



SURVEILLANCE AND HUMAN RIGHTS

Background paper prepared by Mr. Leith Jeroudi for the Geneva Centre for Human Rights Advancement and Global Dialogue

Surveillance, derived from the French word 'surveiller' for 'to watch over', has seen a tremendous evolution in the era of digitization. Previously a tool primarily for control by governments and powerful groups, it has expanded to encompass electronic data acquisition and interpretation. This form of digital surveillance utilizes a spectrum of technologies, including closed-circuit television (CCTV), biometric analysis, sophisticated tracking software, and artificial intelligence.¹ These technologies, while raising some concerns, also offer tangible benefits such as increased security and potentially enhanced efficiency in service delivery.² The omnipresence of surveillance in our day-to-day lives, a product of technological advancement, underscores the need for dialogue about human rights. Basic liberties such as privacy, freedom of expression, and association are potentially endangered due to unchecked surveillance practices. Popular discourse often presents this as a 'trade-off' between privacy and security, but we aim to investigate this deeper. The effects of surveillance seep into many aspects of our daily lives, beyond the familiar security-freedom paradigm. It is crucial, then, to address the extensive influence of surveillance in order to strike a balance between essential security needs and the preservation of human rights. This understanding is integral to navigating the complexities of this ever-expanding concern.

Key Concepts

The use of advanced technologies to monitor, intercept, collect, analyze, and store digital communications and metadata is known as digital surveillance, which is the most common form of surveillance today. The methods employed range from monitoring email and browsing history to using GPS to track physical locations, as well as conducting large-scale data mining of online activity.³ The use of surveillance in society is a topic of debate as it raises concerns about the infringement of basic human rights. Surveillance practices can significantly impact digital rights, privacy, freedom of association, and freedom of expression, which are some of the most fundamental human rights, leading to the fulfillment of many other important rights. Another key concept is that of data protection. Private and public entities are gaining increased capacity to

¹ United Nations, "Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism.", 4.

² Fontes, Hohma, Corrigan & Lütge, "AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them.", 2-5.

³ Ajunwa, Crawford & Schultz, "Limitless Worker Surveillance.", 743

extract more and more personal data of a variety of nature, such as personal health information or precise location. As technology advances, the protection of our rights is becoming more challenging due to the prevalence of digital surveillance. This is often justified by the need for national security and public safety. Surveillance poses a significant threat to the right to privacy, which is protected under Article 12 of the Universal Declaration of Human Rights.⁴ The use of surveillance technologies without consent can lead to the collection of personal information and tracking of activities, which is a breach of privacy rights.

Human Rights Risks and Violations

Digital surveillance carries substantial risks to human rights, particularly in terms of privacy. Instances such as the use of the surveillance technology Pegasus, which targeted journalists and politicians globally, stand as notable violations. Surveillance also affects freedom of expression and association; the knowledge of being under observation can lead to self-censorship, which limits democratic discourse.⁵ Such surveillance practices can cultivate an atmosphere of fear and mistrust and can amplify discriminatory practices. Moreover, the misuse of digital ID systems can further compromise individual privacy. Governments and organizations may use these systems to track people's movements, purchases, and even political beliefs without their knowledge or consent, creating an additional layer of human rights infringement.⁶ Similarly, abuse of counter-terrorism plans poses another threat, as seen in some instances where such measures have been used to target activists under the guise of national security,⁷ thereby suppressing dissent and infringing upon the freedom of expression.

Relevant Human Rights Principles

The right to privacy, central to the debate on surveillance, is protected under Article 12 of the Universal Declaration of Human Rights. However, it is under threat due to digital surveillance practices. Other affected rights include freedom of expression and association, which are stifled due to surveillance-induced fear. The ongoing debate revolves around achieving the balance between national security requirements and individual rights.

International and Regional Norms

Surveillance technologies are governed by a framework, which is yet to be rooted in international norms and standards. This suggests that there is a lack of emphasis on the balance between enhancing security and respecting human rights internationally. This area has been closely monitored by the United Nations, as the UN Human Rights Council has underscored the right to privacy in the digital age, noting that intrusive surveillance can infringe on human

⁴ Privacy International, "Digital Health: What Does It Mean for Your Rights and Freedoms."

⁵ Fatafta, "Unsafe Anywhere: Women Human Rights Defenders Speak Out about Pegasus Attacks."

⁶ Council of Europe, "Convention 108 on Data Protection: Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.", 16-23

⁷ Fussey & Sandhu, "Surveillance Arbitration in the Era of Digital Policing.", 14

rights.⁸ The Special Rapporteur on the right to privacy has issued directives, advising states to ensure their surveillance activities comply with international human rights law. The International Covenant on Civil and Political Rights (ICCPR), in its Article 17 and General Comment 16, also provides a strong international normative framework against unlawful or arbitrary interference with privacy. Interpretation and application of these standards can vary, influenced by regional and national contexts. In Europe, the General Data Protection Regulation (GDPR) offers strict rules for data collection and usage, with the aim of protecting the privacy rights of European Union citizens.⁹ The European Commission and the Council of Europe have made substantial strides in this area, with instruments such as the Convention 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data. Some have even proposed extending Convention 108 into a global treaty to address the digital privacy challenges worldwide.¹⁰ The non-member states that have ratified Convention 108 are Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay. These countries, despite not being members of the Council of Europe, have committed themselves to the standards set by Convention 108 for the protection of individuals with regard to the automatic processing of personal data. This reflects the convention's significance in setting international standards for data protection and privacy. The Organisation for Economic Co-operation and Development has also contributed significantly, establishing a landmark agreement on safeguarding privacy in cases of law enforcement and national security data access.¹¹ However, as discussed in the International Journal of Human Rights, these international norms only effectively apply within the domestic legal frameworks of individual states.¹² Additional measures include export controls such as the Wassenaar Arrangement, which restricts the trade of certain surveillance technologies.¹³ The European Union is also developing guidelines on the export of cyber-surveillance items, seeking to prevent the misuse of such technologies.

Current Multilateral Discussions

The topic of human rights and surveillance is currently being discussed on various international platforms. Discussions have taken place in various forums, such as the UN General Assembly and the Human Rights Council, to examine how contemporary surveillance methods impact essential rights like individual privacy. Many governments claim that surveillance measures are necessary to protect their citizens, especially when dealing with national security threats. Privacy International and Access Now are actively advocating for the protection of

⁸ United Nations, “Special Rapporteur on the Right to Privacy.”, 1

⁹ Privacy International, “New Year, New Noom? What Our Re-Testing of the Weight-Loss Platform Taught Us.”

¹⁰ Greenleaf, “The UN Should Adopt Data Protection Convention 108 as a Global Treaty: Submission on ‘The Right to Privacy in the Digital Age’ to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy.”

¹¹ Organization for Economic Co-operation and Development, “Landmark Agreement Adopted on Safeguarding Privacy in Law Enforcement and National Security Data Access.”

¹² Humble, “International Law, Surveillance and the Protection of Privacy.”, 15

¹³ European Commission, “Guidelines on the Export of Cyber-Surveillance Items Under Article 5 of Regulation (EU) No. 2021/821.”

individual privacy rights and are pushing for legal limitations on unchecked surveillance, while various rights groups are also supporting their cause. These discussions involve tech companies to a significant extent. Moreover, the use of data by foreign actors in the context of elections adds another dimension to this debate, raising concerns about the integrity of democratic processes.¹⁴ The negotiation of a new Cybercrime Treaty is underway, which aims to strengthen international cooperation and establish unified standards against cyber threats.¹⁵ However, challenges remain, including the lack of a binding international agreement regarding the trade of surveillance technology and the variable application of existing standards across regions. The adoption of resolutions by the UN that highlight the importance of privacy in the digital era has been viewed as a noteworthy advancement.¹⁶ Simultaneously, there persist obstacles, including the absence of a mandatory global accord regarding the trade of surveillance technology and the diverse execution of current standards across different regions.

The Surveillance Industry

The demand for surveillance solutions is increasing globally, leading to the rapid growth of the surveillance technology industry, which is constantly evolving due to technological advancements. The industry has grown considerably due to the importance of ensuring both public safety and private security. Prominent companies in the sector consist of Hikvision, Dahua, and Bosch Security Systems, among other notable competitors.¹⁷ Surveillance technologies are significantly influenced by tech companies in terms of their development and widespread use. The impact of the industry extends beyond manufacturing, as technology corporations also play a role in shaping public discussions and legal standards related to privacy and surveillance.¹⁸ In contrast, surveillance technologies are extensively used by governments as consumers. Consumer buying habits have the power to shape industry trends, while regulatory policies can have a major impact on the direction of the industry. Enhanced surveillance policies for national security reasons can promote economic growth, whereas strict privacy regulations can limit it. The expansion of the surveillance technology industry is impacted by various factors. Strong drivers in the market include the demand for advanced security systems in both public and private sectors. The expansion of industries can be influenced by the policy environment, which includes regulations and laws related to data privacy and surveillance. In addition, societal elements such as how the public views safety and privacy also have an impact.

¹⁴ Bennett, “The Privacy Advocates: Resisting the Spread of Surveillance.”, 31

¹⁵ United Nations, “Electronic Frontier Foundations and Privacy International: Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty: Chapters on International Cooperation, Technical Assistance, and Proactive Measures.”, 4

¹⁶ United Nations, “Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism.”

¹⁷ Brandessence Market Research And Consulting Private Limited, “Global Mobile Video Surveillance Market to Amplify Significantly by 2029 - Brandessence Market Research.”

¹⁸ Emanuilov & Yordanova., “Business and Human Rights in Industry 4.0: A Blueprint for Collaborative Human Rights Due Diligence in the Factories of the Future.”, 7

