Data Privacy in the Age of Surveillance

# Members Names

1. **Ahmed Muse Ahmed**
2. **Hussein Ali Salad**
3. **Abdirahman Ismail Ilmi**
4. **Ahmed Mohamed Mohamud**
5. **Husni Isack Nur**
6. **Ismail Ali Salad**
7. **Abdullahi Mohamed Ahmed**
8. **Abdirahman Hassan Heider**
9. **Hassan Dahir Ali**
10. **Amina Ahmed Nur**
11. **Sacdiya Salad Mohamed**

Prepared by: Group Name

SIMAD University  
Course: Ethics for Computing

Date: June 14, 2025

Table of Contents

[Data Privacy in the Age of Surveillance 3](#_Toc200777414)

[Introduction 3](#_Toc200777415)

[Data as Oil 4](#_Toc200777416)

[Government Surveillance 5](#_Toc200777417)

[Government Surveillance – Visual Insight 6](#_Toc200777418)

[Smart Devices 7](#_Toc200777419)

[Smart Devices – Visual Insight 8](#_Toc200777420)

[Facial Recognition 8](#_Toc200777421)

[Facial Recognition – Visual Insight 9](#_Toc200777422)

[Corporate Collection 10](#_Toc200777423)

[Corporate Collection – Visual Insight 11](#_Toc200777424)

[Privacy Laws 12](#_Toc200777425)

[Privacy Laws – Visual Insight 12](#_Toc200777426)

[Digital Consent 13](#_Toc200777427)

[Digital Consent – Visual Insight 15](#_Toc200777428)

[Data Breaches 16](#_Toc200777429)

[Data Breaches – Visual Insight 17](#_Toc200777430)

[Digital Minimalism 18](#_Toc200777431)

[Digital Minimalism – Practices and Benefits 18](#_Toc200777432)

[Conclusion 19](#_Toc200777433)

[References 21](#_Toc200777434)

# Data Privacy in the Age of Surveillance

# Introduction

We live in an era where data is created every second every click, tap, search, or purchase we make online adds to a growing pool of digital information. From using mobile phones and apps to visiting websites and smart cities, we are constantly leaving behind digital footprints. These footprints are being collected, analyzed, and stored by companies, governments, and other entities, often without our full understanding or consent.  
  
The concept of privacy has changed dramatically in the digital age. In the past, privacy was mostly physical who we spoke to, what we did behind closed doors, or where we went. Today, our personal lives are digitized and monitored through our online interactions. Surveillance is no longer limited to cameras on the streets or security agents; it now includes cookies in browsers, GPS tracking on phones, social media behavior, voice commands given to smart assistants, and even facial recognition in public spaces.  
  
The purpose of this report is to explore the different dimensions of data privacy in this surveillance-driven age. It looks at how governments, corporations, and technologies are involved in surveillance practices, how they use or abuse data, and what laws and measures are being taken to protect individuals. It also aims to highlight the responsibilities of users, the risks of careless digital behavior, and strategies for protecting one’s personal information in a connected world.  
  
By understanding the scope and impact of surveillance, we can better advocate for strong privacy protections, demand transparency from organizations, and take personal steps to stay safe online. This is not just a technical or legal issue it is a matter of freedom, dignity, and trust in the digital era.

# Data as Oil

Data has become one of the most valuable resources in the world often called the "new oil." Companies collect, analyze, and sell user data for profit. The more they know about people, the more power and revenue they can generate.

Data fuels many of the services we use daily. **Netflix** recommends shows based on viewing habits. **Google** builds advertising profiles by collecting data from Gmail, YouTube, Maps, and searches. **Amazon** tracks purchases, browsing behavior, and Alexa voice interactions to shape recommendations and offers.

Data helps businesses improve services and predict user behavior.

Most data is collected without users fully understanding how it’s used.

Selling and sharing personal data has become a **multi-billion-dollar industry**.

This ecosystem influences not only marketing, but also **political campaigns**, **financial decisions**, and **public policy**. The rise of **data brokers** companies that buy and sell consumer data has added complexity to how personal information flows through the digital economy, often without public awareness or oversight.

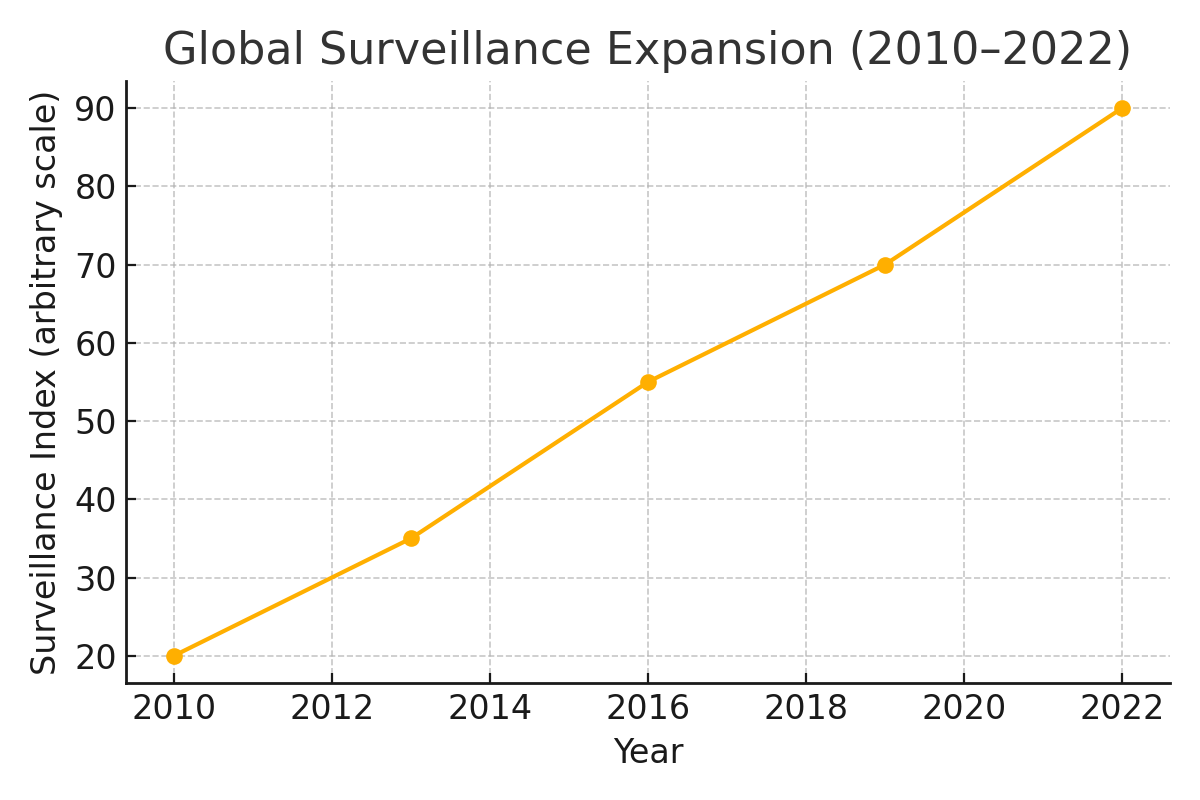


Figure. 1: Growth of Global Surveillance Systems from 2010 to 2022.

# Government Surveillance

Governments use surveillance to ensure national security and detect criminal activity. However, too much surveillance can harm people’s rights. It can make people feel watched, limit free speech, and cause fear. Programs like PRISM and XKeyscore revealed how some governments gather massive amounts of information on citizens.

Modern surveillance technologies include mass data collection from internet service providers, biometric tracking through facial recognition and fingerprint scanning, and real-time monitoring of public spaces via smart CCTV networks. In countries like **China**, surveillance is deeply embedded in the social system, with the **Social Credit System** tracking citizen behavior to enforce compliance. In contrast, countries like **Germany** and **Canada** emphasize judicial oversight and legal safeguards.

The **2013 Snowden revelations** showed that agencies like the **NSA** had extensive access to emails, phone metadata, and online activity of U.S. citizens and foreign nationals. These disclosures sparked international outcry and encouraged companies to adopt **end-to-end encryption** and better data protection.

The **United Nations** and other global organizations have warned against unchecked surveillance, emphasizing the importance of balancing national security with civil liberties. As technology advances, so must global privacy standards.

Mass surveillance can impact innocent individuals.

There is a need to balance safety with civil liberties.

International discussions are ongoing about ethical boundaries.

The Snowden leaks highlighted risks of unchecked government access.

Some nations enforce strict surveillance; others require judicial approval.

Over-surveillance can erode public trust and democratic values.

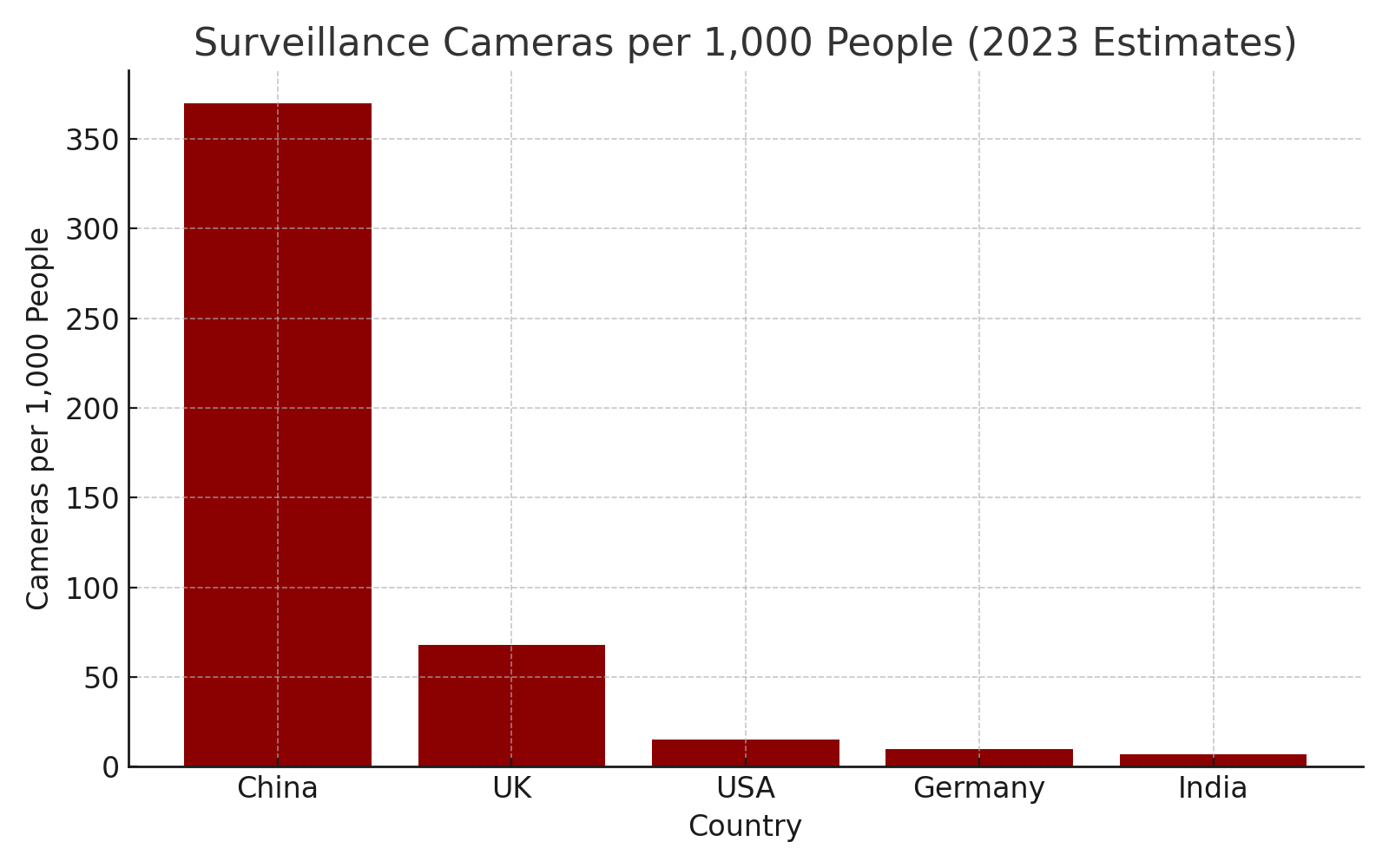


Figure. 2: Estimated Surveillance Camera Density by Country (2023) — Number of Cameras per 1,000 People

## Government Surveillance – Visual Insight

The use of surveillance cameras by governments has rapidly increased over the past decade. While helpful in crime detection, these cameras also raise privacy concerns.

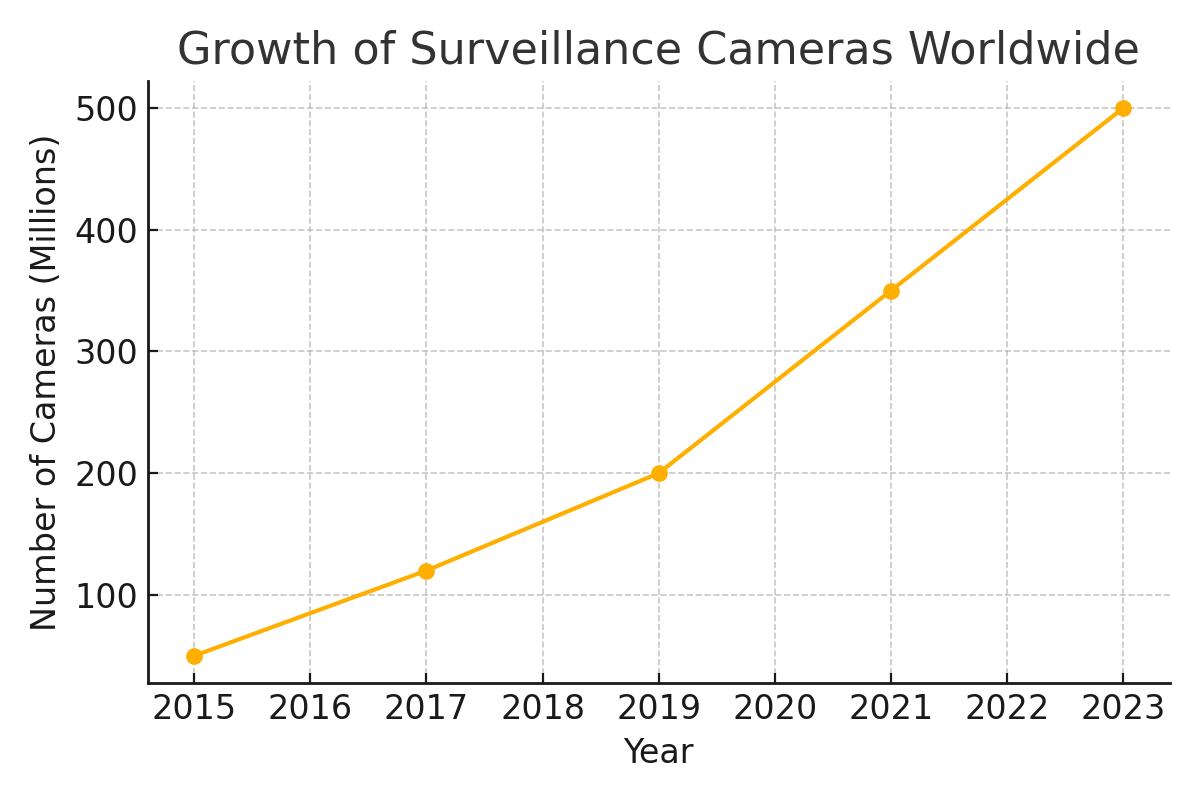


Figure. 3: Global Growth of Government Surveillance Cameras (2015–2023).

# Smart Devices

Smartphones, smartwatches, home assistants, and IoT devices collect real-time data. This includes location, voice, and health metrics. While they offer convenience, they also silently track habits and preferences.

Devices like **smart TVs**, **robot vacuums**, and **fitness trackers** are capable of recording behavior, preferences, and movement patterns. Smart speakers such as **Amazon Alexa** or **Google Home** are designed to be always listening, which can inadvertently lead to the collection of sensitive conversations. These devices often send data back to manufacturers or cloud services, where it's processed and sometimes shared with third-party advertisers.

* Smart speakers can listen 24/7 and may store recordings unless settings are manually adjusted.
* Many users don’t realize how much behavioral and biometric data is gathered from wearables.
* Privacy settings are often buried or default to data-sharing modes.

According to **Statista**, the number of IoT-connected devices worldwide surpassed **10 billion in 2021**, and it's projected to exceed **25 billion by 2025**. Despite this rapid growth, surveys show that **over 60% of users do not fully understand how to manage or restrict the data their smart devices collect**.

These trends highlight the need for **stronger consumer protections**, **clearer interfaces**, and **increased public education** on smart device privacy.

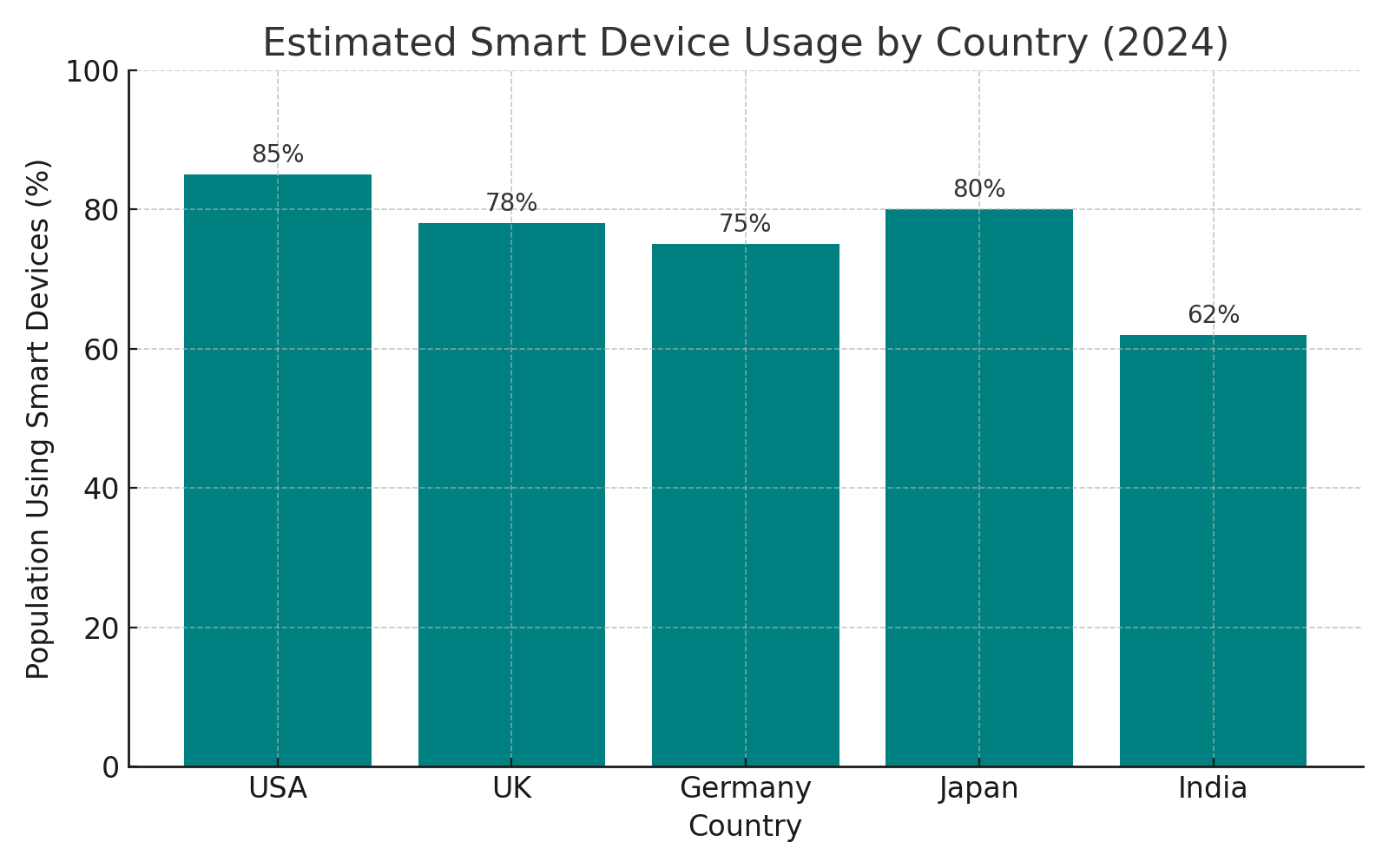


Figure 4: Percentage of Population Using Smart Devices in Selected Countries (2024 Estimate)

## Smart Devices – Visual Insight

The chart below shows how widely smart devices are used in different countries. This highlights the scale of data collection from everyday technology.

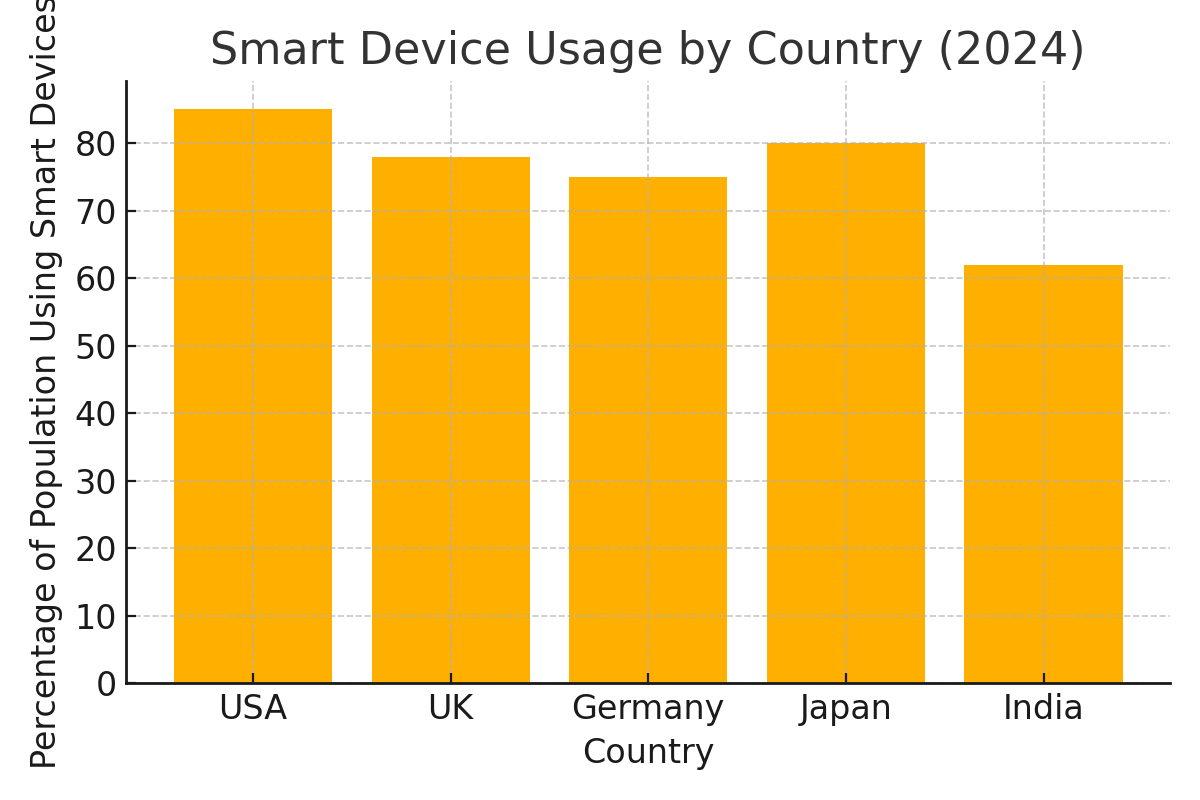


Figure. 5: Smart Device Usage by Country in 2024.

# Facial Recognition

Facial recognition uses AI to identify people from photos or video. It's used in airports, phones, and public safety systems. However, it has accuracy problems, especially with minorities, and can be abused by authorities.

Facial recognition systems have been deployed by law enforcement, retail outlets, and even school districts to improve identification speed and public safety. However, this convenience comes with serious concerns. In the U.S., cities like **San Francisco** and **Boston** have banned the use of government facial recognition over concerns about racial bias and lack of oversight.

A study by **MIT Media Lab** revealed that major commercial facial recognition tools misidentified **darker-skinned women up to 35% of the time**, while the error rate for lighter-skinned men was below 1%. These accuracy gaps can result in wrongful arrests and other discriminatory outcomes.

In **China**, facial recognition is integrated into the country’s **social surveillance infrastructure**, especially in regions like Xinjiang, where it's used to monitor ethnic minorities. In contrast, **European countries** and the **UK** are calling for stricter laws and transparent oversight.

* Used to unlock phones and catch suspects
* Raises ethical issues and risks of racial bias
* Lack of regulation increases potential for misuse
* MIT studies show significant accuracy gaps between demographics
* Cities like San Francisco have banned it for civil rights reasons

## Facial Recognition – Visual Insight

Facial recognition accuracy is not equal for all groups. Research shows lower accuracy for people of color and women, which can lead to false identifications.

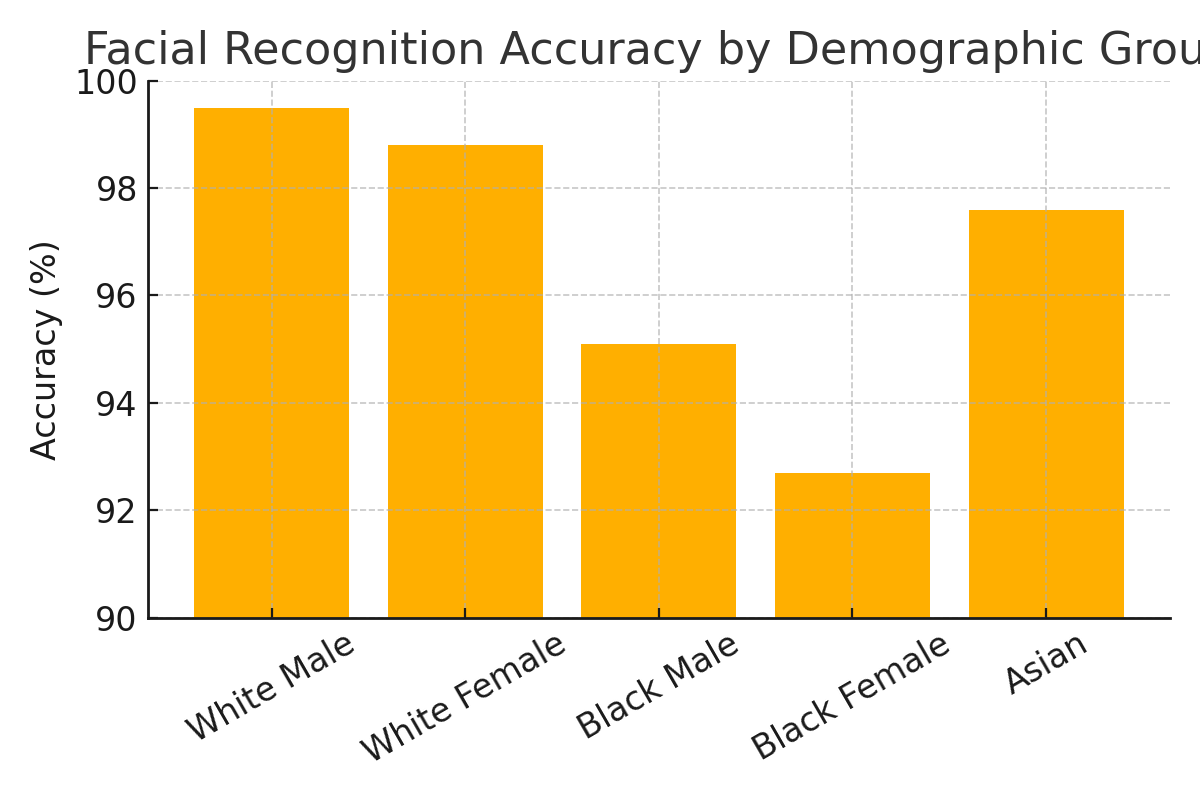


Figure. 6: Facial Recognition Accuracy by Demographic Group.

# Corporate Collection

Tech companies gather vast data through apps, search engines, and online behavior. They build user profiles to target advertisements. Many users agree to this unknowingly when they accept lengthy privacy policies.

In 2022, Meta (Facebook) generated over 98% of its revenue from advertising powered largely by user data. Apps often request access to contacts, location, camera, and microphone permissions not always needed for app functionality.

A key example is Google’s ad ecosystem, which combines data from Gmail, YouTube, Android, and Chrome to deliver hyper-targeted advertising. Amazon also uses purchase behavior and Alexa voice data to influence shopping trends.

The imbalance of power is striking. Users “consent” under pressure to gain access to services, while companies exploit that access for profit. Transparency reports and third-party audits are necessary to rebuild trust.

**Real-World Example – Meta’s Revenue Model:** Meta’s 2022 financial report shows that advertising generated approximately **$114 billion**, accounting for **98.5% of total revenue**. This shows how user data directly powers business models in the tech industry.

**Real-World Example – China's Social Credit System:** China’s Social Credit System integrates data from public behavior, financial records, surveillance footage, and social connections to score citizens. Low scores can restrict travel, school access, or even internet speeds. It represents one of the most centralized uses of mass surveillance.

**Real-World Example – Global Breach Figures:** According to the Identity Theft Resource Center, **over 4,100 data breaches** were publicly reported in 2023, exposing billions of records. Major victims included Twitter, T-Mobile, and Marriott, showing that even tech giants struggle to secure personal data.

* Terms and conditions are often unreadable.
* Data is shared with third parties and advertisers.
* Companies benefit financially, while users lose control.

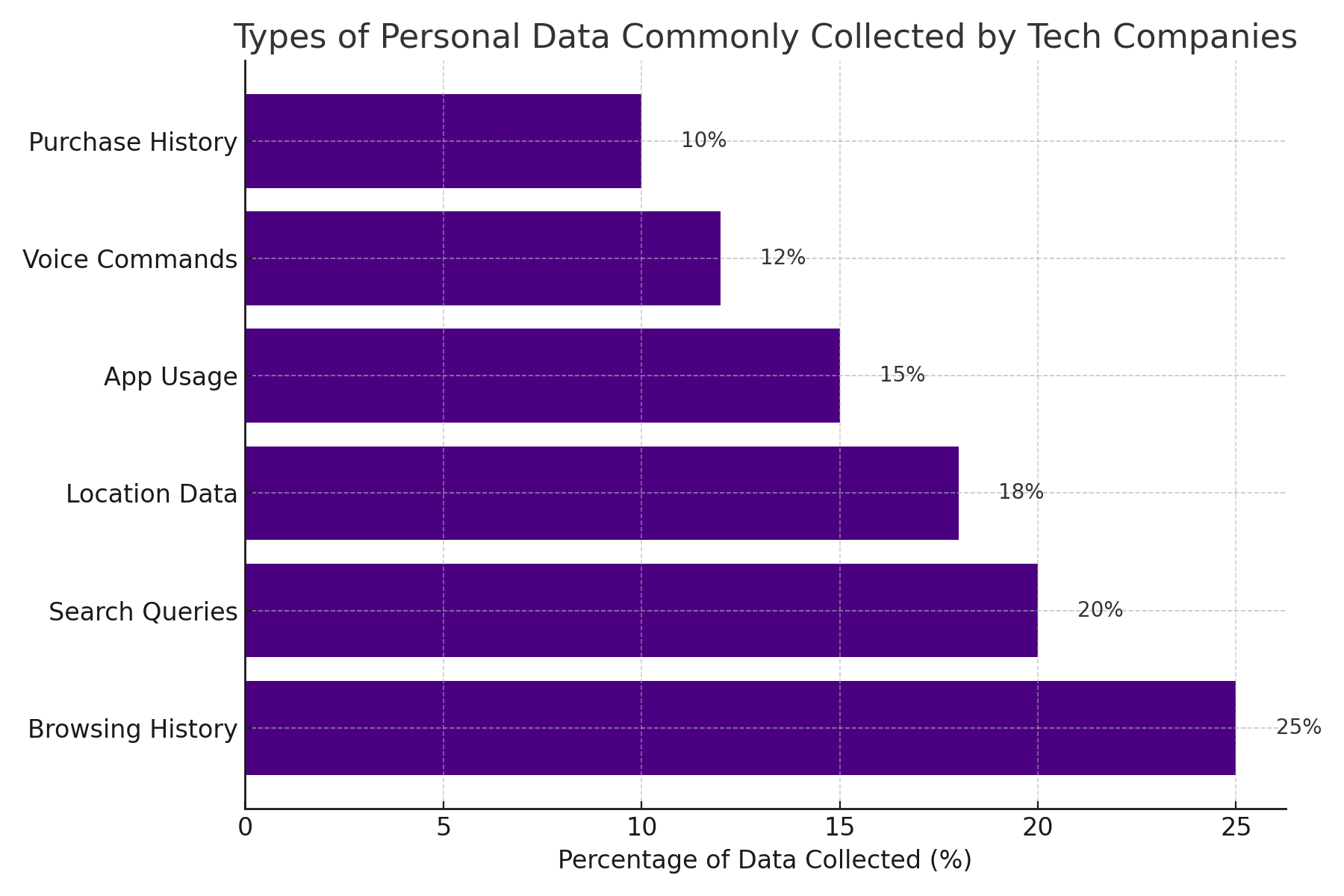


Figure. 7: Breakdown of Common Personal Data Types Collected by Major Tech Companies (2024 Estimate)

## Corporate Collection – Visual Insight

Technology companies gather various types of personal data to build user profiles. This data is then used for targeted advertising, recommendations, and business analytics.

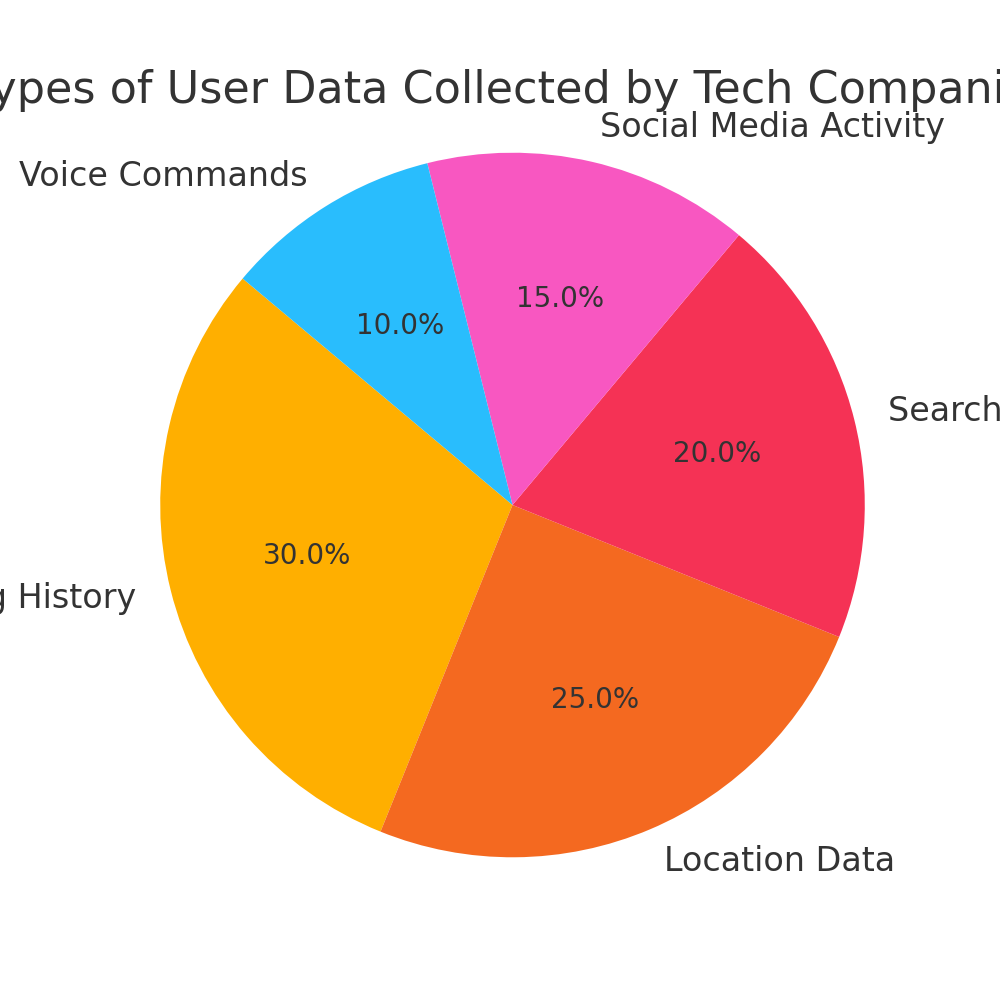


Figure. 8: Common Types of User Data Collected by Tech Corporations.

# Privacy Laws

Countries have started introducing privacy laws to protect data. The European Union’s GDPR and California’s CCPA are examples of laws giving people more control over their personal data.

|  |  |  |
| --- | --- | --- |
| **Feature** | **GDPR (Europe)** | **CCPA (California)** |
| Scope | Applies to all EU citizens and companies handling their data | Applies to California residents |
| Consent | Requires clear user consent | Allows opt-out of data sales |
| Penalties | Up to €20 million or 4% of global revenue | $2,500 - $7,500 per violation |
| User Rights | Access,correction, deletion, data portability | Access, deletion, opt-out |

Table 1: Comparison of Key Privacy Law Features – GDPR (Europe) vs. CCPA (California)

Other countries like Brazil (LGPD), South Africa (POPIA), and India (DPDP) have also introduced laws. Still, more than 40% of countries lack comprehensive data privacy regulations. The effectiveness of laws depends on enforcement, penalties, and cross-border cooperation.

## Privacy Laws – Visual Insight

The chart below compares key privacy law elements between the GDPR and CCPA. GDPR is generally stricter and offers broader protections, while CCPA focuses on consumer rights in California.

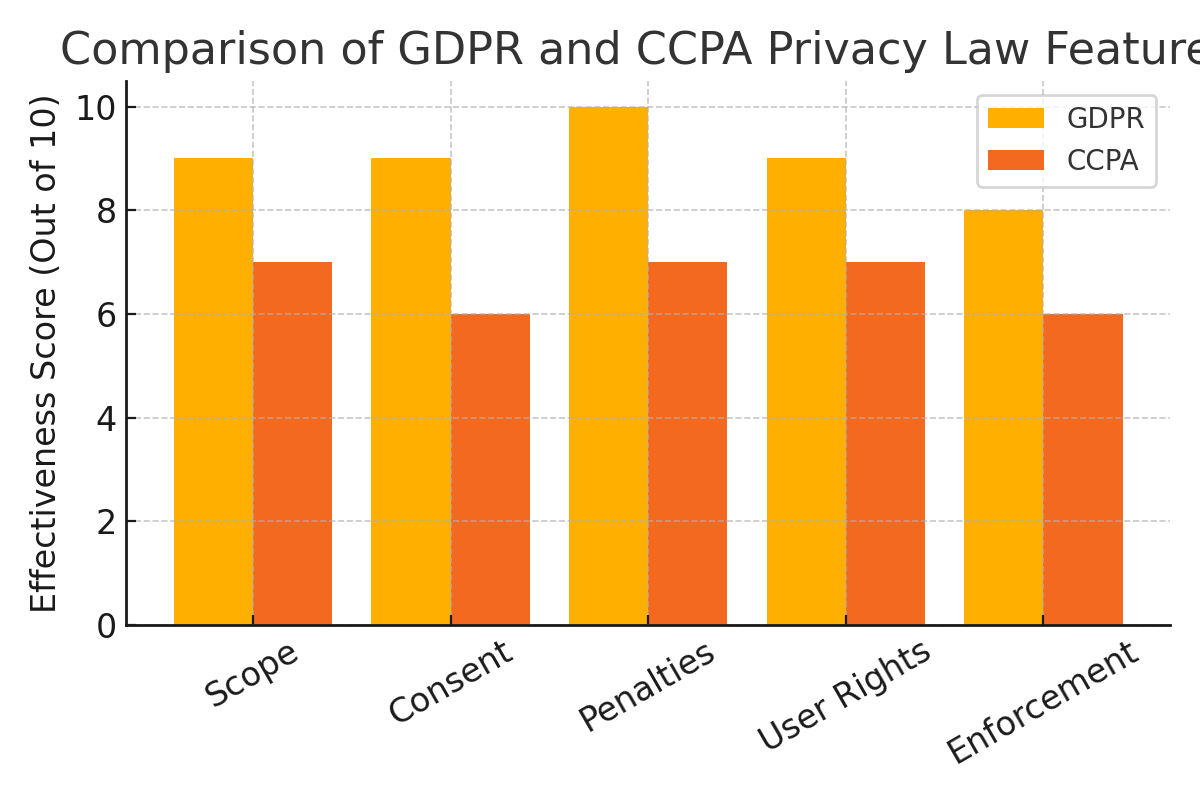


Figure. 9: GDPR vs. CCPA – Feature Comparison Chart.

# Digital Consent

Digital consent means users must give permission before companies collect and use their data. However, in practice, consent is often buried in long documents. Real consent must be informed, clear, and optional.

A 2021 study found the average privacy policy would take over 25 minutes to read. Most people simply click “I Agree.” Worse, companies use dark patterns design tricks that nudge users toward consenting.

Clear design, layered notices, and purpose-specific consent should be the new standard. Users should be empowered to grant or deny access without fear of losing access to essential services.

In many countries, regulations like GDPR require explicit consent, yet platforms often exploit gray areas to push users toward agreeing. For example, cookie banners on websites may feature bright “Accept” buttons while hiding “Reject” or “Manage Preferences” options under multiple clicks. These deceptive UX strategies can undermine true choice.

Informed consent should also be renewable and revocable. A person who grants access once should always have the ability to later revoke that permission just as easily.

Digital consent is not a one-time checkbox it is a continuous process. Users should be notified of any changes in data usage, and prompted to renew consent periodically. Companies like Apple and Mozilla have introduced permission reminders and privacy reports as proactive steps.

In addition, platforms should give users the ability to tailor their preferences, such as choosing which types of data to share or restricting access to sensitive information like health, location, or financial data. User dashboards with toggles and explanations can make privacy management accessible.

One notable example is **Mozilla Firefox’s Privacy Report**, which shows users how many trackers were blocked, making consent and data use more transparent. Similarly, **Apple’s iOS App Tracking Transparency** feature, introduced in 2021, forced all apps to explicitly request user permission before tracking leading to a significant reduction in app tracking across devices.

Educational efforts also play a role. Organizations like the **Electronic Frontier Foundation (EFF)** and **Mozilla Foundation** promote digital literacy, helping users understand their rights and make better-informed decisions about consent.

* People rarely read terms and conditions.
* Consent should be clear and easy to understand.
* Users should have the right to withdraw consent at any time.
* UX patterns should not manipulate or trick users.
* Consent should be updated over time, not treated as one-time permission.
* Notifications and reminders should prompt users to recheck their choices.
* Dashboards should give users visibility and control over the data they share.
* Technology companies should invest in consent education and transparency tools.

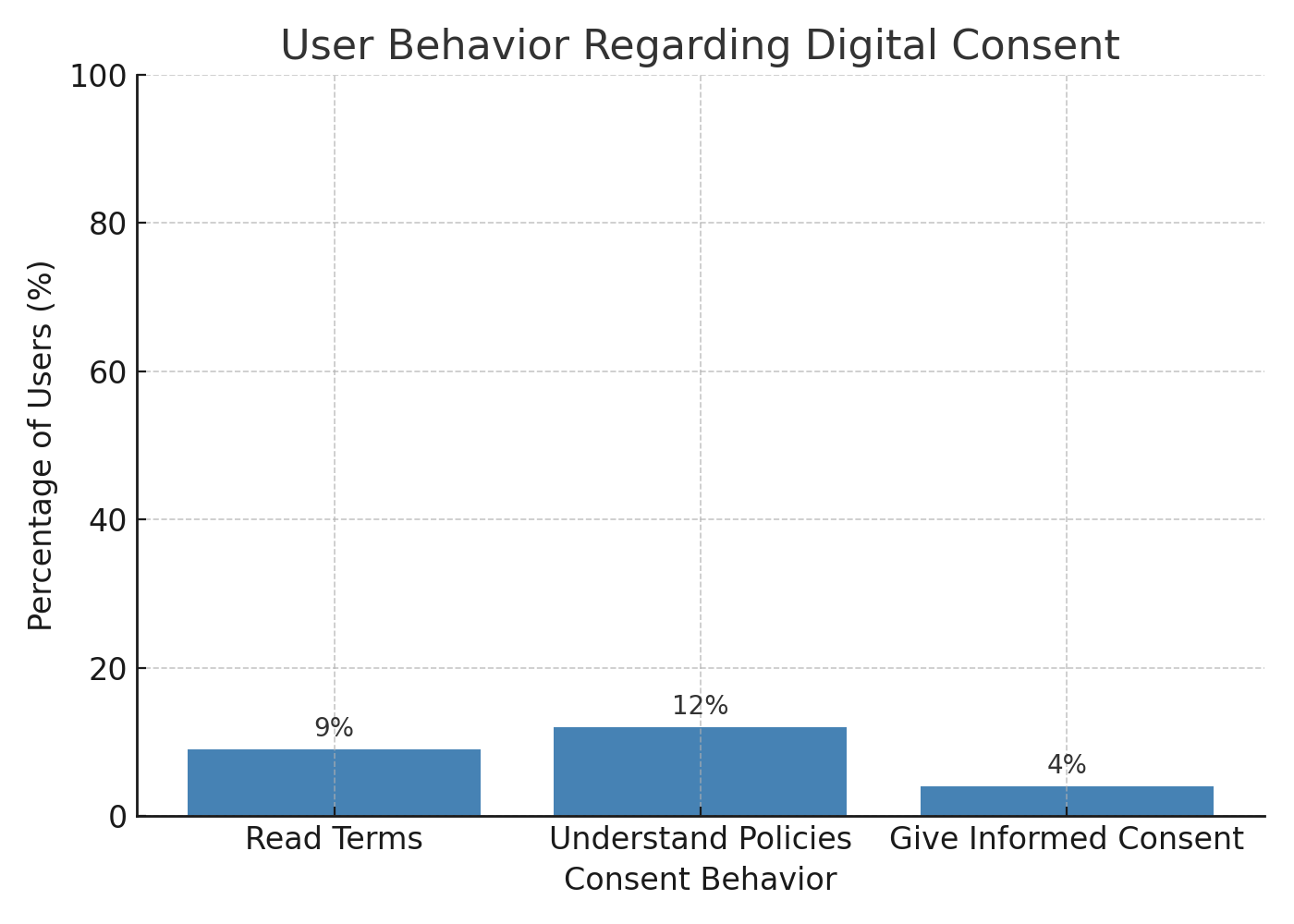


Figure 10: Percentage of Users Who Read, Understand, and Provide Informed Digital Consent (2023 Survey Estimate)

## Digital Consent – Visual Insight

Digital consent is supposed to ensure that users knowingly agree to data collection. However, research shows that most users don’t read or understand what they are agreeing to.

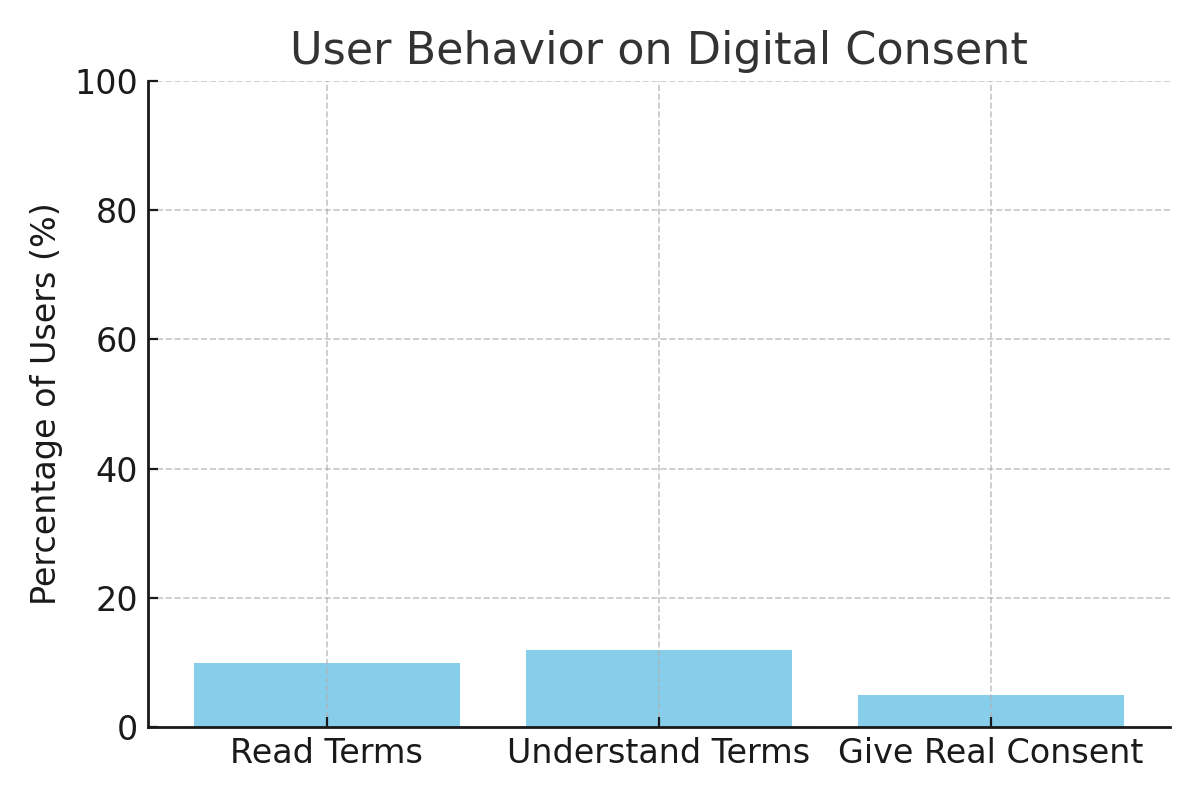


Figure. 11: User Engagement with Digital Consent (Hypothetical Estimates).

# Data Breaches

A data breach happens when unauthorized individuals access protected information. This often results in the loss of passwords, financial records, and private messages. Breaches can damage trust and cost companies millions.

In 2023 alone, over 4,100 data breaches were reported globally, exposing billions of records. Major incidents have included Twitter, T-Mobile, and Marriott, among others.

Cyberattacks are increasing in frequency, sophistication, and impact. Ransomware attacks in particular have surged, targeting hospitals, schools, and even local governments. In 2023, the average cost of a data breach reached **$4.45 million**, according to IBM’s annual report.

Sensitive data such as health records, biometric identifiers, and payment credentials are frequent targets, and once compromised, they can be used for identity theft, fraud, and blackmail.

To prevent breaches, companies must adopt a multilayered security strategy. **Zero-trust architecture**, **multi-factor authentication (MFA)**, **regular security audits**, and **employee cybersecurity training** are all critical components of breach prevention.

Transparency is also essential. Under laws like GDPR and CCPA, organizations are required to report data breaches to users within a specific time frame. Failing to do so not only risks legal penalties but also erodes consumer trust.

Strong encryption and data management are needed.

Victims face identity theft and other long-term impacts.

Ransomware and phishing attacks are rising in volume and cost.

Organizations must respond promptly and transparently.

Legal compliance requires swift notification and user protection.

Human error remains a major cause training is vital.

Small and medium businesses are especially vulnerable due to limited resources.

## Data Breaches – Visual Insight

Data breaches come in many forms. Hacking remains the most common, but internal errors and lost devices also expose person.

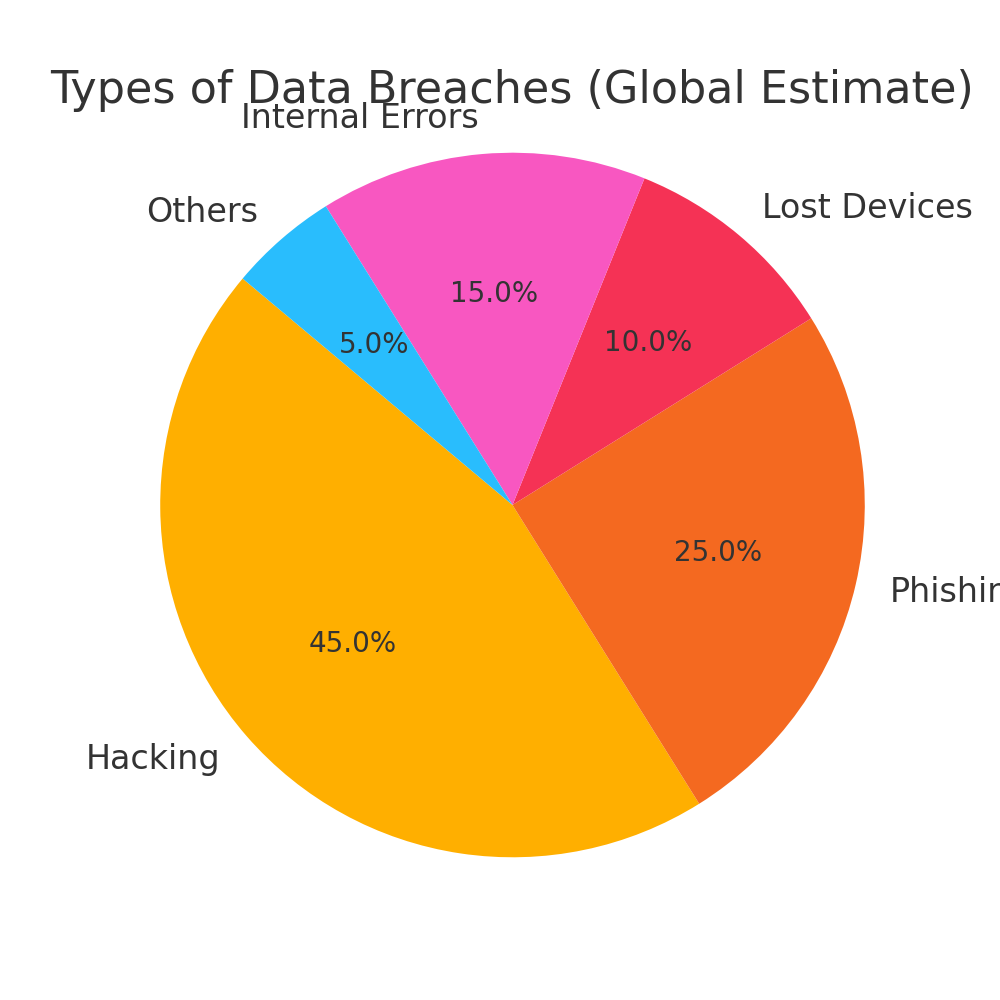


Figure. 12: Distribution of Data Breach Types Globally.

# Digital Minimalism

Digital minimalism is a lifestyle choice. It encourages using technology with purpose and reducing unnecessary digital exposure. By limiting app usage and sharing less, people can protect their privacy.

In addition to improving privacy, digital minimalism helps reduce anxiety, screen addiction, and decision fatigue. Studies show people who limit screen time report improved mental well-being and focus. A 2022 study published in the Journal of Behavioral Addictions found that individuals who practiced digital minimalism for just two weeks reported significantly better sleep quality and emotional regulation.

The practice promotes intentional living choosing tools that serve us instead of being controlled by them. Minimalism isn’t about abandoning technology altogether, but about aligning digital habits with personal values.

Digital minimalists often schedule regular “tech breaks,” set screen time limits, and opt for single-purpose devices. For example, using an e-reader rather than a tablet can help reduce distractions. Some also adopt minimalist phone setups with only essential apps on the home screen.

This lifestyle also encourages reflection on digital consumption asking, “Does this app add value to my life, or does it distract me?” Over time, these practices can lead to more mindful, less reactive relationships with technology.

## Digital Minimalism – Practices and Benefits

Digital minimalism is a way to reduce digital clutter and protect your privacy. Here are some strategies:

|  |  |
| --- | --- |
| **Practice** | **Privacy Benefit** |
| Disable location services | Prevents apps from tracking your movements |
| Uninstall unused apps | Reduces hidden data collection |
| Use privacy-focused browsers | Limits add tracking and fingerprinting |
| Turn off background data | Stops apps from collecting info while idle |
| Limit social media time | Reduces exposure of personal life online |

Table 2: Common Digital Minimalism Practices and Their Corresponding Privacy Benefits

# Conclusion

Data privacy is no longer just a technical or legal issue it is a fundamental human right. In the digital age, where surveillance technologies grow more advanced and invasive by the day, protecting that right has become both a personal and societal responsibility.

Every interaction with a smartphone, website, or smart device generates data that can be collected, analyzed, and potentially misused. This makes it crucial for individuals, governments, and corporations to play an active role in shaping a safer and more transparent digital world.

As shown throughout this report, individuals often unknowingly give up personal information through vague terms and conditions, while governments implement large-scale surveillance programs in the name of security. Corporations, in turn, collect, store, and monetize this information often without full user awareness or control.

To address these issues, legal frameworks like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States represent important steps in the right direction. While both laws aim to protect consumers, they differ in scope, consent mechanisms, and enforcement. These laws show that policy plays a key role in building a future where privacy is respected.

However, legal protections alone are not enough. They must be supported by transparent business practices, technological safeguards, and digital literacy among users. Global cooperation is also necessary, as data often flows across borders. Organizations such as the United Nations and the OECD have called for international agreements that respect privacy while enabling innovation.

In addition, privacy-enhancing technologies like end-to-end encryption, privacy-by-design frameworks, and user-controlled data vaults must be prioritized. These tools can give users practical control over their digital lives.

Educational efforts must also continue, empowering individuals to understand privacy risks and take informed actions. Digital literacy campaigns, particularly in schools and developing countries, are vital for building a privacy-conscious society.

Therefore, a truly privacy-respecting society depends on three pillars:

* **Governments** must enforce data protection laws and regulate surveillance powers responsibly.
* **Corporations** must prioritize ethical data usage, simplify consent, and be transparent about what they collect and why.
* **Individuals** must stay informed, adopt smart digital habits, and use tools like encrypted messaging, privacy browsers, and minimal apps.

Ultimately, data privacy is not about hiding it’s about having control. It's about ensuring that people can participate in digital life without being exploited, monitored, or profiled unfairly. With better laws, clearer digital consent, advanced privacy tools, and stronger public awareness, we can move toward a world where innovation and human dignity coexist.

# References

1. Zuboff, S. (2019). \*The Age of Surveillance Capitalism\*. PublicAffairs.
2. Greenwald, G. (2014). \*No Place to Hide\*. Metropolitan Books.
3. European Union. (2016). \*General Data Protection Regulation (GDPR)\*. https://gdpr.eu
4. California State Government. (2018). \*California Consumer Privacy Act (CCPA)\*. https://oag.ca.gov/privacy/ccpa
5. Schneier, B. (2015). \*Data and Goliath\*. W. W. Norton & Company.