SERIES ON DIGITAL RIGHTS AND INTERNET FREEDOM

Topic 6: Surveillance and Privacy

Greater Internet Freedom

The Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University

August 2023

Surveillance and Privacy

Author: The Centre for Intellectual Property and Information Technology Law (CIPIT).

Acknowledgements: We would like to express our gratitude to the Centre for Intellectual Property and Information Technology Law (CIPIT) acknowledging, Florence Ogonjo, Joshua Kitili, Lilian Olivia Orero, Doreen Aoko Abiero, Josephine Kaaniru, and Dan Allan Kipkoech who prepared this learning material. The CIPIT team authored this material in close consultation with the Greater Internet Freedom team at Internews, including Sigi Waigumo Mwanzia, Digital Rights Advisor, and Olga Kyryliuk, Technical Advisor on Internet Governance and Digital Rights.

Copy-Edited by: Internews.

Design & Layout by: CIPIT.

Strathmore University
Centre for Intellectual Property and Information Technology Law

Internews

About CIPIT	About GIF
The Centre for Intellectual Property and Information Technology Law (CIPIT) is an evidence-based research and training Centre based at Strathmore University, Nairobi, Kenya. CIPIT was established in 2012 and focuses on studying, creating, and sharing knowledge on the development of intellectual property and information technology utilizing diverse methodological approaches to inform debates on ICT applications and regulation.	The Greater Internet Freedom Project (GIF) is a three-year, consortium-based, global program implemented by Internews and the GIF consortium across 39 countries. GIF places regional and local organizations at the forefront of the fight to preserve an open, reliable, secure, and interoperable Internet – and, by extension, protects the citizens, civic actors, journalists, and human rights defenders who rely on it to realize fundamental freedoms.

Table of Contents

Introduction

The CIPIT and the GIF have developed exploratory material relevant to pertinent digital rights and internet freedom topics. The 'Surveillance and Privacy' topic examines the state of surveillance globally and its impact on individuals' rights to privacy. It delves into the different forms of surveillance including communications surveillance, government-led digital surveillance, Internet and social media surveillance and monitoring, biometric identification surveillance. It also explores pertinent privacy issues in the digital age, including data breaches privacy policies and consent, browser fingerprinting, and social engineering.

Surveillance is the act of gathering and analyzing data about populations in order to regulate their actions, and can either be conducted legally or illegally by States, private actors, such as Internet Service Providers (ISPs), or by individuals.[1] On the other hand, privacy, in its varied variations, is commonly defined as the "right to be let alone, or freedom from interference or intrusion."[2] Online surveillance is therefore a threat to privacy especially when personal data is obtained without an individual's consent or authorization.[3]

The intersection of privacy and surveillance encapsulates the delicate balance between personal autonomy and the monitoring of individuals' activities. Technological advancements have enabled widespread data collection by state and private actors, leading to concerns about the erosion of individual privacy.

Surveillance involves carefully observing, documenting, and classifying data relating to individuals, procedures, and organizations.[4] Common modern examples of surveillance include the use of CCTV cameras with facial recognition software in public places to prevent terrorism and crime, the deployment of full body scanning technology at airports, and the use of biometric passports featuring digital fingerprint data for citizen control.[5]

A key feature of surveillance is the gathering of personal or sensitive personal data connected to individuals, such as communications data.[6] Generally, surveillance is data-dependent, often resulting in the breach of individuals' right to privacy where data is shared and transferred illegally or where organizations collect information that they do not require. Surveillance exhibits a strong connection with censorship, as it allows entities to observe content prior to implementing censorship measures. This practice is frequently employed to suppress the expression of unrestricted opinions.

Important Note

"Public surveillance undoubtedly entails substantial human rights risks and can substantially undermine the right to privacy. It is thus essential that States resorting to the use of public surveillance assess the potential human rights impacts of their actions and strictly ensure compliance with international human rights law, which requires that any such interference or restriction be based in law, necessary to achieve a legitimate aim and proportional. Current public surveillance measures often fail to meet those requirements."

Source: Office of the United Nations High Commissioner for Human Rights.

Key Terms

Term	Definition/Explainer
Digital Surveillance	The use of the "Internet or Internet-enabled technologies and services… not literally to watch people, but to gather and crunch data about them - because of what one might control or gain by doing so."[7]
Surveillance	Surveillance is the act of gathering and analyzing data about populations in order to regulate their actions.[8]
Privacy	The "right to be let alone, or freedom from interference or intrusion."[9] The right to privacy is protection against arbitrary interference with an individual's privacy, family, home or correspondence, and provides for the right to the protection of the law against interference or attacks.[10]

Surveillance and Privacy: International Instruments

Insufficient policy, legal, and institutional frameworks capable of staying abreast of rapid technological progress represent a major hurdle in the realm of surveillance. Globally, more than '150 countries and self-governing jurisdictions and territories have enacted legislation to secure the protection of personal data held by private and public bodies.'[11]

Resource: OHCHR Annual Thematic Reports

Annual thematic reports of the UN Special Rapporteur on the Right to Privacy: *these canvass emerging privacy issues, including examining how surveillance impacts the protection of the right to privacy and data protection. The reports are presented by the Special Rapporteur to the UN Human Rights Council and the UN General Assembly.*[12]

Source: Annual Thematic Reports, OHCHR.

Globally, the right to privacy is guaranteed and protected under Article 12 of the Universal Declaration of Human Rights (UDHR), and legal force is granted through Article 17 of the International Covenant on Civil and Political Rights (ICCPR). These provide for protections against arbitrary interference with individuals' privacy, family, home or correspondence and provide for the right to the protection of the law against such interference or attacks.

While the international human rights law framework requires States to protect, promote, and fulfill the right to privacy, the right to privacy is **not absolute,** meaning there are circumstances whereby States can limit this right. In the surveillance context, privacy protections do not always guarantee protection against unnecessary and disproportionate surveillance since many governments justify surveillance under the guise of national security, public interest, public health or safety, public order, and the provision of public services. Concerningly, in many GIF countries, national/public security is prioritized over individuals' privacy.[13]

Table 1: Selected Resources - Right to Privacy, International Instruments

Global Instruments
Convention on the Rights of the Child, 1989
Convention on the Rights of Persons with Disabilities, 2006
International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990
International Covenant on Civil and Political Rights (ICCPR), 1966
Universal Declaration of Human Rights (UDHR), 1948
Africa: Regional Instruments
African Charter on Human and Peoples' Rights (ACHPR), 1986
African Charter on the Rights and Welfare of the Child, 1990
AU Data Policy Framework 2022
Resolution on Business and Human Rights in Africa - ACHPR/Res.550 (LXXIV) 2023
Asia: Regional Instruments
Association of Southeast Asian Nations (ASEAN) Human Rights Declaration, 2009
Balkans (Europe): Regional Instruments
General Data Protection Regulation (GDPR) 2018
Charter of Fundamental Rights of the European Union, 2009
Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, or ECHR), 1953
Latin America and the Caribbean: Regional Instruments
American Declaration of the Rights and Duties of Man (1948)
American Convention on Human Rights (1969)
Inter-American Democratic Charter (2001)

Table 2 below outlines the high-level obligations and responsibilities of States and business enterprises respectively, in the context of surveillance, noting that this should

adhere to the three-part test under international law.[14] Specifically, these activities should be legal, strictly necessary, proportionate, and pursue a legitimate aim.[15] Surveillance and censorship are linked, with the knowledge or perception that one is being surveilled encouraging or resulting in self-censorship.

Table 2: Selected Resources - States Obligations and Business Enterprise Responsibilities

States	Business Enterprises
Enact overarching framework protecting against undue interference ● Establishing the criteria for the handling of personal information by both governmental bodies and private entities guided by principles of data protection which include: ○ Lawfulness, ○ Fairness & transparency, ○ Purpose limitation, ○ Data minimisation, ○ Accuracy, ○ Storage limitation, ○ Integrity and confidentiality; and ○ Accountability. ● The law should be publicly accessible ● Frameworks should cover State requests to business enterprises. **Institute procedural safeguards and oversight for surveillance and communications interception** ● State surveillance-related activities must be conducted on the basis of a law. ● Any secret surveillance should be strictly necessary and proportional. It should be limited to the prevention and investigation of serious crimes and be for a limited	**Respect all internationally recognized human rights:** ● Respect human rights in dealings and business relationships, including privacy frameworks. ● Uphold data protection principles when handling personal and special forms of data.

duration. **Promote and prioritize transparency and oversight** ● Surveillance measures and data requests to business enterprises and data-sharing, should be authorized, reviewed and supervised by independent bodies. ● Procedures should be transparent and open for public scrutiny.	
Sources: United Nations High Commissioner for Human Rights: A/HRC/39/29. The Corporate Responsibility to Respect Human Rights.	

Surveillance

Communications Surveillance

Communications surveillance is defined as the "*monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks to a group of recipients by a third party.*[16] Third parties include law enforcement agencies, intelligence agencies, private companies or even malicious actors.[17] It may be conducted at a mass (large) level, for instance, through programs like the UK's Tempora initiative, or at a more invasive level, such as the installation of spyware on an individuals' electronic devices, such as mobile phones or computers. This automated communication surveillance amounts to a breach of the right to privacy.[18]

Courts worldwide have provided direction on state-led communication surveillance practices, providing ***persuasive jurisprudence for GIF countries***. Some of these cases include:

- **United Kingdom:** in the case of *Big Brother Watch and Others v the United Kingdom*, the European Court of Human Rights (ECtHR) determined that the United Kingdom's bulk surveillance regime violated Article 8 of the ECHR on the right to privacy. The violation was due to the regime's failure to sufficiently safeguard confidential journalistic material from being collected and inspected during the monitoring of communications data carried out by UK intelligence agencies.[19]
- **South Africa:** in the case of *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others,*the High Court held that 'the need of journalists and their sources for confidential communications required special protections against surveillance abuses.'[20]

In one of the most pervasive incidents of corporate-sponsored communication surveillance underscoring global calls for a moratorium on surveillance technologies,[21]

Forbidden Stories, a nonprofit journalism group, documented the global deployment of ***Pegasus***. Further, this investigation contributes to the growing apprehensions regarding unauthorized government surveillance carried out using private spyware as well as the seeming trade-off between private security and national security or public safety.

Pegasus is 'military-grade zero-click surveillance software' sold by NSO Group Technologies to governments around the globe for alleged purposes of curbing terrorism and crime.[22] Zero-click surveillance software enables hackers to obtain access to the mobile phones of targets without any user interaction, such as opening malicious links or performing any action.[23] According to the findings of the investigation, the software had been used to surveil more than 50,000 phone numbers between 2016 and 2021 belonging to several heads of state and government officials (comprising cabinet ministers, diplomats, politicians, military and security officers) business executives, human rights activists and journalists.[24]

Upon being sued by WhatsApp, NSO Group argued that it should be granted "sovereign immunity" due to the fact that NSO's clients consist of government customers who are thoroughly scrutinized, and legal principles dictate that governments cannot be sued for executing their lawful duties. NSO has further asserted that it is their customers who conduct the targeting, not the company itself.[25]

Spotlight: NSO Group Spokesperson's Statement

"Millions of people around the world are sleeping well at night, and safely walking in the streets, thanks to Pegasus and similar technologies which help intelligence agencies and law enforcement agencies around the world to prevent and investigate crime, terrorism, and pedophilia rings that are hiding under the umbrella of End-to-End encryption apps.

"We reiterate: NSO does not operate the technology, nor do we have visibility to the data collected. Our products, sold to vetted foreign governments, cannot be used to conduct cyber surveillance within the United States, and no foreign customer has ever been granted technology that would enable them to access phones

with U.S. numbers. It is simply technologically impossible."

Source: *The Guardian*.

The use of surveillance software to target individuals, including journalists and media personnel has a chilling effect. Concerningly, surveillance not only affects the target individuals but also individuals who they are in contact with, which forces informants to self-censor out of fear of censure. The very existence of such hacking programs threatens varied human rights that are underpin democratic states, including privacy, freedom of expression and access to information, impeding the media's work and restricting public discourse and engagement.[26]

Resource: The Necessary and Proportionate Principles on the Application of Human Rights to Communications Surveillance (or the "13 Principles")

The 13 Principles have been endorsed by 600 organizations and over 270,000 individuals worldwide, and provide for the application of human rights law to communications surveillance.[27] They include (1) Legality; (2) Legitimate Aim; (3) Necessity; (4) Adequacy; (5) Proportionality; (6) Competent Judicial Authority; (7) Due Process; (8) User Notification; (9) Transparency; (10) Public Oversight; (11) Integrity of Communications and Systems; (12) Safeguards for International Cooperation; and (13) Safeguards against Illegitimate Access and Right to Effective Remedy.

Source: **Necessary and Proportionate.Org**.

Government-Led Digital Surveillance

Government-led digital surveillance entails the use of digital technologies by governments to control their citizenry.[28] More specifically, government-led surveillance as a whole entails the collection of information by the government for purposes of "intelligence, threat monitoring and recognition, prevention and investigation of criminal activity, political information or social control."[29]

Important Note

The Government of China, utilizes a wide array of surveillance technologies powered by AI to track its 1.4 billion population. Some of the surveillance techniques include the 'use of a network of 200 million CCTV cameras coupled with sophisticated big-data analytics, software recognising facial features, voice patterns, walking styles and other biometric collection programs.'

Source: Matthieu Burnay.

Mass surveillance is a key component in government-led digital surveillance and it involves the gathering, processing, creation, examination, utilization, retention, or storage of information related to a substantial number of individuals, without considering whether they are suspected of any wrongdoing.[30] This information is often sourced directly from data subjects themselves, who generate large amounts of personal data using digital technologies. Further, this information is also commonly obtained from digital service providers, who process subjects' data sets as their 'de facto property' using advanced algorithms to identify correlations.[31]

Mass surveillance negatively impacts the enjoyment of human rights and freedoms such as the rights to freedom of assembly, freedom of expression, freedom of movement and also political participation.[32] Further, mass surveillance instills a culture and an environment of fear, with citizens being presumed *de facto* culpable unless proven otherwise, eventually altering the 'power balance between a state and its citizens.'[33]

Across GIF regions, mass surveillance is an entrenched practice. For example, in the Africa region, the deployment of biometric data collection programs in countries such as Angola, Central African Republic, Democratic Republic of Congo, Uganda, Mozambique and Zimbabwe facilitates enhanced mass surveillance, profiling and targeting of citizenry. A large number of these countries use national security justifications to deploy surveillance technologies.[34] In Central Asia, countries such as Kyrgyzstan and Tajikistan have deployed Chinese technologies to facilitate mass state surveillance, including through the deployment of smart city programs.[35]

Social Media Surveillance and Monitoring

Resource: Freedom House Freedom on the Net 2019 Report

"What was once a liberating technology has become a conduit for surveillance and electoral manipulation."

Source: *Freedom House*.

Social media surveillance is defined as the "*collection and processing of personal data pulled from digital communication platforms, often through automated technology that allows for real-time aggregation, organization, and analysis of large amounts of metadata and content.*"[36] It serves as one of the tools used to obtain large personal data sets and is often justified under the guise of maintaining security, public order and curbing disinformation.

Globally, there is a thriving commercial market for social media surveillance tools, systems and technologies. This has decreased the barrier to entry not only for the security apparatus of autocratic regimes but also for law enforcement agencies at the national and local levels in democratic societies. Research reveals that both authoritarian and democratic governments are procuring social media surveillance systems, leveraging AI technologies, to recognize potential threats and quell undesirable speech. AI-technologies have the ability to 'identify patterns and infer individuals past, present, or future behavior,' and are deployed with minimal supervision or responsibility.[37]

Problematically, social media surveillance interferes with a range of human rights and freedoms, particularly the right to privacy and has a chilling effect on freedom of expression online. This has led to a worldwide surge in violations of civil and political rights and freedoms.[38] Across GIF regions, social media surveillance is rife, and authorities have been known to procure digital technologies to monitor social media users. These social media surveillance efforts are often approved as part of a country's national budgets, with funding being allocated to national intelligence and security agencies.[39]

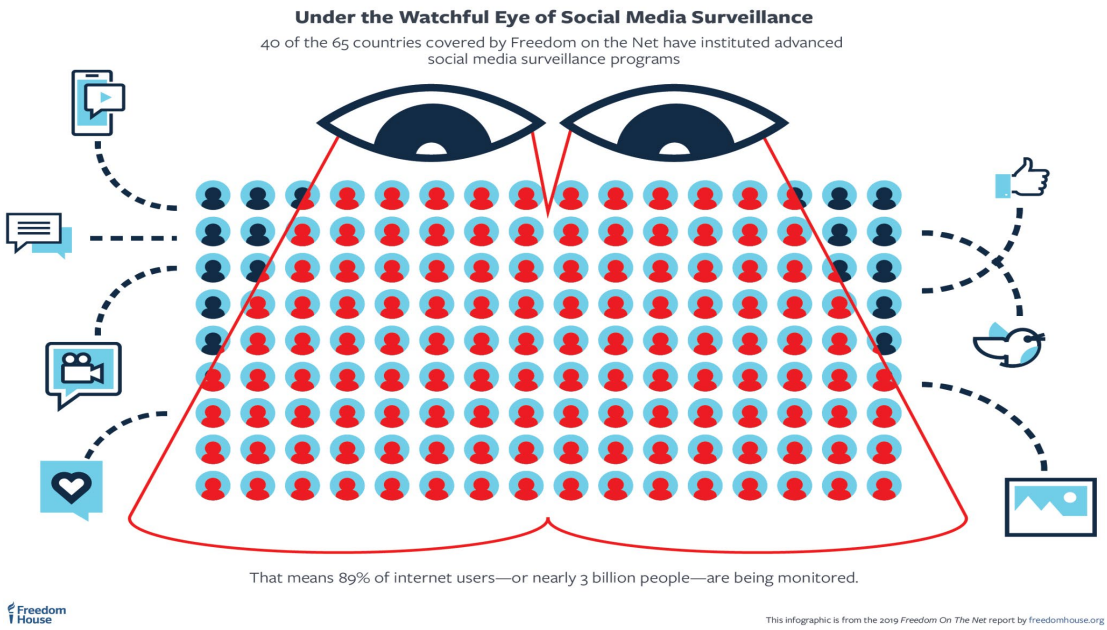
Important Note

In Russia, the Roskomnadzor (RKN), a state agency formed following presidential decree (No. 1715) in 2008 is mandated to regulate the country's internet and media. Investigations by Meduza following a RKN data leak by nonprofit whistleblower site Distributed Denial of Secrets (DDoSecrets) revealed that the agency has been surveilling the mass media and Internet for content "capable of destabilizing [Russia's] socio-political situation" since 2020. This serves as a reminder of how the online and offline worlds intersect and the manner in which internet communication can be used by authoritarian regimes to censor freedom of expression as well as to track down and arrest opposition leaders.

Sources: Council on Foreign Relations. Meduza.

In the South and Southeast Asia (SSE) region, it was reported that social media monitoring of users' accounts is the most common form of surveillance deployed by governments to "track critical voices and political oppositions and force them to align their online activities with State agenda."[40] In the Balkans region, as part of efforts to prevent firearm crimes, the South Eastern and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons (SEESAC) is working with state agencies to deploy social media intelligence (SOCMINT), which are a "*set of tools and solutions that enable law enforcement agencies to analyze conversations, react to social media cues, and combine social media data points into significant trends and analyses, according to investigation requirements.*"[41]

Figure 1: ***Under the Watchful Eye of Social Media Surveillance*****. Source:** ***Freedom House*****.**


Under the Watchful Eye of Social Media Surveillance
40 of the 65 countries covered by Freedom on the Net have instituted advanced social media surveillance programs
That means 89% of internet users—or nearly 3 billion people—are being monitored.
Freedom House
This infographic is from the 2019 Freedom On The Net report by freedomhouse.org

Biometric Identification and Surveillance

Biometrics are defined as a "measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant,"[42] with this data being classified as sensitive personal data. Biometrics are presented as more reliable than other traditional authentication techniques, such as passwords, since they cannot be easily lost, damaged, forgotten or stolen.[43]

Important Note

Identity verification refers to the concept of "determining the veracity of particular attributes or credentials," with digital identity verification taking place online. Examples of digital identity verification methods include (i) ID document verification, (ii) biometric verification, and (iii) database verification. Across GIF regions, some data protection laws provide for data controllers to use all reasonable measures to verify data subjects' identity.

Sources: **World Bank**. CyberSecurity Insiders. GDPR (Recital 64).

Biometric identification technology is used for many different purposes, from banking and finance to immigration control and law enforcement. The use of biometrics for these purposes is now an entrenched practice, resulting in the deployment of fingerprints, facial recognition, or iris scanning technologies.[44]

Spotlight on Facial Recognition Technology

Facial recognition technologies (FRT) are utilized for different purposes and applications. This is defined as *"a technology capable of matching a human face from a digital image or a video frame against a database of faces to confirm an individual's identity. Although less accurate than fingerprint recognition, it is often favored because of its contactless nature. It is mostly used in personal security, law enforcement, or digital onboarding in finance."*

- FRTs are commonly utilized within individual mobile devices, exemplified by Apple's iPhone (from X and subsequent models) with its Face ID feature, allowing users to access their phones using a facial scan captured by the device's camera.
- FRTs have also been used for border control and crime prevention, through integration into CCTV cameras.
- FRTs are also used by government authorities to engage in surveillance activities, including tracking and identifying individuals participating in political rallies or protests, enabling the restriction and suppression of political dissent.
    - *"The possibility of such outcomes transforms the issue of FRT from one of merely an individual's right to privacy being affected to one that affects a much wider range of*

fundamental rights including the right to dissent, protest and peaceful assembly."

GIF - Africa Region: Examples

- 2018:
  - Tanzania: a biometric border screening with facial recognition was installed at Kilimanjaro and Julius Nyerere International Airports.[45]
  - Uganda: H.E. President Yoweri Museveni commissioned a CCTV surveillance center with facial recognition covering Metropolitan Kampala.

Sources: Innovatrics; Apple Inc; The Centre for Internet and Society, India & The Human Rights, Big Data and Technology Project, University of Essex, UK.

Despite the benefits, biometric identification is accompanied with concerns about privacy and civil liberties. Concerningly, the collection of vast amounts of biometric data sets enables biometric surveillance which often takes place without proper oversight or accountability, leading to abuses of power and potential violations of human rights. Biometrics surveillance gives rise to privacy and data protection concerns permitting the unregulated monitoring of citizens without their consent.

Additionally, the storage and sharing of biometric data, coupled with fears of potential data misuse, are key data protection concerns, resulting in the enactment of data protection laws across GIF regions. Further, biometric surveillance technologies are also "*used in fundamentally discriminatory ways that continue to disadvantage those who have been historically excluded,*"[46] based on factors such as race, ethnicity, gender or religion.

Important Note

"Biometric technologies are infiltrating new markets like automobiles, workplaces and virtual reality, but they are not always labeled as such. Often relying on flawed technology for purposes it's not well-designed for, the industries making widespread use of biometrics are nevertheless depending on them for sensitive and inappropriate decision-making, such as evaluating a worker's productivity or a driver's attentiveness."

Source: AI Now Institute.

The biometrics surveillance market is steered by private sector and multilateral organization investments, with the former stakeholder taking the lead in the development and implementation of biometric identity management systems and biometric

surveillance systems at state levels, and the latter providing financial and technical assistance.

However, this approach brings forth certain associated risks, including (i) a reliance on proprietary systems supplied by specific vendors, often contracted at a steep financial cost, (ii) data transfer and data sovereignty concerns regarding the hosting of critical databases outside countries' jurisdiction, and (iii) the lack of technology transfer and skill development after the deployment of such systems.

Consequently, this leaves government agencies responsible for implementation in a vulnerable position, as their control over information and systems becomes limited due to dependency on suppliers. Furthermore, the adoption of proprietary systems, as opposed to open-source alternatives, can hinder a government's ability to engage different service providers, and further prevents states from gaining access to their own databases. Illustratively, in Kenya, Smartmatic International, the organization contracted by the elections body (IEBC), declined access to server images citing infringement on their intellectual property rights. This refusal persisted despite a court order issued by the Supreme Court in August 2022.[47]

Privacy

Data Breaches

A data breach is defined as a "any security incident in which unauthorized parties gain access to sensitive data or confidential information."[48] Data breaches can be deliberate or inadvertent generally occurring due to "weaknesses in technology or user behavior."[49] Other causes of data breaches include malicious insiders or outsiders, both permitting the leak or theft of personal or sensitive data or information.[50]

Important Note

The terms 'data breach' and 'breach' are often used interchangeably with 'cyberattack.' But not all cyberattacks are data breaches—and not all data breaches are cyberattacks.

Source: IBM.

At the legal level, data breach notifications are mandated in data protection laws across GIF countries to varying degrees and with an application impact on specific entities (private versus public sector) and authorities. Generally, these "*laws require entities that have been subjected to a breach (and are covered by the law) to contact the individuals whose data was breached and other relevant parties and inform them about the incident."*[51]

Data breaches pose a significant risk to individuals' rights and freedoms, resulting in the exposure of sensitive information that could be used to exploit individuals and their data privacy.[52] Across GIF regions, data breaches are common, partially attributed to efforts aimed at digitizing both public and private systems and services. According to the UN, the Latin America and the Caribbean (LAC) region is the "world's least-prepared area for cyberattacks" as evidenced by a string of cyber attacks on state databases and systems.[53] Illustratively, in 2022, more than 9 LAC countries were affected by hacking incidents resulting in extensive data breaches.

Resource: Electronic Frontier Foundation's *'Hacking Governments and Government Hacking in Latin America: 2022 in Review*

"To give some examples, ransomware attacks affected government services in Quito, Ecuador; targeted Chile's judicial system and the National Consumer Service (Sernac); as well as impacted operations that are dependent on the digital platforms of the Colombian sanitary authority (Invima) and companies' oversight agency (Supersociedades). Probably the most extensive attack took place in Costa Rica, disrupting government services and leading President Rodrigo Chaves to declare a national emergency."

Source: Electronic Frontier Foundation.

Privacy Policies and Consent

Resource: IAPP White Paper – The UX Guide to Getting Consent

While the IAPP White Paper is centered on the EU's GDPR, the document is useful for establishing how 'consent' intersects with the 'notice' requirement.

Source: IAPP.

A privacy policy is an essential document that outlines how an organization or agency collects, processes, uses, and shares individuals' personal data using simple language, fostering trust and transparency in data processing.[54] A comprehensive privacy policy will also include details about how individuals' can exercise their right to access, modify, or delete their data. Privacy policies are fundamental for any digital medium like an e-service portal, websites, web and mobile applications, amongst others, with the phrase being interchanged with 'privacy statement,' 'privacy page,' 'privacy notice,' and 'privacy information.'[55] However, these terms have different legal meanings across GIF regions .

Consent is an important part of any privacy policy, referring to a data subject's informed and unequivocal agreement permitting the collecting entity to process, use and transfer (where necessary) their data for specified purposes, prior to the data collection activities, which can be revoked at any given time.[56] According to the IAPP, a not-for-profit privacy organization, consent "may be affirmative; i.e., opt-in; or implied; i.e., the individual didn't opt out."[57]

Across GIF regions, many countries have mandated privacy policies as integral for compliance with data privacy and protection laws. For instance, in the SSE Asia region, notice requirements are provided under Philippines Data Privacy Act of 2012 (R.A. 10173) and the Implementing Rules and Regulations of the Data Privacy Act of 2012. Illustratively, the National Privacy Commission provides a Privacy Statement that outlines where consent applies, and where it will not be used as a basis for the processing of personal data collected.[58]

Resource: IAPP's Global Comprehensive Privacy Law Mapping Chart

The IAPP's Global Comprehensive Privacy Law Mapping Chart provides a detailed examination of data protection laws at a global level, exploring "commonalities in terms of the rights, obligations and enforcement provisions." Critically, the chart outlines notice and transparency requirements, including for GIF countries in the Africa, LAC, and SSE Asia regions.

Source: IAPP.

Browser Fingerprinting

Resource: W3C's Draft on Mitigating Browser Fingerprinting in Web Specifications

The W3C's draft on 'Mitigating Browser Fingerprinting in Web Specifications' (2021) builds on a similar 2019 document. This document provides best practices regarding browser fingerprinting for Web specification authors.

Source: W3C.

Browsers are an essential gateway enabling users' to access the Internet, but they are also used to track and profile individuals online. Browser fingerprinting is an online tracking technique used by companies and other entities to monitor users' online activities without their consent or knowledge. Browser fingerprinting goes beyond cookie-based tracking, and works by creating a unique identifier about a users "*based on [one's] computer hardware, software, add-ons, and even preferences. Your settings like the screen you use, the fonts installed on your computer, and even your choice of a web browser can all be used to create a fingerprint.*"[59]

This fingerprint can then be used to track an individual from site to site, gather information about users' online activities, and even target advertisements at users.[60]

Browser fingerprinting is intrusive, being used to violate users' privacy and collect personal information without users' knowledge. In turn, this can result in long-term and continuous problems impacting users, such as targeted advertising or identity theft, ultimately eroding users' control over their online experiences.[61]

Social Engineering

Social engineering is the "*use of social disguises, cultural ploys and psychological tricks to get computer users (i.e targets) to assist hackers (i.e offenders) in their illegal intrusion or use of computer systems and networks*."[62] It involves an exploitation of human psychology to gain access to confidential information or resources, rather than relying on technical vulnerabilities to breach personal boundaries.

Social engineering techniques exploit the interconnected nature of online and offline identities. Attackers gather seemingly innocuous information from various sources, such as social media profiles or public records, and then use this data to craft convincing scenarios. By tailoring their approach to the target's background, interests, and relationships, social engineers are able to construct persuasive narratives that deceive even extremely cautious individuals.[63]

Generally, attackers use malicious tactics like phishing, vishing, and smishing (which are all forms of social engineering) to obtain sensitive data such as usernames, passwords, credit card numbers, and more, using varied communication methods. Some examples of these methods include 'voice calls, emails, text messages, Other forms of social engineering activities include 'pretexting, baiting, quid-pro-quo and tailgating.'[64] Due to the online-offline connection, these attacks have long-lasting consequences for individuals, resulting in identity theft, amongst other nefarious and continuing attacks.

Supplementary Resources

Legislation (International, Regional National)

African Charter on Human and Peoples' Rights (ACHPR), 1986.

American Convention on Human Rights (1969).

American Declaration of the Rights and Duties of Man (1948).

Association of Southeast Asian Nations (ASEAN) Human Rights Declaration, 2009.

Charter of Fundamental Rights of the European Union, 2009.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, or ECHR), 1953.

Declaration of Principles on Freedom of Expression in Africa, revised in 2019.

Guidelines on Freedom of Association and Assembly in Africa, 2017.

Inter-American Democratic Charter (2001).

International Covenant on Civil and Political Rights (ICCPR), 1996.

Universal Declaration of Human Rights (UDHR), 1948.

Journal Articles & Papers

Chika Ebere Odoemelam (2015). Adapting to Surveillance and Privacy Issues in the Era of Technological and Social Networking.

Daniel J. Power, Ciara Heavin & Yvonne O'Connor (2021). Balancing privacy rights and surveillance analytics: a decision process guide.

Ian Brown (2015). Social Media Surveillance.

International Review of Law, Computers & Technology. Surveillance, Privacy.

Justice Alfred Mavedzenge (2020). The right to privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance.

Katherine Dormandy (2020). Digital Whiplash: The case of Digital Surveillance.

Pierre Laperdrix and others (2019). Browser Fingerprinting: A Survey.

Surveillance and Society. Vol. 21 No. 2 (2023): Open Issue.

Books

Sara M. Smyth (2019). Biometrics, Surveillance and the Law.

Training Material and Learning Resources

IAPP. What does privacy mean?

Media Defence. Surveillance.

Privacy International (2018). Communications Surveillance.

Privacy International (2022). PI's Guide to International Law and Surveillance.

Guides

Electronic Frontier Foundation. Surveillance Self-Defense (SSD).

Electronic Frontier Foundation. Cover Your Tracks.

References

[1] Joe Robinson (2023). Internet Surveillance and how to keep your activity private; Kevin Haggerty and Richard Ericson (2006). The New Politics of Surveillance and Visibility.
[2] IAPP. What does privacy mean?; Ira S. Rubinstein (2015). Voter Privacy in the Age of Big Data.
[3] Chika Ebere Odoemelam (2015). Adapting to Surveillance and Privacy Issues in the Era of Technological and Social Networking.
[4] Christian Fuchs (2010). How can Surveillance be Defined? Remarks on Theoretical Foundations of Surveillance Studies.
[5] *Ibid.*
[6] Gary T Marx. Surveillance Studies.
[7] Katherine Dormandy (2020). Digital Whiplash: The case of Digital Surveillance.
[8] Kevin D. Haggerty and Richard V. Ericson (2006). The New Politics of Surveillance and Visibility.
[9] *Ibid, n. 2*.
[10] Article 12 of the Universal Declaration on Human Rights; Article 17 of International Covenant on Civil and Political Rights.
[11] David Banisar (2023). National Comprehensive Data Protection/Privacy Laws and Bills 2023; UNCTAD (2021). Data Protection and Privacy Legislation Worldwide.
[12] OHCHR. The right to privacy in the digital age - A/HRC/39/29.
[13] Telecom Review (2020). Personal privacy vs public security: Where do we draw the line?
[14] United Nations High Commissioner for Human Rights (2018). The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (A/HRC/39/29).
[15] OHCHR (2022). The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/51/17); *S and Marper v United Kingdom* [2009] 48 ECHR 50, at para 118.
[16] Privacy International (2018). Communications Surveillance.
[17] *Ibid.*
[18] Amnesty International (2021). UK: Europe's top court rules UK mass surveillance regime violated human rights.
[19] ECtHR - Grand Chamber (2021). *Case of Big Brother Watch & Ors. v The United Kingdom,* Application nos. 58170/13, 62322/14 and 24969/15.
[20] Constitutional Court of South Africa (2021). *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).
[21] See: OHCHR (2021). Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech; Amnesty International (2021). Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology; CyberPeace Institute (2022). Renewed call for moratorium on sale and use of spyware.
[22] The Washington Post (2022). Takeaways from the Pegasus Project.
[23] OHCHR (2022). The right to privacy in the digital age (A/HRC/51/17).
[24] Dana Priest and Elizabeth Dwoskin (2021). Chief of WhatsApp, which sued NSO over alleged hacking of its product, disputes firm's denials on scope of, involvement in spyware operations.
[25] The United States District Court for the Northern District of California (2020). *WhatsApp Inc. v. NSO Group Technologies Limited;* SCOTUS Blog (2023). *NSO Group Technologies Limited v. WhatsApp Inc.*
[26] *Ibid,* n. 23.
[27] Electronic Frontier Foundation (2014). Necessary and Proportionate Principles.
[28] Maximiliano Emanuel Korstanje, Geoffrey Skoll (2018). Technology and Terror.
[29] NordVPN. Government Surveillance.
[30] Privacy International. Mass Surveillance.
[31] *Ibid.*
[32] *Ibid.*
[33] Daniel Anyemedu (2021). Digital Surveillance in Violation of Human Right and Data Justice.
[34] CIPESA (2022). The State of Internet Freedom in Africa 2022: The Rise of Biometric Surveillance.
[35] Bradley Jardine (2019). China's Surveillance State Has Eyes on Central Asia.
[36] Adrian Shahbaz and Allie Funk (2019). Social Media Surveillance.
[37] *Ibid.*
[38] Adrian Shahbaz and Allie Funk (2019). Freedom on the Net 2019: The Crisis of Social Media, pp. 2.

[39] In Nigeria, 4.87-billion-naira ($11.85 million) was allocated to the National Intelligence Agency (NIA) in 2021 to facilitate state-sponsored monitoring of WhatsApp messages, phone calls and text messages. See: Premium Times (2021). Nigerian govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls; Yitong Wu and Chingman (2022). WeChat warns users their likes, comments and histories are being sent to China, RFA Cantonese.
[40] Manushya Foundation & the ASEAN Regional Coalition to #StopDigitalDictatorship (2022). Joint Submission to the United Nations High Commissioner for Human Rights - The Right to Privacy in the Digital Age: Mass surveillance, Digital Contact-tracing, Social Media Monitoring, and Data Requests in Southeast Asia.
[41] SEESAC (2023). Authorities from Western Balkans, Moldova, and Ukraine Build Capacities in Social Media Intelligence.
[42] NIST Computer Security Resource Center. Glossary: Biometrics.
[43] Sara M. Smyth (2019). Biometrics, Surveillance and the Law.
[44] ShuftiPro. Biometric Identification.
[45] CIPESA (2022). State of Internet Freedom in Africa 2022, The Rise of Biometric Surveillance.
[46] ARTICLE 19 (2021). When bodies become data: Biometric technologies and free expression.
[47] CIPESA (2022). State of Internet Freedom in Africa 2022, The Rise of Biometric Surveillance, pp. 36.
[48] IBM (2022). What is a data breach?
[49] Kaspersky. How Data Breaches Happen.
[50] *Ibid, n. 50.*
[51] UNODC (2020). Data breach notification laws.
[52] European Commission. What is a data breach and what do we have to do in case of a data breach?
[53] Americas Quarterly (2023). NEW AQ: Hacker's Paradise: Why Latin America Is So Vulnerable; Inter American Development Bank; Organization of American States (2016). Cybersecurity: Are We Ready in Latin America and the Caribbean?
[54] World Bank (2019). Practitioner's Guide: Data Protection and Privacy Laws.
[55] Medium (2018). Data Privacy in the Digital Age: Understanding Your Rights and Protecting Personal Information.
[56] IAPP. Consent.
[57] *Ibid.*
[58] NPC. Privacy Statement.
[59] Mozilla. Firefox blocks fingerprinting.
[60] Tamas Kadar. What is browser fingerprinting & how does it work?
[61] WIRED (2022). The Quiet Way Advertisers Are Tracking Your Browsing.
[62] Jan-Willem H. Bullee and Marianne Junger. Social Engineering.
[63] Chloe Pilette (2021). What is Social Engineering? Definition + Protection Techniques.
[64] Joe Pettit (2023). *Social Engineering: Definition and 6 Attack Types*.