Forum: Human Rights Commission

Issue: The Question of Digital Privacy and Human Rights in the Age of Surveillance

Student Officer: Hayley Horkan

Position: Assistant President of the Human Rights Commission

Introduction

The question of [1] Digital privacy and human rights in the age of surveillance has long been a well discussed and a difficult topic in human rights and international law. Privacy is a fundamental right for all; Article 12 of the Universal Declaration of Human Rights states that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence.[1] However in the twenty-first century as human life is becoming more dependent on data-driven technologies, this right to privacy is under threat.

As digital technology and surveillance techniques develop, international privacy laws fail to keep up. In response, international organisations and states have attempted to address these challenges. In 2015 The United Nations stated that the right to privacy applies both, online and offline.[2] At the same time, governments have introduced laws, such as the US Privacy Act (1974), the OECD Privacy Guidelines (1980), and EU data protection laws, which later developed into the General Data Protection Regulation (GDPR) in 2018, to protect personal data. Despite these efforts, the rapid development of digital technology and surveillance continues to outpace existing legal protections.

[1] Universal Declaration of Human Rights | United Nations
[2] Amount of Data Created Daily (2025)

Definition of Key Terms

Encrypted

Encryption is the process of protecting information by converting it into unreadable code using mathematical algorithms and a secret key so only authorized parties can access the original data[3]

Mass Surveillance

Mass surveillance is the large-scale, systematic monitoring and collection of data about people's activities, communications, or behavior, often done by governments or organizations.[4]

Sensitive data

Sensitive data is personal information that, if exposed or misused, can cause serious harm to an individual, such as identity theft, discrimination, or financial loss.[5]

AI

Artificial Intelligence is a rapidly developing technology that enables computers to simulate autonomous human learning, comprehension and decision making.

Metadata

Metadata is data that describes other data. It provides information like what the data is, how it was created, when, by whom, and how it should be used.[6]

Biometric data

Biometric data is data based on unique physical or behavioral characteristics of a person. It is used to identify or verify someone's identity. Biometric data can for example be fingerprints, facial recognition data, iris scans, and voice patterns.[7]

Background

The question of Digital privacy in the age of surveillance refers to the challenge of protecting individuals' personal information, communications, and online behavior, in a world where data is constantly collected, monitored, and analyzed by governments, corporations, and other organizations. Digital privacy refers to an individual's right to control their personal information as they access the

[3] Encryption - Wikipedia
[4] Mass surveillance - Wikipedia
[5] Mass surveillance - Wikipedia
[6] Metadata - Wikipedia
[7] What is Biometric Data? - Securiti

internet. It is often divided into three categories: information privacy which is the ability to control your sensitive data, communication privacy which ensures that messages and calls stay private, and individual privacy of your identity. Digital privacy ensures that people can think, express themselves and communicate without fear of constant monitoring and misuse of their personal information. Every time an individual uses their phone, computer or other electronic device, data is being collected. Some data is collected directly, for example when you create an account, make a purchase or post on social media. Other data is collected automatically through cookies[8], location services and logs of browsing app usage. Finally, data can be collected indirectly when companies buy data or analyse data using algorithms.[9] Most modern data protection laws prohibit certain types of data collection called “sensitive data”. Sensitive data is for example biometric data, health information, sexual orientation or health related data.[10] Many countries around the world have weak laws to support digital privacy, prime examples of these kinds of countries are China, Russia and Malaysia.

Data storage is typically divided into different types: physical, digital, database and cloud based storage.[11] Physical, also known as direct data storage, is data that is directly saved on devices, for example, photos can be directly stored onto a device. Digital data is stored in remote servers that are usually managed by companies, an example of digital data storage would be school records. Sometimes data is stored in databases, which are a specific genre of software, designed to store data efficiently, as it can be written and retrieved very fast, while always maintaining its integrity. A core feature of modern databases is the ability to cross reference and correlate information through direct and more subtle relational structures. There are a variety of common database designs in use today ranging from traditional relational databases to graph databases, and many types that focus on the storage and management of unstructured data.[12] Cloud-based data storage is a method of saving data over the internet instead of on your own computer or a local server. The data is stored on remote servers managed by companies, such as Google, Amazon (AWS), or Microsoft (Azure), and you can access it from anywhere using a device with an internet connection.[13]

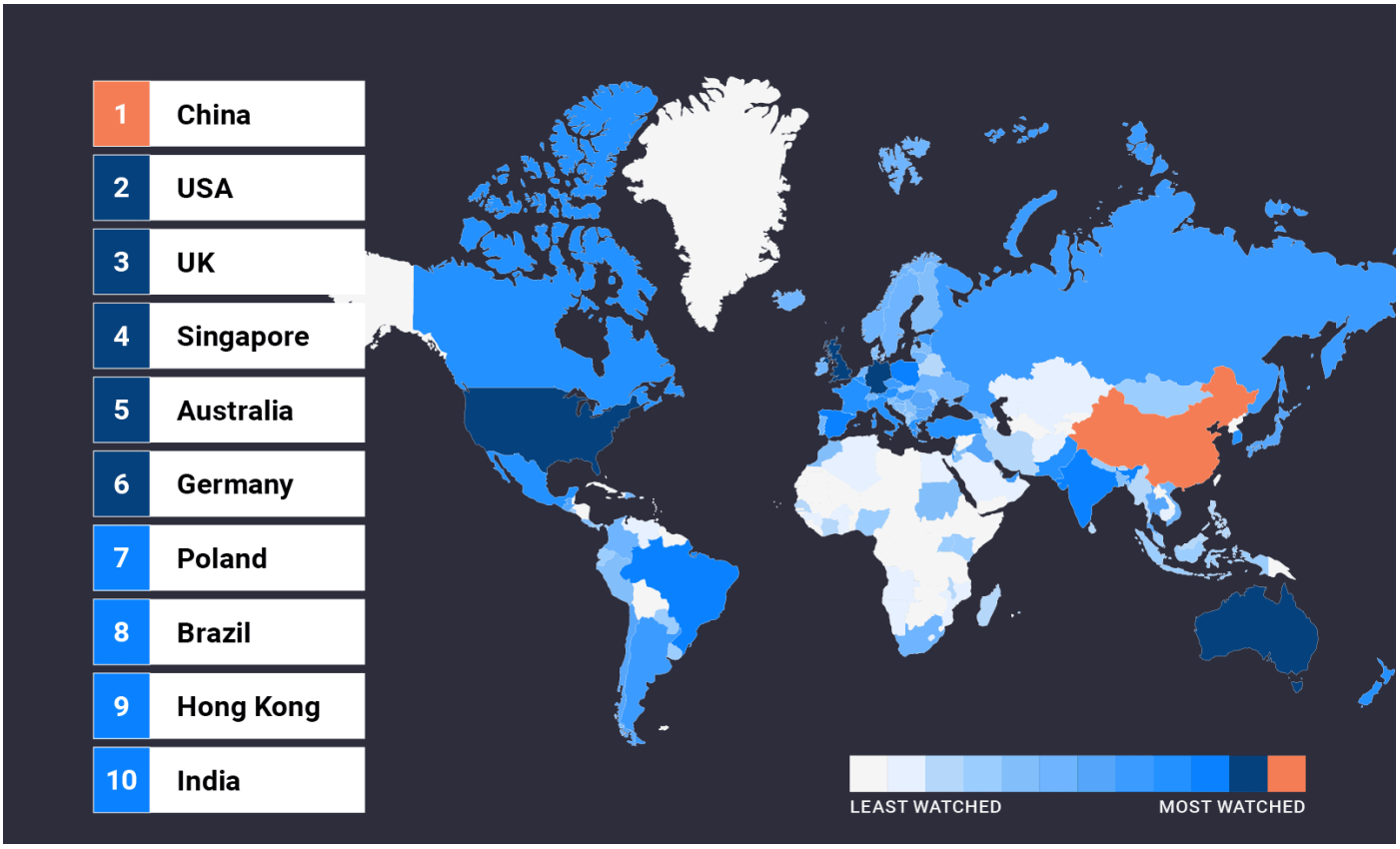
[8] HTTP cookies
[9] Data storage What is data storage: methods, types, and devices to store
[10] What personal data is considered sensitive? - European Commission
[11] What is data storage: methods, types, and devices to store
[12] Database
[13] Cloud storage

Sensitive data should be encrypted, but that is not always the case. Insufficient or poorly managed storage can be dangerous because it increases the risk of data leaks, making it easier for hackers or unauthorized parties to access sensitive information.[14] Even with laws like GDPR and other privacy regulations, weaknesses in storage systems can put personal data at risk if organizations fail to implement proper security, encryption, and access controls. Many companies buy or trade personal data collected from users, often without individuals fully knowing what information is being shared or sold. Data brokers are companies that specialize in collecting and selling data.[15] They create detailed profiles that can include interests, buying habits, demographics, location, and more. Other businesses purchase these profiles to target advertisements, assess credit or insurance risk, or for other marketing and analytics purposes. In Europe GDPR sets some limits on how data can be collected, shared, or sold, requiring clear consent and giving individuals rights to access or opt out of data processing.[16] In the USA on the other hand there are no federal laws prohibiting data brokers, so they can legally collect and sell much information without restrictions in almost all states.[17] Even when legal, these practices raise concerns about privacy. Data brokers can inform data collection in cookies and tracking pixels many people don't understand or read. This leads to individuals often not knowing how much information is collected about them or how it is used.

The rapid technological advancements in AI and algorithm analytics have had a huge impact on digital privacy and surveillance. With AI it is possible to mass analyse data, create profiles on individuals and figure out personal information based on their social media activities, browsing, or photos. Data that wasn't considered sensitive can reveal personal information with the help of AI.[18] AI also has a huge impact on mass surveillance. AI can easily process, and analyse vast amounts of personal information far more quickly and deeply than humans could. AI-powered surveillance technologies, such as facial recognition, location tracking, and behaviour analysis, can constantly monitor people in public and private spaces without explicit consent, raising concerns about privacy invasion and loss of anonymity.[19] AI systems are also often opaque, meaning individuals may not know how decisions about them are made or how their data is used.

[14] What is encryption? | IBM
[15] Data broker - Wikipedia
[16] Is buying data legal and GDPR compliant? - GDPR Local
[17] Data protection laws in the United States - Data Protection Laws of the World
[18] The Authoritarian Risks of AI Surveillance | Lawfare
[19] How AI can enable public surveillance | Brookings

Advances in the internet, mobile communications, AI, and big data analytics have enabled surveillance on an unprecedented scale, often without the knowledge of people. Mass surveillance refers to the widespread, indiscriminate monitoring and collection of data on large populations.[20] While governments often justify mass surveillance for national security or crime prevention, it raises serious concerns about digital privacy because individuals may be monitored without consent or knowledge. Mass surveillance is especially bad in China where the streets are equipped with millions of face recognizing CCTV cameras.[21] Laws like GDPR and international human rights frameworks attempt to regulate surveillance practices, but the rapid development of digital technologies outpaces legal protections.

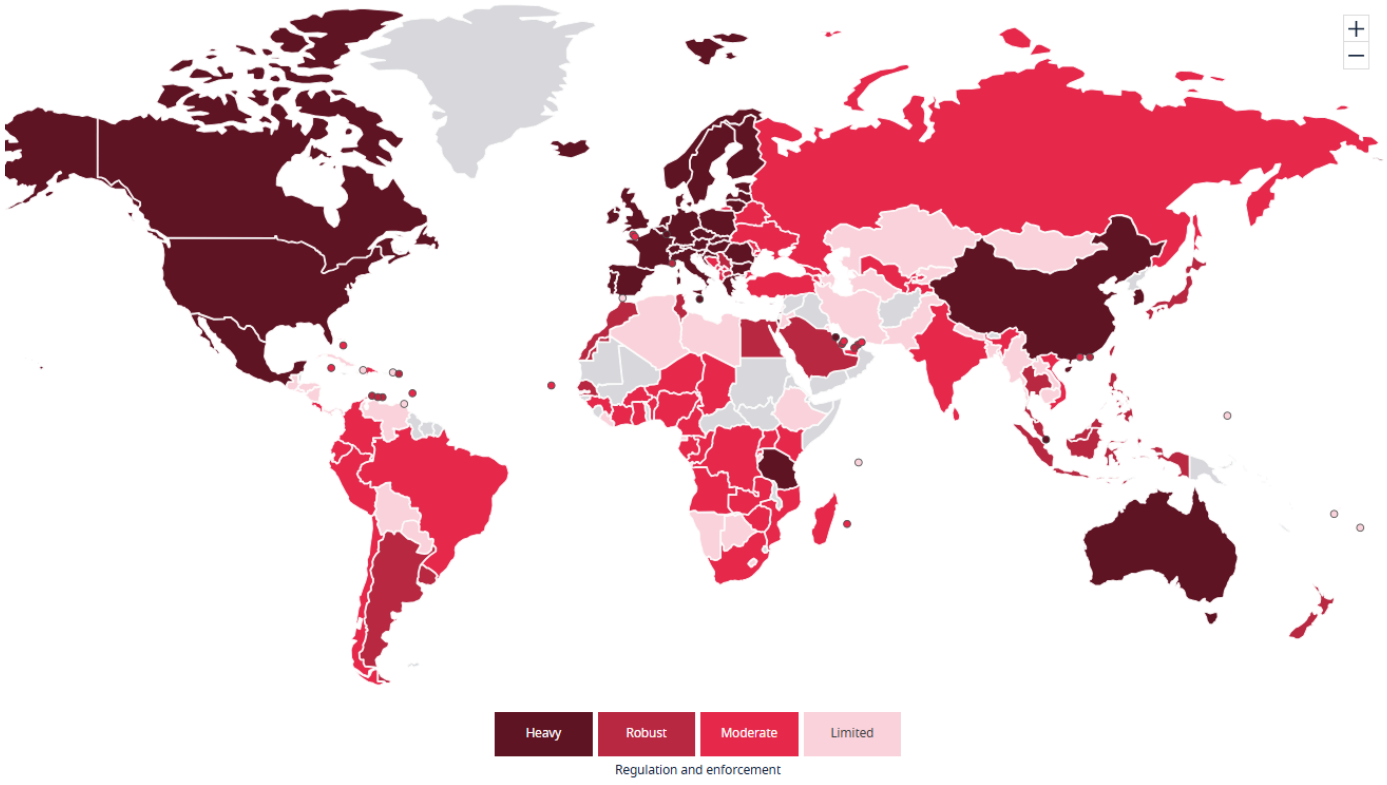


Map showing countries with the most surveilled citizens in 2022

Between many countries significant legal and regulatory gaps remain, data protection laws vary

[20] Mass surveillance
[21] Internet censorship and surveillance by country

widely between countries, enforcement can be weak, and some states lack comprehensive regulations altogether. Third world countries struggle especially with digital privacy.[22] The lack of education on digital literacy means that people don't understand what are their rights and what they might agree to whilst being on the internet. [23] Laws protecting personal data are often outdated, incomplete, or loosely applied, leaving citizens vulnerable to misuse of their information by both private companies and governments. [24] Widespread surveillance, sometimes used for political control, further threatens individual freedoms, as social media and digital communications can be monitored without oversight. This not only complicates data flow between countries, but also endangers human rights of privacy.



Map showing country my country how heavy regulations for data protection is

[22] Data Protection Regulation in the Global South | Carnegie Endowment for International Peace
[23] Digital Skills in the Global South: Gaps, Needs, and Progress
[24] Data and privacy unprotected in one third of countries, despite progress | UN Trade and Development (UNCTAD)

Key Member States and NGOs Involved and Their Views

European union

The European Union plays a central role in shaping global standards on digital privacy. In article 7 of the EU charter of fundamental rights it is stated that everyone has the right to privacy, and article 8 that everyone has the right for their data to be protected [25]. One of the EU's most significant contributions to digital privacy is the GDPR. The GDPR was created in 2016, but was put into force in 2018. As technology surpassed the, the EU recognized that their old privacy laws have a need for an update to include the digital world.[26] The GDPR sets strict rules on how personal data may be collected, processed, stored, and shared by both governments and private companies. It emphasizes user consent, imposes the mandatory use of technical safeguards like encryption, and grants individuals the rights such as access to their data, correction, erasure and the ability to challenge misuse. The GDPR has a big global effect, as it applies not only within the EU but also to non-EU entities that process the data of EU residents.[27] The Court of Justice of the European Union (CJEU) and recently The European AI act have worked actively against mass surveillance by such as limiting biometric surveillance, banning manipulative systems, social scoring, and untargeted scraping for facial databases.[28]

United States of America (USA)

The United States of America is a complex digital privacy landscape. Unlike in the EU, the United States doesn't recognize digital privacy as a fundamental human right.[29] However, the US does have a number of largely sector-specific privacy and data security laws at the federal level and state level.[30] For example the California Consumer Privacy Act (CCPA) is much like the GDPR and grants the rights for individuals such as the right to access their data, the right to erase data and the right to non-discrimination. In 2023 the right to correct and limit data was also added.[31] Although some states have digital privacy laws much like in the EU, a comprehensive nationwide digital privacy framework comparable to the EU's GDPR does not yet exist in the USA.

The USA Patriot Act, passed in 2001 after the September 11 attacks. This significantly expanded

[25] Charter of fundamental rights of the European union
[26] What is GDPR, the EU's new data protection law?
[27] Does the GDPR apply to companies outside of the EU? - GDPR.eu
[28] EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act
[29] Data protection laws in the United States - Data Protection Laws of the World
[30] Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance
[31] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

U.S. government surveillance powers by lowering legal barriers to collecting and sharing personal data in the name of national security and counterterrorism.[32] Following the patriot act programs managed by the National Security Agency (NSA) expanded largely, collecting and analyzing massive amounts of digital communications, including emails, phone metadata, internet traffic, and social media activity. The USA patriot act essentially expired on march 15th 2020 when congress failed to renew section 215 which allowed bulk collection of phone metadata. Although some parts of the patriot act were made permanent, so they remain in force for law enforcement and counterterrorism purposes.[33] Surveillance programs such as PRISM and Upstream, created during the Patriot Act era, continue to operate under updated legal authorities. Mass surveillance in the USA is well hidden, but mostly operates under Section 702 of the Foreign Intelligence Surveillance Act (FISA). Section 702 of FISA allows the government to collect electronic communications in bulk from foreign targets.[34]

Russia

Digital privacy in Russia is very limited.[35] In 2016 the yarovaya law was put into place, which requires telecommunications providers and internet companies to provide users metadata and to provide encryption keys and data to security agencies upon request. [36]SORM is the System for Operative Investigative Activities, an infrastructure created by the Russian government to give the state extensive access to personal information.[37]

SORM-1 was introduced in 1995 and is designed to monitor telephone and traditional landline communication methods. SORM-1 requires telecommunication operators to install hardware provided by the Federal Security System (FBS) allowing the agency to monitor users' metadata. In 1998 SORM-2 was introduced as a reaction to the development in technology. SORM-2 enables the FSB to monitor internet traffic, emails, messaging apps, and web activity. The most recent iteration; SORM-3, expands surveillance to cover modern digital communications comprehensively, including mobile networks, encrypted messaging apps, and cloud services. Because SORM operates independently of service providers and with limited judicial review, individuals have little control over who accesses their personal data or how it is used. This allows mass surveillance to be very routine and individuals' can be closely monitored by the state.[38]

---

[32] Patriot Act
[33] Patriot Act Repeal:What Expired and What Remains? - LegalClarity
[34] Warrantless Surveillance Under Section 702 of FISA | American Civil Liberties Union
[35] Data protection laws in Russia - Data Protection Laws of the World
[36] Yarovaya law
[37] SORM
[38] Russia: Internet Blocking, Disruptions and Increasing Isolation | Human Rights Watch

China

China's mass surveillance system commonly referred to as the skynet, which is a large scale video surveillance system that is composed from millions of CCTV cameras making it the most widespread and advanced mass surveillance systems in the world.[39] These CCTV cameras are equipped with biometric facial recognition and AI analytics and monitor streets, public transportation and residential areas. This surveillance system was introduced and justified by China's government as a project to prevent crime and maintain public order.[40] Though this surveillance is primarily conducted by the government, private companies do also take part in it.[41]

Unlike in the EU, Digital privacy in China is limited and heavily influenced by the state's emphasis on national security, social stability, and cyber sovereignty. While China has introduced modern data protection laws such as the Personal Information Protection Law and the Data Security Law, these frameworks primarily regulate how companies handle personal data and do not significantly restrict government access.[42] Broad security laws, such as the Cybersecurity Law, grant authorities extensive powers to collect, monitor, and analyze digital information.[43]

Timeline of Events

1948	The Universal Declaration of Human Rights establishes privacy as a fundamental human right. [44]
1960s	Early computer networks emerged, and governments began experimenting with electronic monitoring for national security and intelligence purposes. [45]
1973	Sweden passed the Data Act, the world's first law to regulate personal data processing and require licensing for systems handling personal data, laying an early foundation for digital privacy protection

[39] Operation Sky Net - Wikipedia
[40] China announces expansion of Sky Net and long-arm policing_0.pdf
[41] Mass Surveillance in China | Human Rights Watch
[42] Internet censorship in China - Wikipedia
[43] The Invisible Risks of Insecure Chinese Surveillance Cameras – chinaobservers
[44] A Brief History of the Internet
[45] Data Protection Law: How It All Got Started - Data Catalyst

	worldwide.[46]
1980	OECD privacy guidelines established the first international framework for world data privacy. By for example setting principles that explain how personal data should be collected, used and protected.[47]
1981	The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also known as the Convention 108 was held. Convention 108 created a framework for countries to cooperate internationally on data protection.[48]
1995	The EU Data Protection Directive was the first comprehensive European law regulating the processing of personal data across EU member states.[49]
2000	Global expansion of digital surveillance. Governments around the world invest in surveillance infrastructure, including CCTV, telecom monitoring, and internet surveillance, often justified by national security and counterterrorism objectives.
2013	Edward Snowden, a former NSA member revealed that the NSA was conducting mass surveillance which led to world wide reforms in privacy laws. [50]
2018	The GDPR became law over European countries. Significantly increased individuals digital privacy and decreased government surveillance.[51]
2023	India's digital personal data protection act is a set of laws that regulate how organizations collect, use,

[46] Origins, history and evolution of European Data Protection and Privacy | Purpose and Means
[47] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data | OECDOECD
[48] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
[49] Data Protection Directive - Wikipedia
[50] Snowden effect - Wikipedia
[51] General Data Protection Regulation - Wikipedia

	store, and share personal data, ensuring privacy, consent, security, and user rights while holding data handlers accountable.[52]
2024	The European AI act is introduced. The world's first comprehensive legal framework regulating AI systems, such as the requirement of transparency and traceability.[53] This act protects digital privacy by restricting high risk AI systems such as biometric surveillance and requires human oversight. The AI act will be fully put in place by 2027.[54]

UN Involvement, Relevant Resolutions, Treaties, and Events

International human rights organizations have consistently expressed concern over the erosion of digital privacy in the age of surveillance. In recent years, leading UN bodies and experts have repeatedly urged governments to limit mass surveillance practices, uphold the right to privacy, and ensure accountability for violations of fundamental human rights. They have emphasized the need for stronger legal frameworks to protect individuals from unlawful data collection and misuse.

- The document on International Principles on the Application of Human Rights to Communications Surveillance launched at the UN Human Rights Council (UNHRC) by the Electronic Frontier Foundation[(EFF), 10 July 2013 [55]
- General Assembly, Human Rights Council on the right to privacy in the digital age, 1 April 2015 **(A/HRC/RES/28/16)** [56]
- General Assembly adopted resolution concerning the right to privacy in the digital age, 25 January 2017 **(A/RES/71/199)** [57]
- United Nations Convention against Cybercrime, 24 December 2024 [58]

[52] Data protection laws in India - Data Protection Laws of the World
[53] Article 5: Prohibited AI Practices | EU Artificial Intelligence Act
[54] The timeline of implementation of the AI Act
[55] International Principles on the Application of Human Rights to Communications Surveillance
[56] A/HRC/RES/28/16 General Assembly
[57] A/RES/71/199 General Assembly
[58] United Nations Convention against Cybercrime

Possible Solutions

Finding solutions for the Question of Digital Privacy and Human Rights in the Age Surveillance is a challenging task. Technology keeps developing faster than laws can follow and the problems within digital privacy and mass surveillance are multilayered and multitudinal. In order to create digital privacy laws that work across countries, laws must be developed alongside technology. Laws need to completely reconstruct how data is stored and moved, so that it all supports digital privacy. Lastly it is exceedingly important to increase digital literacy in general people, so that the general public understands terms that they are agreeing to.

Data protection laws need to be strengthened

Although several countries and jurisdictions have established relatively good data protection frameworks, such as the GDPR in the European Union, the CCPA in the United States, and the Digital Personal Data Protection Act (DPDP) in India, many regions still lack comprehensive privacy legislation. Stricter laws regarding data harvesting and monetizing data should be established nationwide. Mandatory financial audits to ensure transparency and lawful use of data should be put in place.[59] These laws need stronger enforcement, international cooperation, and heavier penalties for non-compliance.

The structure of data storing has to be changed

Privacy-by-design is a proactive approach to data protection that requires privacy safeguards to be built into technologies and systems from the outset, rather than added after deployment.[60] Privacy-by-design essentially requires companies to apply encryption immediately upon data collection. [61] This increases digital privacy by reducing the traceability of data back to an individual. This protects the digital privacy of individuals in general and in data breaches. In order to safeguard data privacy-by-design, the approach has to be implemented universally. Companies should have mandatory data audits ensuring that personal data is processed lawfully, securely, and only for defined purposes, while identifying risks such as excessive data retention or unauthorized access.

Increase Cross jurisdictional cooperation

Cross-jurisdictional cooperation is essential for effective data protection in a globalized digital environment, as personal data routinely crosses national borders through cloud services, social media

[59] Finance's Evolving Role in Safeguarding Sensitive Data | BDO
[60] Privacy by Design - General Data Protection Regulation (GDPR)
[61] Privacy by design

platforms, and international corporations. Without cooperation between states, companies can exploit legal gaps by storing or processing data in countries with weaker privacy regulations, undermining existing protections. To address this, governments should establish international agreements and mutual assistance mechanisms that allow regulatory authorities to share information, coordinate investigations, and enforce penalties across borders, for example, by creating joint oversight frameworks for multinational technology companies.

Increase digital literacy

Both education and workplaces should emphasize and invest into educating people about digital privacy, data protection and mass surveillance. People should know what their rights are when it comes to their data, and what kind of surveillance they are agreeing to whilst, for example, pressing yes to cookies

Bibliography

1. Universal Declaration of Human Rights | United Nations 22.12
2. Amount of Data Created Daily (2025) 22.12
3. Encryption - Wikipedia 22.12
4. Mass surveillance - Wikipedia 22.12
5. Metadata - Wikipedia 11.1
6. What is Biometric Data? - Security 11.1
7. What is data storage: methods, types, and devices to store 26.12
8. What personal data is considered sensitive? 26.12
9. What is data storage: methods, types, and devices to store 26.12
10. Database - Wikipedia 26.12
11. Cloud storage - Wikipedia 26.12
12. What is encryption? | IBM 26.12
13. Data broker - Wikipedia 27.12
14. Is buying data legal and GDPR compliant? - GDPR Local 27.12
15. Data protection laws in the United States - Data Protection Laws of the World27.12
16. The Authoritarian Risks of AI Surveillance | Lawfare 27.12
17. How AI can enable public surveillance | Brookings 27.12
18. Mass surveillance - Wikipedia 27.12
19. Internet censorship and surveillance by country - Wikipedia 27.12

20. Data Protection Regulation in the Global South | Carnegie Endowment for International Peace 27.12
21. Digital Skills in the Global South: Gaps, Needs, and Progress 27.12
22. Data and privacy unprotected in one third of countries, despite progress | UN Trade and 27.12
23. Development (UNCTAD) 27.12
24. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION 27.12
25. What is GDPR, the EU's new data protection law? 27.12
26. Does the GDPR apply to companies outside of the EU? - GDPR.eu 27.12
27. EU AI Act 27.12
28. Data protection laws in the United States - Data Protection Laws of the World 27.12
29. Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance 27.12
30. California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the 27.12
31. Attorney General 27.12
32. Patriot Act - Wikipedia 27.12
33. Patriot Act Repeal:What Expired and What Remains? - LegalClarity 27.12
34. Warrantless Surveillance Under Section 702 of FISA | American Civil Liberties Uni 27.12
35. Data protection laws in Russia - Data Protection Laws of the World 27.12
36. Yarovaya law - Wikipedia 27.12
37. SORM - Wikipedia 27.12
38. Russia: Internet Blocking, Disruptions and Increasing Isolation | Human Rights Watch 27.12
39. Operation Sky Net - Wikipedia 27.12
40. China announces expansion of Sky Net and long-arm policing_0.pdf 27.12
41. Mass Surveillance in China | Human Rights Watch 27.12
42. Internet censorship in China - Wikipedia 27.12
43. The Invisible Risks of Insecure Chinese Surveillance Cameras – chinaobservers 27.12
44. A Brief History of the Internet 28.12
45. Data Protection Law: How It All Got Started - Data Catalyst 28.12
46. Origins, history and evolution of European Data Protection and Privacy | Purpose and Means28.12
47. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data | OECDOECD 28.12
48. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - Wikipedia 28.12
49. Data Protection Directive - Wikipedia 28.12
50. Snowden effect - Wikipedia 28.12

51. General Data Protection Regulation - Wikipedia 28.12
52. Data protection laws in India - Data Protection Laws of the World 28.12
53. Article 5: Prohibited AI Practices | EU Artificial Intelligence Act 27.12
54. The timeline of implementation of the AI Act 28.12
55. International Principles on the Application of Human Rights to Communication Surveillance 25.01
56. Finance's Evolving Role in Safeguarding Sensitive Data | BDO 28.12
57. Privacy by Design - General Data Protection Regulation (GDPR) 26.12
58. Privacy by design - Wikipedia 26.12

Photo

1. Who has the most CCTV in the world? The world's most watched people
2. Data Protection Laws of the World Resource | Embedding Project.