DISEC

1.9 Issue Description

COMMITTEE	Disarmament and International Security Committee
ISSUE	Addressing the Right of Privacy in the Digital Age
SUBMITTED BY	Leo Gulyás-Gorka and Levente Cséri, Chairs of the Disarmament and International Security Committee
APPROVED BY	Vilmos Eiben, President of the General Assembly

Introduction

The right to digital privacy, in the past couple of years, has been a topic procuring significant relevance, due to many concerns about Big Brother actually watching us through our portable screens, without our conscious consent. Historically, privacy was primarily concerned with physical intrusions, but the digital era has introduced new challenges. The United Nations recognised the right to privacy as a fundamental human right in 1948, but its application in the digital realm is complex and evolving. As technology nowadays is able to evolve day by day, hour by hour or even minute by minute thanks to self-learning artificial intelligence, privacy laws become outdated at this same unprecedented pace. Attempts to address these issues include the implementation of regulations like the General Data Protection Regulation (GDPR) in Europe and the development of privacy-enhancing technologies.

Ensuring robust digital privacy apart from being vital to protect individual privacy rights is also crucial for maintaining global security alongside both national and international peace. Without updated regulations, vulnerabilities in data protection can be easily exploited, leading to cyberattacks, misuse of sensitive information, and destabilizing effects on national and international security frameworks. Therefore, revisiting this issue is imperative to uphold both personal freedoms and collective safety in an increasingly digital world.

Definition of Key Terms

Right to Privacy - The right of an individual to keep their personal matters and relationships secret, including the right to control what information about them is communicated to others. The exact UN definition of the term can be found in the 12th article of the UDHR.

Personal Data - Any information relating to an identified or identifiable individual.

Data Protection - Legal measures to safeguard personal information from unauthorised access, use, or disclosure.

Encryption - The process of encoding information in such a way that only authorized parties can access it.

Surveillance - The monitoring of behaviour, activities, or information for the purpose of information gathering, influencing, or directing.

GDPR - Refers to the General Data Protection Regulation, a comprehensive data protection legislation adopted by the European Union in 2016 (effective since 2018).

Big Brother - A fictional character from George Orwell's famous novel 1984, who watches over every move of each citizen.

AI - Short for artificial intelligence. In this text, this abbreviation usually refers to highly intelligent language models that users interact with.

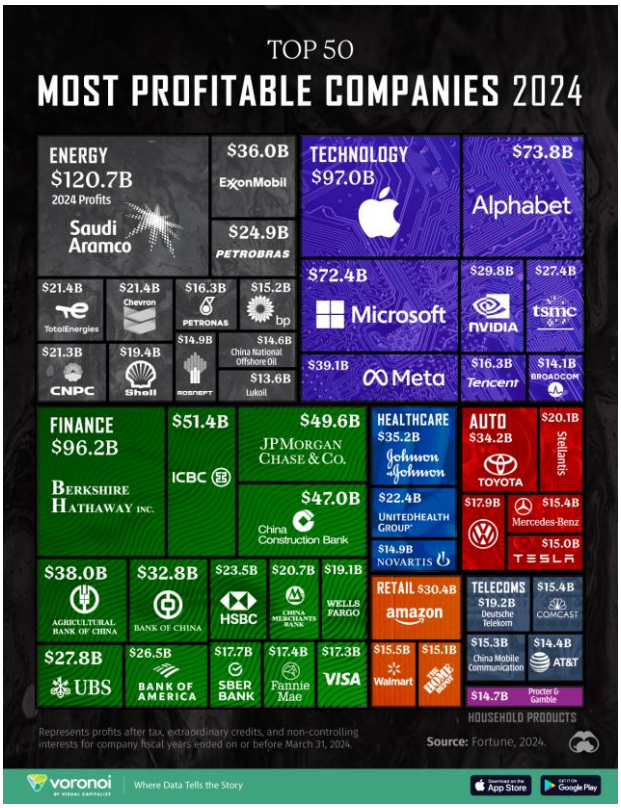
The Internet of Things (IoT) - IoT is a network of interconnected physical devices, vehicles, appliances, and other objects embedded with electronics, software, sensors, and network connectivity, enabling them to collect and exchange data without requiring human intervention - according to IBM.

General Overview

The rapid evolution of digital technology has brought both benefits and challenges to the concept of privacy. Traditionally focused on physical spaces, privacy now encompasses complex issues like data collection, surveillance, and artificial intelligence. Various regions have approached these challenges differently, creating disparities in privacy protections.

Concerns for digital privacy and surveillance is a relatively new concept. Even in the early 2000s, most people would never have thought the most valuable companies would secure a stable stream of income by selling user data for a profit. Surveillance on the other hand is not such a foreign concept, as it has been proven to be an effective and convenient tool to gain, enforce, and keep power in the past centuries, especially in politically unstable environments and time periods.

However, with the appearance of personal mobile devices connected to the internet, it has never been easier to track and surveille anyone. The issue of data privacy in 2025 extends beyond mere tracking; it encompasses the vast collection, analysis, and monetization of personal data by tech giants, governments, and various organizations. This includes everything from browsing habits and location data to biometric information and social interactions, raising profound questions about individual autonomy and the right to privacy in the digital age.



The responsibility for protecting privacy is increasingly seen as a shared obligation. Governments are enacting stricter regulations, but enforcement remains challenging across international borders. Companies are expected to implement privacy-by-design principles, but many still prioritize data collection for profit. Individuals are becoming more aware of their digital footprint, but often lack the tools or knowledge to effectively protect their privacy.

In the past couple of years, artificial intelligence (AI) has also become increasingly prevalent. Many are left concerned about the privacy risks such platforms pose. Major AI developing companies include OpenAI with their pioneer GPT, Google with their search-focused Gemini, and the newest addition to the team, the Chinese developed Deepseek AI model. The main concern about this type of language intelligence software lies in the extent and variety of user data processed through platform usage, alongside the potential private information a language model of such may acquire, even if the user never explicitly shared it.

Major Parties Involved

Globally, 137 countries have enacted data privacy laws, covering 79% of the world's population. Recent trends include heightened attention to children's privacy and the regulation of artificial intelligence, with the EU AI Act passed in 2024 as a landmark initiative. However, enforcement disparities and the rapid pace of technological change continue to challenge the effective implementation of these measures.

United Nations: The UN advocates for privacy as a fundamental human right, as outlined in Article 12 of the Universal Declaration of Human Rights (UDHR). Through initiatives like the International Covenant on Civil and Political Rights (ICCPR), the UN provides guidelines for member states to develop privacy frameworks. However, its lack of enforcement power means implementation varies widely. Countries with weak governance structures, such as those in Sub-Saharan Africa and parts of Southeast Asia, are often most affected by the absence of robust privacy protections, leaving their citizens vulnerable to data exploitation and surveillance.

European Union: The EU's General Data Protection Regulation (GDPR) is a global benchmark for data privacy, influencing legislation worldwide. The GDPR grants individuals rights such as data access, erasure, and portability while imposing strict accountability measures on organizations. The EU has also taken a leading role in regulating emerging technologies, such as the AI Act passed in 2024. Countries within the EU, like Germany and France, have been particularly proactive in enforcing these regulations. However, nations outside the EU, such as those in the Balkans and Eastern Europe, often struggle to align with GDPR standards due to resource constraints, leaving their citizens' data less protected.

Germany: Germany has been a pioneer in digital privacy, influenced by its historical experiences with state surveillance. The Federal Data Protection Act (BDSG) complements the GDPR, ensuring stringent data protection at the national level. Germany's proactive stance has set an example for other EU member states. However, countries like Poland and Hungary, which have weaker enforcement mechanisms, face challenges in implementing similar protections, making their populations more susceptible to data breaches and surveillance.

France: France's Commission Nationale de l'Informatique et des Libertés (CNIL) has been instrumental in enforcing GDPR compliance, issuing record fines to companies like Google for transparency violations. France's emphasis on accountability and transparency has strengthened privacy protections within its borders. However, countries in North Africa, such as Morocco and Tunisia, which have close ties to France, often lack comparable frameworks, leaving their citizens' data exposed to misuse.

United States: The U.S. lacks a comprehensive federal privacy law, relying instead on a patchwork of state-level regulations like the California Consumer Privacy Act (CCPA). While states like California and Virginia have made progress, the absence of uniform federal standards creates gaps in protection. This fragmented approach has made the U.S. a hotspot for data exploitation, particularly by tech giants. Countries like Mexico and Canada, which share significant digital trade with the U.S., are also affected by these inconsistencies, as their citizens' data often flows across borders with inadequate safeguards.

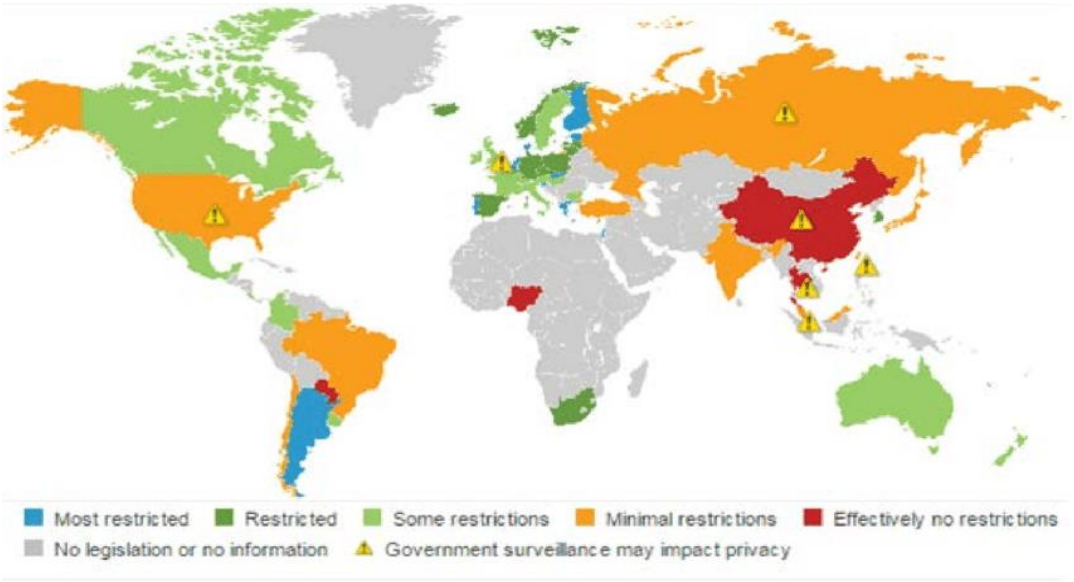
India: India's Digital Personal Data Protection (DPDP) Act of 2023 represents a significant step forward, emphasizing data minimization, strict consent protocols, and accountability. However, enforcement remains a challenge due to the country's vast population and digital divide. Neighbouring countries like Bangladesh and Nepal, which lack similar legislation, are heavily impacted by India's data practices, as their citizens' data is often processed by Indian firms without adequate protection.

China: China's Personal Information Protection Law (PIPL) establishes a comprehensive framework for data privacy, but its enforcement is often overshadowed by the government's extensive surveillance practices. Chinese tech companies, such as TikTok and WeChat, collect vast amounts of data domestically and internationally, raising concerns about data security. Countries in Southeast Asia, such as Indonesia and Malaysia, are particularly affected by China's data practices, as their citizens' data is frequently accessed by Chinese firms with limited oversight.

Tech Giants (Google, Facebook, Apple, TikTok): These companies process enormous volumes of personal data, shaping global privacy practices. While they have introduced measures like encryption and user controls, concerns about data misuse and monopolistic behaviour persist. Developing countries, such as those in Sub-Saharan Africa and Latin America, are disproportionately affected, as their regulatory frameworks are often too weak to hold these corporations accountable.

Privacy Advocacy Groups: Organizations like the Electronic Frontier Foundation (EFF) and Privacy International play a crucial role in raising awareness and advocating for stronger

privacy protections. They have been particularly active in regions with weak privacy laws, such as the Middle East and parts of Asia, where governments often prioritize surveillance over individual rights. These groups also highlight the impact of digital privacy violations on marginalized communities, such as refugees and activists, who are often the most vulnerable to data exploitation.



This map is from a study made in 2018, countries may have changed their digital privacy policies since the issue of this map.

Timeline of Events

1948 - The Universal Declaration of Human Rights recognizes privacy as a fundamental right

1995 - EU Data Protection Directive adopted

2013 - Edward Snowden Reveals Global Surveillance Programs

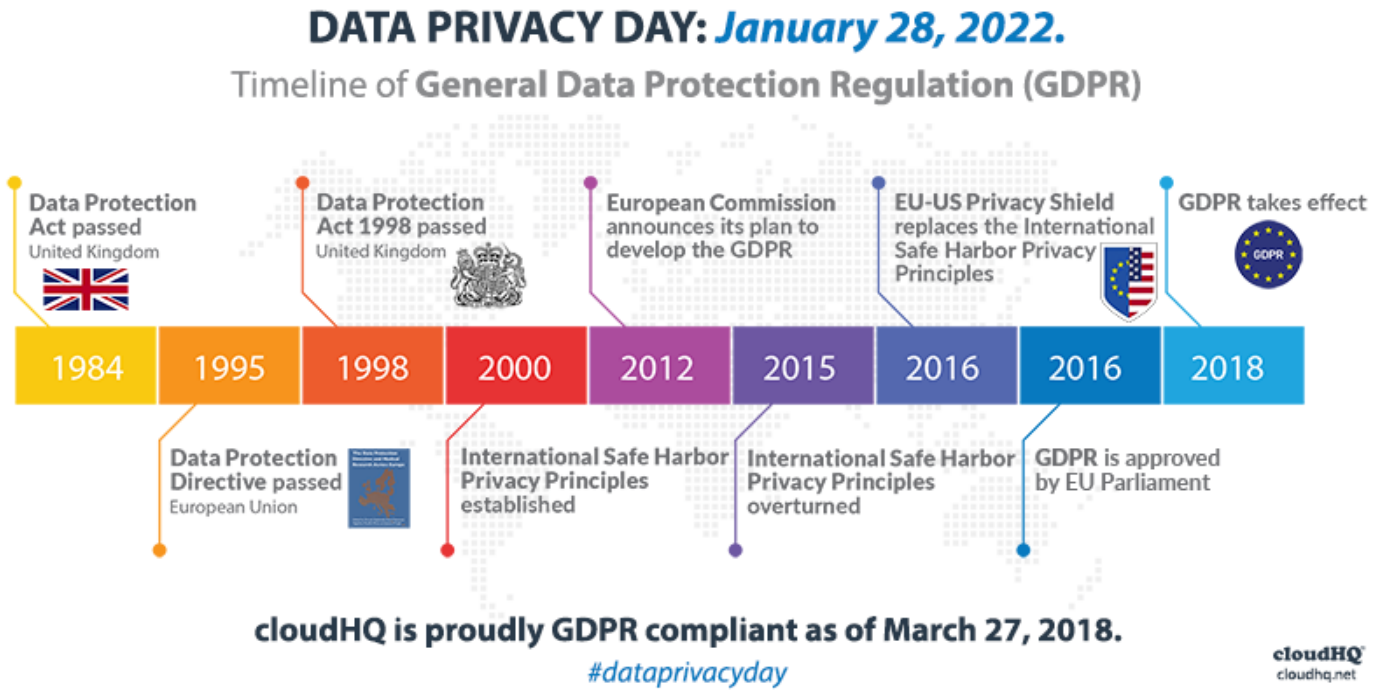
2016 - GDPR adopted by the European Union

2018 - GDPR becomes enforceable; Cambridge Analytica scandal erupts

2020 - California Consumer Privacy Act (CCPA) goes into effect

2023 - AI Act proposed in the EU to regulate artificial intelligence

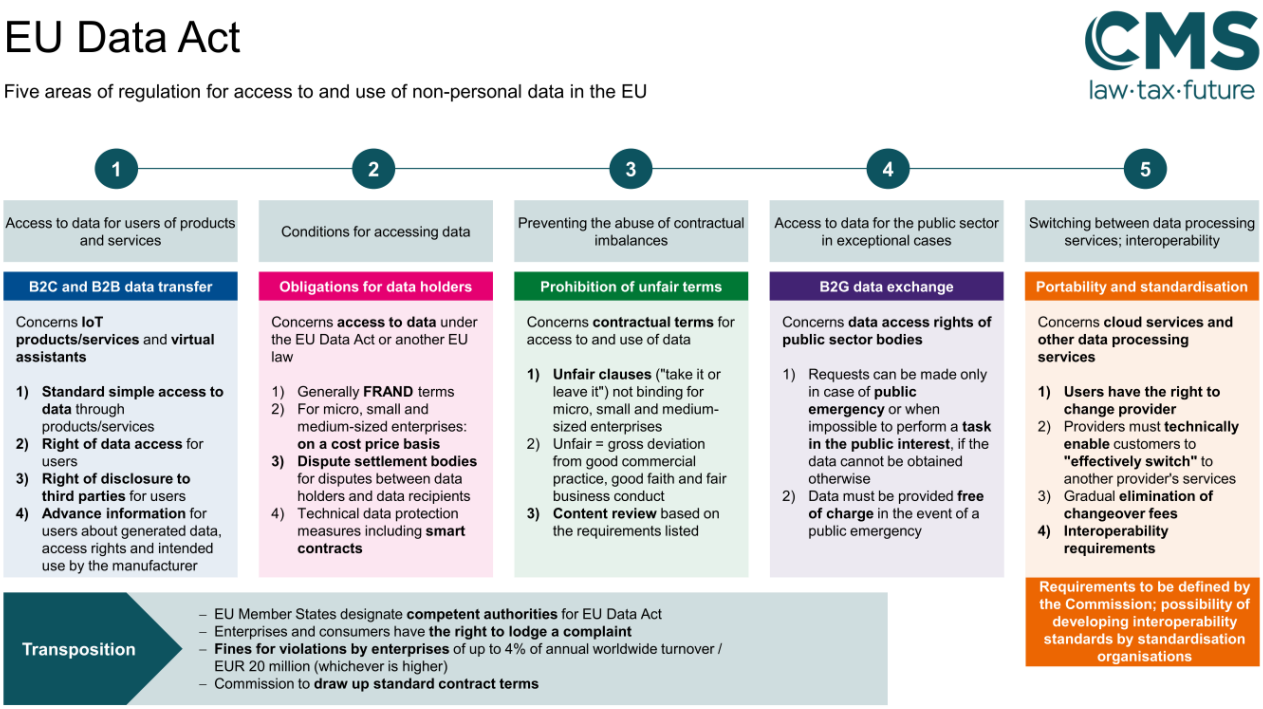
2024 - The EU AI Act passed



Previous Attempts to Solve the Issue

GENERAL DATA PROTECTION REGULATION (GDPR) - 2018

Initiated by the European Union, the GDPR is one of the most comprehensive data privacy frameworks globally. It was designed to harmonize data protection laws across EU member states and grant individuals greater control over their personal data. Key provisions include the right to access, erasure, and data portability, as well as stringent requirements for data minimization and accountability. The GDPR has been largely successful in setting a global benchmark for privacy laws, influencing legislation in countries like Brazil (LGPD) and Japan (APPI). However, its implementation has faced challenges, particularly for small and medium-sized enterprises (SMEs) that struggle with compliance costs. Enforcement is handled by national data protection authorities, such as France's CNIL, which has issued significant fines to companies like Google and Amazon for non-compliance. Public perception of the GDPR is generally positive, as it empowers individuals, but critics argue that its complexity can hinder innovation and create bureaucratic burdens.



CALIFORNIA CONSUMER PRIVACY ACT (CCPA) - 2020

The CCPA was introduced in California as a state-level response to growing concerns about data privacy in the U.S. It grants Californians rights similar to those under the GDPR, including the right to know what personal data is being collected, the right to delete it, and the right to opt out of its sale. The CCPA was spearheaded by privacy advocates and lawmakers in response to high-profile data breaches and scandals like Cambridge Analytica. While it has been praised for increasing corporate accountability and transparency, its effectiveness is limited by its state-level scope, leaving residents of other U.S. states with fewer protections. Enforcement is carried out by the California Privacy Protection Agency (CPPA), which has the authority to impose fines. However, critics note that enforcement has been inconsistent, and the law's complexity has led to confusion among both businesses and consumers. Public perception is mixed, with some applauding its consumer-centric approach and others calling for a more comprehensive federal privacy law.

INDIA'S DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT - 2023

The DPDP Act was introduced by the Indian government to address the growing need for data privacy in one of the world's largest digital economies. It emphasizes data minimization, strict consent protocols, and the establishment of a Data Protection Board to handle grievances and ensure compliance. The act was influenced by global frameworks like the GDPR but tailored to

India's unique socio-economic context. While it represents a significant step forward, the DPDP Act has faced criticism for granting broad exemptions to government agencies, raising concerns about state surveillance. Enforcement is still in its early stages, and challenges such as limited public awareness and resource constraints could hinder its effectiveness. Public perception is cautiously optimistic, with many applauding the move but calling for stronger safeguards against government overreach.

UN GUIDELINES ON DIGITAL PRIVACY

The United Nations has long promoted privacy as a fundamental human right, most notably through Article 12 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). These guidelines emphasize the importance of protecting personal data in the digital age and have inspired national and regional privacy laws. However, the UN's lack of enforcement mechanisms means that adherence is voluntary, leading to significant disparities in privacy protections worldwide. Developing countries, in particular, often lack the resources to implement these guidelines effectively, leaving their citizens vulnerable to data exploitation. Public perception of the UN's role in digital privacy is mixed, with some praising its advocacy and others criticizing its inability to enforce compliance.

WHISTLEBLOWING (EDWARD SNOWDEN, 2013)

In 2013, former NSA contractor Edward Snowden leaked classified documents revealing extensive global surveillance programs operated by the U.S. government and its allies. These revelations sparked widespread public outrage and led to significant policy changes, including the adoption of stronger encryption standards and increased scrutiny of government surveillance practices. Snowden's actions were widely supported by privacy advocates but condemned by governments, which viewed them as a threat to national security. The leaks also exposed the vulnerabilities of international data flows, prompting countries like Germany and Brazil to push for stricter data localization laws. Public perception of Snowden remains polarized, with some hailing him as a hero for exposing government overreach and others labeling him a traitor for compromising national security.

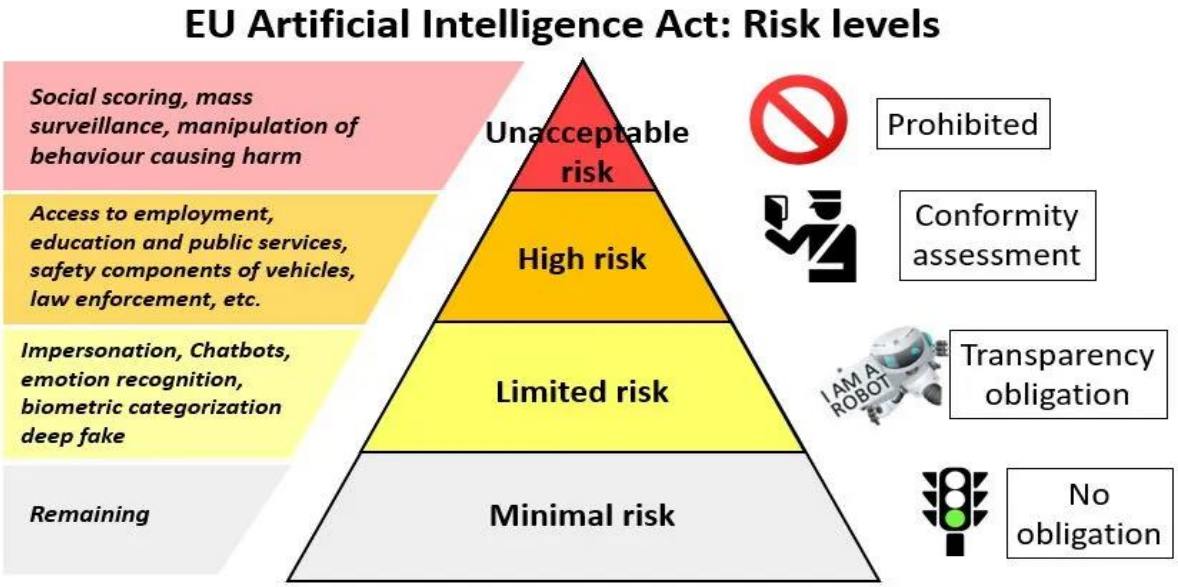
Possible Solutions and Approaches

ADOPT GLOBAL PRIVACY STANDARDS

A solution to the issue at hand could be to create unified international standards, inspired by GDPR, to harmonize privacy protections across borders. It is unjust to live in a world where people are tracked more or less, based on citizenship or geographical location. It is imperative that policies are adopted on a global level, and for such an urgent yet regulatable issue nations must unite regardless of differences and fight back against the exploitation of personal data.

REGULATE AI AND EMERGING TECH

As artificial intelligence is evolving at a never-before-seen pace, countries must start specifying AI regulations in their privacy laws. The European Union for instance just announced recently that it will restrict all 'unacceptable risk' artificial intelligence software. These strict regulations unfortunately can only work if there are serious repercussions for those who chose not to abide. Companies face fines of as much as €35 million or 7% of their global annual revenues — whichever amount is higher — for breaches of the EU AI Act. The fact of the matter is that this fine is even higher than the fines possible under the GDPR, Europe's strict digital privacy law in which companies face fines of up to 20 million euros or 4% of annual global turnover for GDPR breaches.

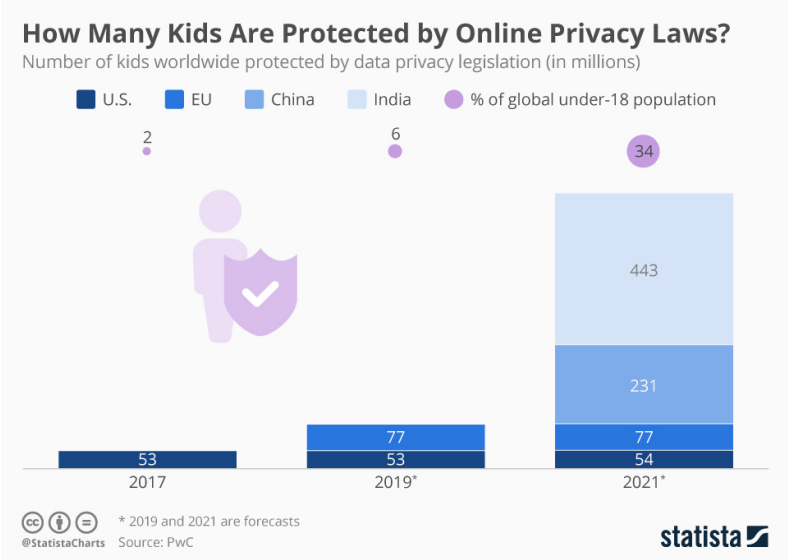


INCREASE TRANSPARENCY

Many users unknowingly consent to extensive tracking due to unclear privacy policies, making increased transparency in data collection essential. It is more than frightening to see the level

of connectedness between these apps. If provided unknowing consent, data starts flowing through all platforms on the user's devices and a hyper detailed profile will be created of the user. Companies should be required to simplify privacy policies with clear language, provide granular consent options, and implement real-time notifications whenever data is accessed or shared.

STRENGTHEN PROTECTIONS FOR MINORS



Children and teenagers are particularly vulnerable to data exploitation, as they generally use platforms much more frequently than their adult counterparts, making stronger privacy protections necessary. This can be addressed through stricter parental consent mechanisms, age-appropriate privacy settings, and complete bans on targeted advertising for minors. Existing laws such as COPPA in the U.S. and the UK's Age-Appropriate Design Code provide frameworks, but enforcement and age verification without excessive data collection remain challenges, especially as currently, it is a breeze to register for an account at any major social media platform and provide an untrue date of birth.

PUBLIC AWARENESS CAMPAIGNS

Public awareness campaigns play a vital role in ensuring privacy protections are effective, as many individuals do not fully understand their rights or digital risks. Educational initiatives should focus on teaching users to read privacy policies, recognize phishing scams, and utilize privacy-enhancing tools like VPNs and encrypted messaging apps. Governments, NGOs, and educational institutions should collaborate on large-scale digital literacy programs, while social media influencers can help reach younger audiences. However, shifting user habits and countering misinformation remain significant obstacles.

Bibliography

Case IQ (2024) A Practical Guide to Data Privacy Laws by Country [2024]. Available at: https://www.caseiq.com/resources/a-practical-guide-to-data-privacy-laws-by-country/ (Accessed: 3 January 2025).

DLA Piper (2024) Law in the United States - DLA Piper Global Data Protection Laws of the World. Available at: https://www.dlapiperdataprotection.com/?t=law&c=US (Accessed: 3 January 2025).

European Data Protection Supervisor (no date) Data Protection. Available at: https://www.edps.europa.eu/data-protection/data-protection_en (Accessed: 3 January 2025).

EU GDPR (no date) General Data Protection Regulation (GDPR) – Legal Text. Available at: https://gdpr-info.eu (Accessed: 3 January 2025).

IAPP (2024) US State Privacy Legislation Tracker. Available at: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (Accessed: 3 January 2025).

Longstaff, G. (2024) 'The importance of data privacy law in the digital age', The University of Law, 11 October. Available at:

https://www.law.ac.uk/resources/blog/the-importance-of-data-privacy-law-in-the-digital-age/ (Accessed: 3 January 2025).

Media Defence (no date) Introduction to Digital Rights - Resource Hub. Available at: https://www.mediadefence.org/resource-hub/introduction-to-digital-rights/ (Accessed: 3 January 2025).

Tableau (no date) Useful GDPR Resources. Available at: https://www.tableau.com/learn/articles/gdpr-resources (Accessed: 3 January 2025).

TechTarget (2024) U.S. data privacy protection laws: 2025 guide. Available at: https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws (Accessed: 3 January 2025).

Wikipedia (2024) General Data Protection Regulation. Available at: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (Accessed: 3 January 2025).

CNBC (2025) 'EU kicks off landmark AI Act enforcement as first restrictions apply', 3 February. Available at: https://www.cnbc.com/2025/02/03/eu-kicks-off-landmark-ai-act-enforcement-as-first-restrictions-apply.html (Accessed: 3 February 2025).

blog.cloudhq.net. (n.d.). Data Privacy Day: A Brief History of GDPR – cloudHQ Blog. [online] Available at: https://blog.cloudhq.net/data-privacy-day-a-brief-history-of-gdpr/.Cms-lawnow.com. (2023).

Disharmony between Data Act and GDPR. [online] Available at: https://cms-lawnow.com/en/ealerts/2023/12/disharmony-between-data-act-and-gdpr.

Securiti Research Team (2024). Data Privacy Laws and Regulations Around the World. [online] Securiti. Available at:

https://securiti.ai/privacy-laws/.Statista Infographics. (n.d.).

Infographic: How Many Kids Are Protected by Online Privacy Laws? [online] Available at: https://www.statista.com/chart/18795/digital-advertising-laws-for-kids/.

The Economist. (n.d.). As GDPR nears, Google searches for privacy are at a 12-year high. [online] Available at: https://www.economist.com/graphic-detail/2018/05/21/as-gdpr-nears-google-searches-for-privacy-are-at-a-12-year-high.

Zandt, F. (2024). Infographic: Who Puts Dampers on Data Protection? [online] Statista Daily Data. Available at: https://www.statista.com/chart/31665/pressure-to-limit-gdpr-compliance/