled responsibly, securely, and ethically, the truth is often more complicated. The information asymmetry, power imbalance, and contextual nature of privacy make it difficult for individuals to make informed choices about their personal data.

Privacy Expectations: What People Assume

Most people expect that their data will be handled appropriately—that companies and governments will act in good faith and follow ethical data practices. There is an assumption that organizations will do what they say they will do, particularly when they claim to protect user privacy. However, the reality is that privacy is often a legal checkbox rather than a genuine commitment.

As one expert said, “Consumers believe they have more privacy rights than they actually do. They assume companies are required to protect their data in ways that aren’t legally mandated."

These experts said that there is also no collective understanding of privacy issues. Privacy means different things to different people, and individuals often apply their own reasoning—whether it’s shaped by personal experiences, culture, or a general misunderstanding of how digital systems work. Some expect too much protection, believing their privacy is fully safeguarded by existing laws. Others expect too little, assuming that privacy is already dead.

Continued next page

Expectations of Privacy (cont.)

The Information and Power Asymmetry

A major issue identified in the interviews is the huge gap between what individuals know about digital privacy and what corporations know.

Few people have enough information to make truly informed decisions about their data. Privacy policies are often dense, vague, and unclear, making it nearly impossible for consumers to assess their risks. Worse, there is a time asymmetry—people interact with dozens or even hundreds of companies. Reading every privacy policy would take an unrealistic amount of time.

One interviewee referenced a study showing that the time required to read all the GDPR-mandated cookie consent notices would total hours of lost productivity per year per user.

Beyond just information, there is also a fundamental power imbalance in privacy decisions. Individuals cannot simply "opt out" of data collection if they want to use an app, a service, or participate in the digital economy. While some privacy settings exist, they are often buried deep within user preferences, difficult to navigate, or designed to discourage users from changing defaults.

Context Matters: Privacy is More Than Security

A recurring theme from experts was that privacy expectations are highly contextual—privacy is not a fixed concept but rather something that changes based on the situation, the type of data, and the environment in which it is shared.

For example, individuals tend to be far more concerned about privacy in healthcare settings, where the sensitivity of medical records is paramount, than they are on social media, where they willingly share personal information. Yet even in seemingly low-stakes environments, privacy risks can be substantial, particularly when data is aggregated, analyzed, and used in unexpected ways.

This presents a challenge for any privacy framework—protections must account for these nuances, recognizing that not all data is equally sensitive, and not all settings are equally private.

Continued next page

Expectations of Privacy (cont.)

Common Misconceptions About Privacy

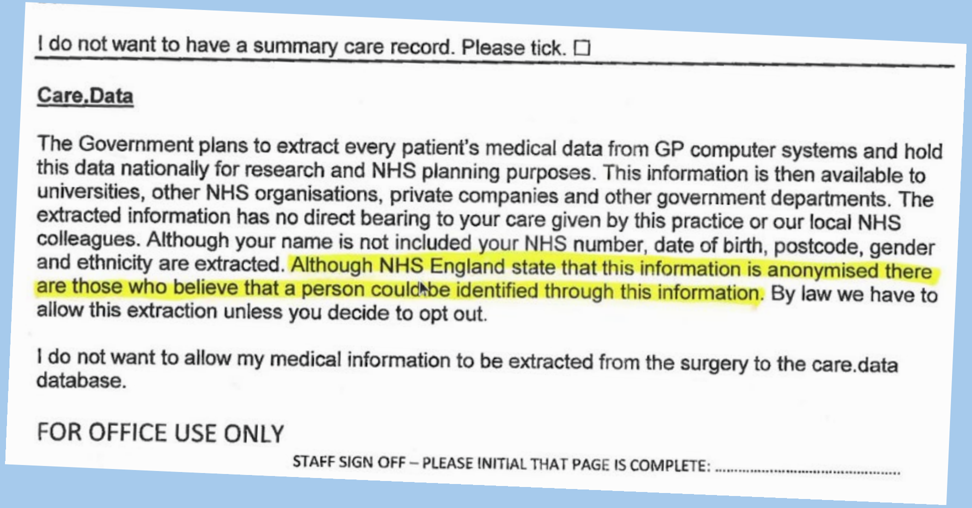
During the course of the interviews, participants identified many commonly-held misconceptions about privacy that impact behaviors and resulting risks:

1. **The "Nothing to Hide" Fallacy** - Many people dismiss privacy concerns by insisting they have nothing to hide. This oversimplifies the issue, ignoring how personal data can be used for profiling, discrimination, and manipulation. Privacy is not just about keeping secrets—it's about maintaining control. The problem is, most people don't even realize how little control they actually have.
2. **Misplaced Trust in Online Identities** - Users often assume that digital personas are authentic, failing to recognize that accounts can be fake, manipulated, or used deceptively. This naivety enables scams, social engineering, and AI-generated misinformation to flourish.
3. **The "Consent Illusion“** - Many believe that clicking "I Agree" on privacy policies or cookie notifications gives them meaningful control over their data. However, as one expert pointed out, privacy policies are designed to protect companies, not individuals, and users rarely read or understand them.
4. **The Anonymization Myth** - People trust that "anonymized" data is safe, but most anonymization techniques can be reversed. These experts insist that with enough data points, re-identification is almost always possible.
5. **False Understanding of Data Sharing** - Many assume private messages are truly private, that deleting a post erases it forever, or that turning off location services stops all tracking. In reality, data persists, propagates, and is repurposed in ways users don't anticipate.
6. **The Power of Data Inference** - People underestimate how small pieces of seemingly innocent data can be combined to reveal highly personal insights.
7. **Applying Physical World Concepts to Digital Spaces** - Many people assume digital privacy works like physical privacy—that browsing an online store is like visiting a physical one. In reality, digital environments track behavior at an unprecedented scale, aggregating data in ways that have no real-world equivalent.

Continued next page

When Privacy Language Backfires: The NHS Data Disclosure Controversy

Privacy policies are supposed to build trust and transparency, but sometimes they do the exact opposite. A case in point: the NHS care.data program in the UK, where poorly worded privacy disclosures sparked widespread concern and public backlash.



I do not want to have a summary care record. Please tick. □

Care.Data

The Government plans to extract every patient's medical data from GP computer systems and hold this data nationally for research and NHS planning purposes. This information is then available to universities, other NHS organisations, private companies and other government departments. The extracted information has no direct bearing to your care given by this practice or our local NHS colleagues. Although your name is not included your NHS number, date of birth, postcode, gender and ethnicity are extracted. Although NHS England state that this information is anonymised there are those who believe that a person could be identified through this information. By law we have to allow this extraction unless you decide to opt out.

I do not want to allow my medical information to be extracted from the surgery to the care.data database.

FOR OFFICE USE ONLY

STAFF SIGN OFF – PLEASE INITIAL THAT PAGE IS COMPLETE: ....

At the heart of the issue was the way the NHS described the handling of patient data. In official documents, the NHS reassured patients that their information would be anonymized—but then immediately cast doubt on that very statement. One form explicitly stated:

"Although NHS England state that this information is anonymised, there are those who believe that a person could be identified through this information."

This contradictory phrasing raised more questions than it answered:

- If the data is anonymized, why acknowledge that people might still be identified?
- Who are "those who believe" this? Experts? Skeptics? The NHS itself?
- What risks does this actually present to patients?

Instead of reassuring the public, this hedging language triggered distrust. Patients feared that their supposedly anonymous health records might not be so private after all. Combined with unclear opt-out procedures and a lack of public engagement, this wording contributed to the eventual collapse of the care.data initiative in 2016.

Lesson: Transparency Requires Clarity. It is a foundation of trust.

As a surgeon and medical privacy researcher explained, “If you confuse people about privacy, they assume the worst."

The NHS care.data controversy illustrates a fundamental rule of privacy communication: If a statement about data protection raises more doubts than it resolves, it’s a failure.

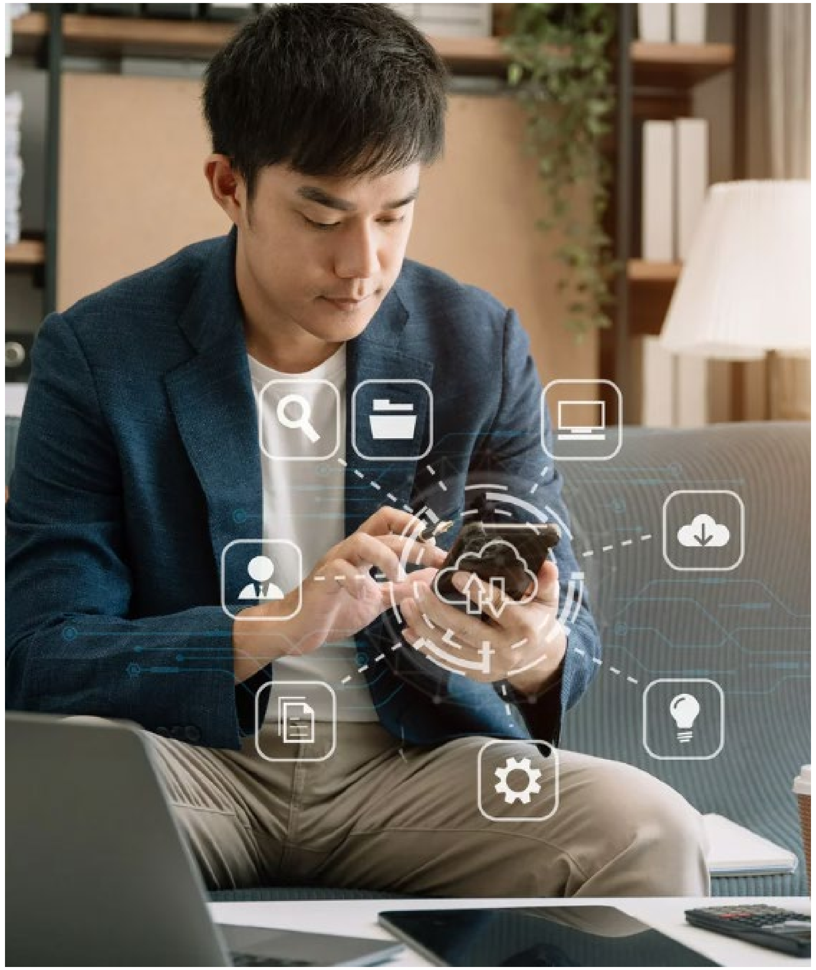
Detailed Findings: Sensitivity of Information and What People Consider Most and Least Private

"In the end, people act in ways they perceive to be safe." – Professor of Engineering

Sensitivity of Information

Some types of data are almost universally recognized as highly sensitive, while others are perceived as lower risk or even public by default. However, as multiple experts pointed out, privacy sensitivity is contextual—what feels private in one setting may be openly shared in another. And sometimes it's hard to even put into words when someone is concerned about their privacy, what one expert called the "creepy factor." If it feels creepy, your privacy is at risk.

These experts explained that privacy is not one-size-fits-all. People react more strongly to certain types of data collection, but even those reactions depend on the situation.



What People Consider Most Sensitive

Certain categories of personal data consistently rank as the most sensitive due to their potential to cause harm if exposed. Experts noted that individuals tend to be most concerned about information that:

- Makes them vulnerable (e.g., financial fraud, identity theft)
- Exposes deeply personal aspects of their lives (e.g., medical records, political beliefs)
- Could be used to manipulate or exploit them (e.g., behavioral tracking, deepfakes)

Financial Information

Nearly all participants agreed that financial data—bank details, credit card numbers, transaction history, and account credentials—remains one of the most highly sensitive categories.

A regulatory authority said, "Financial data is a major target for criminals. People worry about identity theft more than almost any other privacy risk."

However, experts noted that many individuals don't think about the long-term privacy risks of financial transactions, such as how purchasing behavior is tracked and monetized.

Continued next page

Sensitivity of Information (cont.)

Health Data

Medical records, prescriptions, mental health information, and anything related to an individual's physical or psychological well-being rank as extremely private.

Some interviewees highlighted growing concerns about genetic data—with the increasing popularity of consumer DNA testing services, individuals are voluntarily sharing deeply personal information without fully understanding the privacy implications.

Biometric Data

Facial recognition, fingerprints, voice recognition, and iris scans are seen as particularly sensitive due to their permanent nature—they cannot be changed like a password. Once biometric data is compromised, it’s compromised forever. Most people don’t think about that risk when using Face ID or fingerprint scanners.

Location and Behavioral Data

Real-time location tracking, movement patterns, and behavioral profiling often trigger privacy concerns, particularly when people realize they are being monitored without explicit consent.

Several experts pointed to a growing awareness that location tracking is not just about navigation—it fuels targeted advertising, law enforcement surveillance, and even political profiling.

Information about Children

Parents, grandparents, and guardians are increasingly aware of and sensitive to exposing any information about children online, including full names, birthdays and photographs. This is driven not only by fear of exploitation but also of identity theft.

Continued next page

Sensitivity of Information (cont.)

Personal Identity and Reputation

Information related to political affiliation, gender, religious beliefs, and online reputation is also considered highly sensitive.

- **Political Data** - Many interviewees noted that individuals often underestimate the privacy risks of political engagement—such as sharing opinions on social media or signing petitions.
- **Gender and Sexual Orientation** - In some regions, outing someone through digital data can put them at risk of harm or discrimination.
- **Deepfake and Image Manipulation Risks** - The rise of AI-generated images and deepfake videos has led to new privacy concerns about digital identity theft. The misuse of deepfake technology is not just about misinformation—it's about people losing control over their own likeness.

What People Consider Less Sensitive

While highly personal, financial, and biometric data trigger strong privacy concerns, some categories of information are perceived as less sensitive or even public.

Aggregated or De-Identified Data

Many interviewees noted that people are less concerned about data that is stripped of personally identifiable information (PII). However, experts warned that de-identified data is not always as anonymous as people assume—re-identification attacks have proven that large datasets can still reveal individuals. More than one expert explained that people assume anonymized data is safe, but AI models can often reconstruct identities with frightening accuracy.

Publicly Available Information

Users generally assume that information they post publicly—such as social media activity—is not particularly sensitive. However, multiple experts pointed out that even public data can become sensitive when aggregated, analyzed, and combined with other datasets, which can allow for re-identification.

Continued next page

Detailed Findings: Factors Influencing Expectations of Privacy

Factors Influencing Expectations of Privacy

What people expect when it comes to privacy is shaped by personal experiences, cultural norms, education levels, and trust in institutions. Some assume their data is safe by default, while others see privacy as a constant battle. Across interviews, experts described a range of influences that determine how individuals approach digital privacy, highlighting why expectations differ so dramatically from one person to another.

Privacy Becomes Real When It's Personal

For many people, privacy is an abstract concern—until something goes wrong. Several experts pointed out that firsthand experiences, such as identity theft, financial fraud, or a data breach, often serve as a wake-up call. Before that moment, privacy risks feel distant and hypothetical.

A cryptography and privacy researcher emphasized the role of social influence in this process. If someone in your circle experiences a privacy breach, it raises awareness for those around them. "People learn from others," she explained. "If your friends or family start taking privacy seriously, you're more likely to do the same."

Education and Digital Literacy: Knowing the Risks, Understanding the Trade-Offs

The more people understand technology, the more skeptical they become about how their data is collected and used. However, many users simply do not have the technical knowledge to fully grasp the extent of modern digital tracking.

A privacy lawyer and AI/human rights expert pointed out that many people wrongly assume that privacy laws automatically protect them. She described a common pattern where individuals assume that companies must be required to keep their data safe—but in reality, privacy protections vary widely depending on jurisdiction and enforcement. This gap between perceived and actual protections leads many to take fewer precautions than they should.

For those who do understand the risks, behavior shifts dramatically. People who actively follow privacy news, for example, are more likely to use encrypted messaging apps, VPNs, and privacy-focused browsers. But as one expert cautioned, even among well-informed individuals, misconceptions persist. Some believe that using incognito mode hides their activity from employers or internet service providers. Others assume that switching to an encrypted email provider automatically makes all messages secure—even if the recipient isn't using the same service.

Even seasoned professionals sometimes conflate security with privacy, overlooking how secure systems can still harvest and exploit personal data. But as one expert argued, we shouldn't expect people to have high levels of digital privacy literacy. "We don't expect individuals to understand how their car works. It's not fair to expect individuals to understand about privacy and be self-governing."

Continued next page

Factors Influencing Expectations of Privacy (cont.)

Cultural and Regional Differences: Privacy Is Not Universal

Privacy expectations vary dramatically by region, often shaped by historical and political factors. European countries, for example, tend to view privacy as a fundamental human right, a perspective deeply influenced by historical experiences with authoritarian surveillance. A privacy researcher and medical faculty member in Germany noted that privacy in Europe is tied to past abuses, including surveillance by the Stasi in East Germany. “The expectation here,” he said, “is that individuals should have strong rights over their personal data. The GDPR is a reflection of that history.”

In contrast, privacy in the United States is often framed as a consumer right rather than a human right. This difference results in a fragmented legal landscape, with privacy protections dependent on industry-specific laws rather than a unified framework. The result, as several experts pointed out, is that American consumers expect to trade privacy for convenience far more than their European counterparts.

Some countries prioritize state security over individual privacy. In China, for example, privacy concerns are secondary to government surveillance efforts. Citizens understand that state monitoring is widespread, and their expectations reflect that reality. In Papua New Guinea, efforts to implement a national digital identity system ran into challenges because Western-style privacy models did not align with local governance structures.

These cultural differences underscore the fact that privacy expectations are not universal, and any global privacy framework—must be adaptable to different regional realities.

Generational Shifts: Privacy Is Being Redefined

One of the most notable trends in the interviews was how younger and older generations think differently about privacy.

Older generations (50+) tend to define privacy as not sharing information at all. They are particularly concerned about identity theft and financial fraud but often struggle with digital security measures, such as managing multiple passwords or setting up two-factor authentication.

Younger generations, by contrast, see privacy as controlling what they share and with whom. Teenagers, in particular, demonstrate a sophisticated understanding of privacy within social networks, creating “finstas” (fake Instagram accounts) for close friends while maintaining a polished, public-facing profile elsewhere. Despite sharing more online, younger users expect greater control over their data—and are often frustrated by companies that don’t provide it.

These generational differences suggest that privacy frameworks need to evolve to reflect how different age groups define privacy and what control they expect over their information.

Continued next page

Factors Influencing Expectations of Privacy (cont.)

Trust in Institutions: The Role of Governments and Corporations

How much people trust governments, corporations, and regulators plays a huge role in their privacy expectations. A digital identity specialist explained that in countries where governments are trusted, people are generally more willing to share data. In contrast, in societies with high levels of corruption or state surveillance, people assume that any data sharing is a risk.

Technology companies face a similar trust divide. After the Facebook–Cambridge Analytica scandal, public trust in big tech companies plummeted, leading many to rethink how they share data online. Several experts noted that people often say they distrust corporations but continue using their services anyway—a behavior known as the privacy paradox.

While some individuals respond to distrust by adopting privacy-protective tools, others become resigned to a lack of privacy, assuming that their data is already out in the open and that nothing can be done.

Rebuilding Trust Through Transparency

If trust is lost, it is extremely difficult to restore. Several experts emphasized that transparency is the only path forward.

- **Clarity in Privacy Policies** – Vague or contradictory privacy statements (such as those found in the NHS care.data program) undermine trust instead of building it.
- **User Control and Consent** – Meaningful privacy protections should focus on empowering users, not just compliance checkboxes.
- **Consistent Enforcement** – People need to see that privacy laws have consequences for violators, otherwise, they won’t trust legal protections.

One privacy lawyer and AI/human rights expert explained, When people feel deceived about privacy, trust is gone. It doesn’t matter what the fine print says—it’s about how people perceive the system."

Privacy Around the World: Three Telling Examples

New Zealand's Māori Cultural Impact on Data Centers – One interview participant described how Māori cultural beliefs about personal images containing "mana" (spiritual power) influenced where major tech companies locate their data centers. The Māori view photos and personal data as extensions of the person, requiring special protection and local storage. This cultural perspective led companies like AWS to establish data centers in New Zealand rather than storing data overseas, demonstrating how indigenous values can shape modern privacy infrastructure.

The Bunnings Facial Recognition Controversy – One expert highlighted the stark differences in privacy enforcement through the example of Bunnings, a major retail chain. When the company implemented facial recognition in its stores, the same practice received dramatically different regulatory responses in Australia versus New Zealand. While Australian regulators fined the company for not explicitly asking customer consent, New Zealand's weaker privacy laws allowed the practice to continue unimpeded. This case shows how identical privacy issues can lead to vastly different outcomes depending on local regulations.

The European Cookie Paradox – A European expert highlighted the unintended consequences of Europe's strict privacy laws through the example of cookie consent notices. While intended to protect privacy, these notices have become so complex that users regularly encounter warnings about "878 third-party vendors" (or some equally absurd number) sharing their data. Instead of empowering users, this overwhelming transparency has led to what he calls "cookie consent fatigue," where people automatically click "accept" without understanding the implications.

Lesson

These examples reveal how privacy issues transcend simple legal compliance. Cultural values, trust relationships, and human behavior all play crucial roles in privacy protection. Successful privacy frameworks must consider these broader factors rather than focusing solely on technical or legal solutions.

The Privacy Paradox: Mistrust vs. Resignation

One of the most paradoxical aspects of digital privacy is that people often say they care deeply about privacy but continue to use services they don’t trust. This contradiction, known as the privacy paradox, is driven by several factors:

- **Lack of Alternatives** – Even when users don’t trust tech companies, they feel there is no viable way to opt out.
- **Resignation to Data Collection** – Some assume that privacy is already lost, leading them to stop trying to protect it.
- **Convenience Over Privacy** – Many individuals knowingly trade privacy for usability, preferring seamless digital experiences over complex security measures.

This paradox reveals a key issue: trust isn’t just about whether people believe in privacy protections—it’s about whether they feel empowered to act on them. If individuals don’t trust that they have meaningful control over their data, they either disengage from privacy protections or accept risk as unavoidable.

The Privacy Paradox in Action

In a well-known study from Carnegie Mellon University, researchers found that people say they value privacy, but their actions tell a different story.

The experiment offered shopping coupons in exchange for personal data. While participants could get a $10 discount without sharing any information, many opted for larger discounts by providing increasingly personal details. The findings revealed that when faced with an immediate benefit, people often deprioritize privacy concerns.

Lesson

Privacy decisions are often emotional, not rational. Even those who claim to care deeply about privacy may trade it away when incentives are high enough.

Continued next page

Detailed Findings: Contributors and Roadblocks to Digital Privacy

"Public pressure works. Companies don't change their privacy practices because they want to—they change when consumers demand it or when regulators force them to." – Privacy Lawyer & AI/Human Rights Expert

Contributors and Roadblocks to Digital Privacy

The state of digital privacy is shaped by a constant push and pull between those working to protect privacy and those who erode it for profit, power, or convenience. Privacy does not exist in a vacuum—it is the result of legal frameworks, technological innovations, corporate strategies, and individual behaviors.

Experts interviewed for this study identified key contributors to improving digital privacy as well as significant roadblocks that continue to undermine it.

Key Contributors to Digital Privacy

Privacy is safeguarded by a combination of laws, advocacy, technology, and public action. These contributors work toward greater transparency, better security, and stronger individual rights over personal data.

- **Privacy-Focused Regulations** – Laws like GDPR (Europe), CCPA (California), and PIPL (China) create legal frameworks that force companies to implement privacy protections.
- **Regulators and Enforcement Bodies** – Agencies such as the European Data Protection Board (EDPB), U.S. Federal Trade Commission (FTC), and national privacy commissions oversee compliance and issue fines for violations.
- **Advocacy and Watchdog Groups** – Organizations like Electronic Frontier Foundation (EFF) and Privacy International raise awareness, litigate privacy cases, and hold corporations accountable.
- **Privacy-Conscious Companies** – A growing number of companies (e.g., DuckDuckGo, ProtonMail, Signal) are building business models that prioritize user privacy over ad-driven surveillance.
- **Security and Privacy Engineers** – Cryptographers, security researchers, and software developers work on tools such as encryption, VPNs, and anonymization techniques to help individuals protect their data.
- **Public Awareness and Activism** – Individuals and grassroots movements push for greater privacy rights, demand better corporate policies, and challenge invasive government surveillance.

Despite these contributors, privacy remains a fragile right—constantly under pressure from technological advancements, market forces, and political interests.

Continued next page

Contributors and Roadblocks to Digital Privacy (cont.)

Key Roadblocks to Digital Privacy

Digital privacy is threatened by governments, corporations, hackers, and even social norms that devalue privacy. While some threats come from outright malicious actors, others arise from structural imbalances that make privacy difficult to maintain.

- **Surveillance-Oriented Governments** – Some governments use digital tools for mass surveillance, often in the name of national security, law enforcement, or public safety.
- **Profit-Driven Corporations** – The business model of many tech companies is based on collecting and monetizing personal data—what some experts call "Surveillance Capitalism."
- **Hackers and Cybercriminals** – Data breaches, identity theft, and cyberattacks expose personal information to malicious actors who exploit it for financial gain or political leverage.
- **Information and Time Asymmetry** – Companies have far more knowledge about data collection than individuals, and people interact with too many digital services to fully assess every privacy risk.
- **Lack of Consumer Choice** – Opting out of privacy-invasive services is nearly impossible—most people must use tools like email, cloud storage, and social media, even if they distrust them.
- **Public Indifference and Misinformation** – Many people do not fully understand how their data is collected and used. Some believe "If I have nothing to hide, I don't need privacy."
- **AI-Driven Surveillance and Tracking** – Artificial intelligence enables more sophisticated data profiling, behavioral tracking, and predictive analytics, often without user awareness.

Continued next page

Contributors and Roadblocks to Digital Privacy (cont.)

Why Privacy Laws Often Fail

Even in regions with strong privacy laws, enforcement lags behind corporate innovation. Many regulations:

- **Rely on users** to read complex privacy policies (which they rarely do).
- **Struggle to keep pace** with technological change, leaving gaps in protection.
- **Lack strong penalties** for violators, allowing companies to ignore privacy risks.

One expert compared privacy enforcement to seatbelt laws in the early days of automobiles—until public awareness grew and enforcement became strict, compliance was low. Privacy laws face the same problem today.

The Role of Public Pressure in Privacy Reform

While regulation is important, public awareness and activism are equally critical in pushing for stronger privacy protections.

- **Public backlash has led to meaningful policy changes** – After the Facebook–Cambridge Analytica scandal, governments worldwide pushed for tougher privacy regulations.
- **User adoption of privacy tools** – The rise of encrypted messaging apps (Signal, WhatsApp E2E encryption) came in response to growing concerns over corporate surveillance.
- **Boycotts and pressure campaigns** – Companies have been forced to change policies when faced with mass user defections.

A cryptography and privacy researcher explained, "Privacy activism isn't just about laws—it's about shifting public expectations. Companies change when they fear losing customers."

Continued next page

The Cost of Reading Privacy Policies: A Time-Consuming Dilemma

In an era where nearly every online interaction requires agreement to a privacy policy, one might assume users carefully read these documents before clicking "accept." However, a Carnegie Mellon University study titled "The Cost of Reading Privacy Policies" by Aleecia M. McDonald and Lorrie Faith Cranor reveals a stark reality—reading every privacy policy encountered online is simply not practical.

Their research found that if the average American Internet user were to thoroughly read every privacy policy they encountered in a year, it would take approximately 244 hours, the equivalent of 30 full working days. This staggering time commitment underscores why most users opt for convenience over comprehension, accepting terms without reading them.

"It’s unrealistic to expect individuals to read and understand every privacy policy they encounter,” said one privacy policy lawyer. “The time burden alone makes true informed consent nearly impossible."

This phenomenon illustrates a core flaw in modern digital privacy practices—while users are given the illusion of choice, the sheer impracticality of reading every policy means they are functionally unable to make informed decisions about their data.

Lesson

Requiring users to read and agree to complex privacy policies is not a viable solution for ensuring informed consent. Instead, privacy frameworks must focus on clear, concise, and standardized disclosures that empower users without requiring days of legal reading.

Detailed Findings: AI is the Gamechanger for Digital Privacy

AI is the Gamechanger for Digital Privacy

The experts we interviewed agreed: Artificial intelligence marks a turning point for digital privacy—one that even seasoned experts find deeply unsettling. Unlike traditional data collection, AI doesn't just observe; it infers, predicts, and reconstructs personal details from the smallest behavioral signals. Without ever filling out a form or clicking "yes," people are profiled through their typing speed, scrolling patterns, phrasing of comments, or time spent hovering over an image.

Nearly every expert interviewed for this report warned that AI erodes the boundary between what individuals knowingly share and what is silently extracted. Inference is the new frontier. And the consequences are quiet but profound: targeting, manipulation, and surveillance can now occur without a single privacy policy being broken.

As one expert put it, "AI doesn't wait for you to give up your privacy. It takes it before you know you've given anything away."

This isn't just a technical issue—it's an ethical one. How do we protect privacy when machines can guess what we never said? The future of digital privacy may depend not only on how data is collected, but how it is interpreted, inferred, and weaponized.

AI Knows Your Politics—Even if You Never Said a Word

AI doesn't need you to explicitly state your political views to figure them out. By analyzing likes, follows, shared articles, and even the words you avoid, AI can accurately predict political leanings—sometimes better than your own friends and family.

One researcher described a study where AI analyzed images shared on Twitter. Even without looking at text, the AI was able to predict users' political affiliations with high accuracy—just based on the types of images they engaged with.

"You don't need to tweet about politics for AI to know your views. The images you like, the influencers you follow, even the color schemes you prefer—it all contributes to a predictive model." – Computer Science Professor

This has profound implications:

- Profiles can be used for micro-targeting, influencing elections and public opinion.
- People who think they're staying neutral online may still be categorized into ideological "buckets" without their consent.
- Once a prediction is made, users may be served content that reinforces those beliefs, creating information bubbles.

Lesson

AI doesn't just analyze what people say—it makes inferences from the smallest digital traces. This raises major privacy concerns, as individuals have no control over how AI interprets their behaviors, and they may be judged based on invisible, unverifiable assumptions.

Detailed Findings: Privacy in Physical Space vs. Digital Space

Privacy in Digital Space vs. Physical Space

When asked how privacy protections in physical and digital environments influence each other, many interview participants struggled with the concept. The challenge seemed to be that while physical privacy has clear, tangible boundaries (e.g., closing a door, covering a camera), digital privacy is more abstract, invisible, and constantly shifting.

Some key themes emerged from the responses:

- People often apply physical-world privacy concepts to digital spaces, even when they don’t fit. Several participants noted that users assume online interactions function like private, one-on-one conversations, when in reality, data is often collected, stored, and analyzed in ways they do not see or control.
- Laws and norms that work in the physical world don’t always translate to digital spaces. For example, trespassing laws prevent someone from entering a private home without permission, but in the digital world, companies routinely collect personal data without explicit user consent and often face few consequences.
- Surveillance feels different online and offline. Several participants noted that while people generally object to cameras in dressing rooms or government listening devices in homes, they often tolerate or ignore digital surveillance—even though the amount of data collected online is far greater than anything gathered in the physical world.
- Some digital privacy lessons could be applied to physical spaces. One participant pointed out that the detailed tracking and behavioral profiling that companies use online are now influencing physical-world environments, such as facial recognition in public spaces and personalized advertising in stores.

The general takeaway from interviewees was that digital privacy is more difficult to conceptualize, regulate, and enforce than physical privacy. However, as digital tracking extends into the physical world (e.g., smart cities, biometric surveillance), the boundary between the two is becoming increasingly blurred.

Detailed Findings: Best Practices for Achieving Digital Privacy

We will never have privacy as long it's a trade off against convenience. – Privacy Researcher and Medical Faculty Member

Technology waits for no one. – Privacy Policy Lawyer

Best Practices for Achieving Digital Privacy

These experts agreed, while strong security practices and privacy-enhancing technologies are essential, they are not enough. True privacy protection requires a fundamental shift in how businesses, policymakers, and individuals approach personal data. They said that the current privacy landscape is broken—companies are largely driven by compliance rather than ethics, individuals are overwhelmed by legal jargon and misleading consent mechanisms, and policymakers are constantly playing catch-up with fast-moving technology. What, then, are the best ways forward?

Rethinking Privacy: The Role of Businesses and Engineers

The principle of privacy by design was a recurring theme among interview participants. Instead of bolting on privacy safeguards after a product is built, companies should embed privacy into systems from the start. That means collecting only what is necessary (data minimization), ensuring strong encryption, and making privacy policies transparent and user-friendly.

The lawyers and regulators, in particular, asserted that we shouldn't be asking, "Are we compliant?" We should be asking, "Are we respecting user privacy in a meaningful way?"

Transparency was another major concern. Too often, companies bury data collection details in long, unreadable terms of service. Businesses need to rethink the way they inform users—using clear, simple language and giving individuals meaningful choices about their data.

Data retention policies also need reform. One of the biggest risks to digital privacy is the accumulation of unnecessary data. Many companies store personal data indefinitely, increasing the risk of leaks, hacks, and unauthorized access. By limiting data retention and deleting unnecessary information, companies can reduce the impact of data breaches and ensure better security.

But real change will not happen without accountability. Privacy audits, stronger internal policies, and oversight mechanisms are necessary to ensure that companies follow through on their commitments.

Continued next page

Best Practices for Achieving Digital Privacy (cont.)

What Individuals Can Do to Protect Their Privacy

While much of the responsibility should fall on corporations and policymakers, individuals can take steps to protect themselves in an increasingly data-driven world.

Practicing “information hygiene”—being mindful of what data is shared and with whom—can go a long way in reducing personal exposure. Using privacy-focused tools (such as VPNs, encrypted messaging apps, and browsers that block tracking) helps minimize surveillance.

However, several experts pointed out that placing too much responsibility on individuals is unfair. Many people don’t have the time or technical knowledge to fully understand how their data is used. The real solution is stronger systemic protections, not just better personal habits.

The Role of Policymakers and Advocacy in Privacy Protection

Privacy regulations like GDPR have set an important foundation, but many experts stressed that these laws represent only the bare minimum. True privacy protection requires more than compliance—it requires a shift in mindset.

One of the biggest problems with current regulations is the checklist mentality. Many companies do the absolute minimum necessary to meet legal requirements rather than genuinely improving privacy protections. This is why privacy laws need to focus on the spirit of the law, not just the letter of the law.

Education is another major piece of the puzzle. Several experts emphasized that individuals cannot protect their privacy if they don’t understand how their data is being collected and used. Stronger public awareness campaigns—similar to cybersecurity education efforts—could help individuals make more informed decisions.

The Future of Digital Privacy: Two Diverging Paths

When asked about the next decade of privacy, experts had conflicting views on where things are headed. Some were hopeful that we are moving toward a more privacy-conscious world. Others feared that the worst is yet to come.

Some experts believed that privacy laws will strengthen globally, forcing companies to prioritize transparency and user control. They pointed to recent regulatory movements—such as stronger consumer data rights in the EU and emerging privacy legislation in countries like India and Brazil—as signs that digital privacy is gaining traction.

Continued next page

Best Practices for Achieving Digital Privacy (cont.)

There was also optimism about privacy-enhancing technologies, particularly among the technologists interviewed. Innovations such as federated learning, differential privacy, and encrypted computation could allow companies to analyze data without directly exposing personal information. If widely adopted, these technologies could fundamentally change the way data is collected and used.

From a business perspective, there is growing recognition that privacy is a competitive advantage. Companies that prioritize privacy-first design may gain consumer trust and set themselves apart from competitors.

But others had a much darker outlook.

For one, AI-driven surveillance is expanding rapidly, making privacy protection even harder. Facial recognition, behavioral tracking, and real-time inference technologies are eroding the ability to remain anonymous, both online and in public spaces.

There was also concern about the rise of biometric data collection. Unlike passwords, you cannot reset your fingerprints or face. Once compromised, biometric data remains a permanent vulnerability.

Perhaps the most unsettling prediction was that companies will continue to find creative ways to sidestep privacy laws. As one expert put it, “Privacy laws are just speed bumps—companies will always look for ways around them.” Even as new regulations emerge, business models built on data extraction will resist meaningful change.

"Technology is evolving fast, and privacy is playing catch-up. The question is: Will regulators and the public demand better protections, or will we just accept the erosion of privacy as inevitable?" –Digital Identity Specialist

Continued next page

Specific Technologies and Practices

Following are some of the specific technologies and practices these privacy experts said could help protect privacy in the future.

- **Privacy by Design** – Mentioned as a foundational principle that ensures privacy is integrated from the start.
- **Anonymization & De-identification** – Experts noted the limitations and challenges of true anonymization.
- **Homomorphic Encryption** – Brought up in discussions about secure computation.
- **Zero-Knowledge Proofs** – Mentioned as a way to verify transactions without revealing data.
- **Synthetic Data** – Used to train AI models without exposing real user data.
- **Privacy Impact Assessments (PIAs)** – Discussed as a regulatory tool to evaluate risks.
- **Decentralized Identity (DID)** – Raised as a potential alternative to centralized identity management.
- **Self-Sovereign Identity (SSI)** – Related to giving users control over their own digital identities.
- **AI Explainability** – Discussed in the context of transparency and user trust.
- **End-to-End Encryption** – Cited as a key safeguard for communication privacy.
- **Metadata Stripping** – Mentioned as a method to remove identifying details from shared files.
- **Regulatory Sandboxes** – Discussed as environments for testing privacy technologies under real conditions.
- **Federated Learning** – Instead of collecting raw data, AI models are trained locally on users' devices and only send aggregated, anonymized updates to central servers.
- **Privacy-Preserving AI Algorithms** – Differential privacy techniques add noise to datasets to prevent individual identification while still allowing useful analysis.
- **Stronger AI Transparency and Oversight** – Requiring companies and governments to disclose how AI makes decisions could help reduce bias and increase accountability.
- **User Control Over AI Profiles** – Some privacy advocates suggest that individuals should have the right to inspect, edit, or delete AI-generated inferences about them.

Continued next page

Appendix

Major Privacy Legislation, Guidelines, Policies Referenced in these Interviews

- **General Data Protection Regulation (GDPR) – European Union**
  (https://gdpr-info.eu/)
  The GDPR is a comprehensive data protection law that governs the collection, use, and storage of personal data within the EU.

- **Artificial Intelligence Act (AI Act) – European Union (**
  (https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence)
  The AI Act establishes a regulatory framework for AI systems, classifying them based on risk levels and imposing requirements accordingly.

- **Digital Services Act (DSA) – European Union**
  (https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package)
  The DSA sets rules for online platforms to create a safer digital space, addressing issues like illegal content, transparent advertising, and user rights.

- **Digital Markets Act (DMA) – European Union**
  (https://digital-markets-act.ec.europa.eu/index_en)
  The DMA aims to ensure fair competition in the digital market by regulating large online platforms acting as "gatekeepers."

- **ePrivacy Directive – European Union**
  (https://www.edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en)
  Also known as the "Cookie Law," this directive focuses on the privacy and protection of personal data in electronic communications.

- **Data Governance Act (DGA) – European Union**
  (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act)
  The DGA aims to foster data sharing across the EU, promoting a single market for data to enhance innovation and the digital economy.

- **California Consumer Privacy Act (CCPA) – United States**
  (https://oag.ca.gov/privacy/ccpa)
  The CCPA grants California residents rights regarding their personal information, including the right to know, delete, and opt-out of the sale of personal data.

- **California Privacy Rights Act (CPRA) – United States**
  (https://www.caprivacy.org/cpra-exec-summary/)
  An amendment to the CCPA, the CPRA enhances consumer privacy rights and establishes the California Privacy Protection Agency for enforcement.

Major Privacy Legislation, Guidelines, Policies Referenced in these Interviews

- **Personal Information Protection Law (PIPL) – China**
  China's PIPL, effective since November 1, 2021, regulates the processing of personal information, emphasizing consent and individual rights.
- **Artificial Intelligence and Data Act (AIDA) – Canada**
  Canada's proposed AIDA aims to regulate AI systems, focusing on transparency, accountability, and mitigating risks associated with AI.
- **Data Privacy Act of 2012 – Philippines**
  This act mandates the creation of the National Privacy Commission to monitor and maintain policies involving information privacy and personal data protection.
- **Personal Data Protection Act 2012 (PDPA) – Singapore**
  Singapore's PDPA governs the collection, use, and disclosure of personal data by organizations, ensuring individuals' privacy is protected.
- **General Personal Data Protection Law (LGPD) – Brazil**
  Brazil's LGPD is a comprehensive data protection law that regulates the processing of personal data, ensuring individuals' rights are safeguarded.
- **Artificial Intelligence Act – European Union**
  The EU AI Act establishes a comprehensive regulatory framework for AI systems, classifying them based on risk levels and imposing requirements accordingly.
- **Blueprint for an AI Bill of Rights – United States**
  The U.S. has introduced a framework outlining principles to guide the design, use, and deployment of AI and automated systems, emphasizing rights and freedoms.
- **Council of Europe Convention on Artificial Intelligence – International**
  The Council of Europe has adopted the first-ever international legally binding treaty aimed at ensuring the respect of human rights, the rule of law, and democracy in the use of AI systems.

Reports and Studies Referenced in these Interviews

- Global Data Privacy Report - https://globaldma.com/consumer-attitudes/
- The Cost of Reading Privacy Policies," was conducted by Aleecia M. McDonald and Lorrie Faith Cranor. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

FOR MEDIA OR OTHER INQUIRIES:

Please contact digitalprivacyinfo@ieee.org

RECOMMENDED CITATION:

How Experts Think about Digital Privacy. (July 2025). IEEE Digital Privacy. https://digitalprivacy.ieee.org/wp-content/uploads/2025/07/How-Experts-Think-About-Digital-Privacy.pdf