FORUM: Special Conference on Ethos vs. Progress (SPECON)

QUESTION OF: Addressing the ethical considerations and implications of digital surveillance

STUDENT OFFICER: Stavroulaki Olga- Maria

POSITION: President

INTRODUCTION

Data security and privacy have become priorities for people, businesses, and society in the digital age. It is more important than ever to safeguard sensitive data and follow moral data handling procedures because technology and data-driven systems are widespread. Ethically, the act of closely investigating someone else is known as surveillance. However, the concept of surveillance is significantly different from the traditional observation of other individuals, something that, even though it may be targeted, does not have a specific objective and ceases over time.

Additionally, surveillance is characterised by the presence of a specific purpose, meaning that the concentration of attention on a certain individual or group of individuals, for example, has a specified objective.

Contrary to popular belief, surveillance does not always require observation in its traditional meaning. It might entail devices that can detect bombs at a distance or even just sniff, like in the case of canines, meaning drug detection dogs, trained to find drugs or communications intercepted over the phone.

The moral implications of using surveillance are taken into account by surveillance ethics. At the same time, digital surveillance can indeed be a cause of numerous legal infringements, primarily in the area of abuse of privacy rights and protection of personal data. Illegitimate data gathering, lack of consent, and excessive monitoring are all forms of

violations that could easily be under laws such as the Fourth Amendment in the U.S. [1] and the General Data Protection Regulation (GDPR)[2] in the E.U.

Moreover, these surveillance practices could run contrary to anti-discrimination laws and be seen as a serious infringement of civil liberties, something that is a matter of great concern from a legal perspective, among others. This study guide will explore whether this activity has inherent values, whether it can be employed for any purpose, and, on the other hand, whether it is always harmful, and delve into its disadvantages and advantages.

In connection to this year's conference theme, " Ethos vs. Progress: Reassessing our Values in a fragile world," we need to assess whether we should jeopardise privacy rights and ethics in order not to stop technology from evolving.

DEFINITION OF KEY TERMS

Data breach

Data breach refers to "an occasion when private information can be seen by people who should not be able to see it"[3]

Data Privacy

"Data privacy refers to protecting a person's personal information and making sure it is handled in a way that upholds their rights to secrecy, collectively referred to as data privacy. It relates to the power people have over the way their data is gathered, utilised, shared, and kept safe." [4]

---

[1]Reagan Library. "Constitutional Amendments: Amendment 4 – Right to Privacy." *Reagan Library*, National Archives and Records Administration, www.reaganlibrary.gov/constitutional-amendments-amendment-4-right-privacy. Accessed 19 Aug. 2024.

[2] GDPR.eu. "General Data Protection Regulation (GDPR) – Official Legal Text." *GDPR.eu*, GDPR Information Portal, www.gdpr-info.eu/. Accessed 19 Aug. 2024.

[3] *Data Breach | English Meaning - Cambridge Dictionary*, dictionary.cambridge.org/dictionary/english/data-breach. Accessed 19 July 2024.

[4] ForumCosmos. "Ethical Considerations in Data Privacy and Security." Medium, Medium, 13 July 2023, medium.com/@armaanakhan91/ethical-considerations-in-data-privacy-and-security-1874a10061f0.

Data Security

"Protecting data from modification, unauthorised access, and breaches is the main goal of data security. It entails putting safeguards in place to keep data safe from dangers including cyberattacks, illegal disclosures, and unintentional loss." [5]

Wiretapping

Wiretapping refers to "the action of secretly listening to other people's conversations by connecting a listening device to their phone."[6]

Whistleblower

Whistleblower is "a person who tells someone in authority about something illegal that is happening, especially in a government department or a company."[7]

[5] ForumCosmos. "Ethical Considerations in Data Privacy and Security." Medium, Medium, 13 July 2023, medium.com/@armaanakhan91/ethical-considerations-in-data-privacy-and-security-1874a10061f0.

[6] Wiretapping | English Meaning - Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/wiretapping. Accessed 19 July 2024.

[7] Whistle-Blower | English Meaning - Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/whistle-blower. Accessed 31 Aug. 2024.

BACKGROUND INFORMATION

History

Surveillance has undergone significant changes, evolving from the wiretapping methods of the 1950s to the advanced Artificial intelligence (AI)-operated systems of today. During the Industrial Revolution (1760-1840), due to the exponential population growth, a need for increased security was created. That was the first time that the world had faced such a need.

In addition, many technological advancements of that period contributed to the materialization of that idea. For example, the invention of the electrical telegraph by Samuel Morse in 1837, the invention of photography by Louis Daguerre and William Henry Fox Talbot in 1839, and the invention of electric light by Thomas Edison in 1879. Surveillance also had pivotal moments during the Second World War, when German military researchers developed the first Closed-Circuit Television (CCTV) systems, as well as after the war and more specifically in 1949 when US contractors commenced and began the development and sale of CCTV systems for commercial use.

During the 1950s and mostly during the Cold War, simple electronic eavesdropping began and progressed through generalized mass data gathering, culminating in more recent years with real-time monitoring. This early period featured mainframe computers, the first instances of global communication intercepts, including Extraterrestrial Communication High-Energy Neutrino Observatory (ECHELON), and automation. The personal computer and the increased prevalence of internet use in the 1980s–90s drove home surveillance capabilities, which benefits data collection.

During the Cold War, it was discovered that a large number of listening devices had been embedded within areas and walls inside the U.S. Embassy in Moscow. The devices were also planted inside the structure and in parts of walls or furniture, some sealed behind wooden panels added during the construction of a new section at Crusher Row in the 1970s-80s. It was so intrusive that the new building, assumed to be secure due to U.S.-friendly construction, was actually unsafe for any American. The episode underscored the extensive Soviet espionage efforts and resulted in greatly heightened tensions between the U.S. and its adversaries, as well as a global reassessment of security associated with U.S. diplomatic missions from that point on all over the world.

With the rapid growth of social media and the internet during the 2000s, governments and businesses gained the ability to gather vast amounts of data, leading to grave privacy issues. These issues received a lot of attention when whistleblowers revealed the scope of spying in 2013. This sparked legislation such as the USA FREEDOM Act[8] in the US and the General Data Protection Regulation[9] (GDPR) in the EU. The conflict between privacy and security is still a major worry today. There are still ongoing concerns about the moral implications and individual rights in the context of growing surveillance capabilities, especially as machine learning and artificial intelligence continue to expand and improve these technologies.

The September 11 attacks had a profound effect on global surveillance, leading to the broad implementation of national security surveillance to significantly expand government espionage programs. In the US, these events led to the USA PATRIOT Act,[10] which expanded law enforcement powers for investigations in countless ways into matters of surveillance and information gathering, allowing such access with almost no checks by court or legislative oversight. Many other countries have adopted similar policy measures internationally, building up their surveillance apparatus. The UK brought in laws such as the Regulation of Investigatory Powers Act (RIPA)[11], and EU states broadened their data retention and surveillance. These same measures led to the first worldwide discussion and debate over personal privacy, civil liberty, and ethics surrounding the use of mass surveillance.

Today, the tension between security and privacy continues to be a critical concern. Ongoing discussions focus on the ethical implications and individual rights in the context of evolving surveillance capabilities, particularly as advancements in artificial intelligence and machine learning further enhance these technologies.

The ethical concerns

[8] *Text - H.R.2048 - 114th Congress (2015-2016): USA Freedom Act of 2015 | Congress.Gov | Library of Congress*, www.congress.gov/bill/114th-congress/house-bill/2048/text. Accessed 31 Aug. 2024.

[9] "General Data Protection Regulation (GDPR)." *GDPR.eu*, 2024, gdpr-info.eu/. Accessed 20 Aug. 2024.

[10] Public Law 107-56: USA PATRIOT Act." *Congress.gov*, 26 Oct. 2001, www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm. Accessed 20 Aug. 2024.

[11] *Regulation of Investigatory Powers Act 2000*. *UK Government*, 2000, www.legislation.gov.uk/ukpga/2000/23/contents/enacted. Accessed 20 Aug. 2024.

Within the digital surveillance realm, informed consent means that users truly understand what data is being gathered, how it will be used and to whom it will be passed on. But in practice, few responsible governments have taken a stand of real consent; most digital platforms and state surveillance programs are conducted without adequate explicit user permissions or misguided "implicit" consent being extracted from inadequate terms and conditions. Digital surveillance, predominantly since 9/11, and meanwhile the right of the individual to make informed choices about their own digitised data has on all accounts taken a great length. This lack of transparency does not elicit trust, nor uphold the ethical standards required in a digital society that supposedly respects privacy.

The principle of limitation holds that surveillance should be limited to a few, defined purposes, such as countering threats to national security or preventing crime, and not used for wider or arbitrary purposes than those specified. However, since the post-9/11 surveillance programs are so vast, it has been almost impossible to uphold this principle. This surveillance scope frequently grows to include such activities as mining data for commercial market trends or the monitoring of political dissent by governments and other organizations. The key is to take additional measures to ensure that practices of surveillance are not only legally, but ethically constrained and respectful towards the private purposes of information from which rights originate.

Data minimisation means that a company should only collect as much user data as needed for its specific purpose and no more, to decrease the risk of incidents related to unauthorised access or abuse of personal information. But in the age of digital surveillance, it is often neglected. Governments and companies like to collect vast amounts of data in case they might use it one day, resulting in vast pools of information. This overcollection poses serious privacy risks when combined with the more data that is at rest, the more available to abuse—whether unauthorised personnel access, government overreach, or security incident-based exposures.

Many companies also received lawsuits for over-collecting data. In 2017 Equifax, an organization that collects and reports credit-related information on US consumers, one of the big three consumer credit reporting agencies, was subject to a data breach affecting approximately 150 million consumers. The breach occurred due to a long-standing vulnerability in one of Equifax's databases that the company had neglected to patch. Equifax also waited to disclose the breach to the public. The company settled with the Federal Trade

Commission, Consumer Financial Protection Bureau (CFPB), and all 50 U.S. States and territories in a lawsuit filed against them in August 2019. The original settlement was worth $575 million, including a fund to help consumers of up to $300 million and paid out across 48 states. [12]

Similarly,i n 2017, Vizio and its subsidiary, Inscape Services, faced serious issues over unauthorized data collection. The Federal Trade Commission (FTC), the Attorney General of New Jersey, and the New Jersey Division of Consumer Affairs (DCA) filed a joint lawsuit against the company. According to the lawsuit, Vizio has been secretly collecting data from its smart TVs and selling this data to third parties. That data included specific viewing habits, IP addresses, nearby Wi-Fi networks, and other personal information. Even worse, the data collected could be tied to personal facts such as age, sex, marital status, income, education, home ownership, and size of household. Vizio used a "smart interactivity" feature that was supposed to provide viewing recommendations but often didn't, and it did not fully disclose how much data was being collected. The case came to an end when Vizio agreed to the $2.2 million settlement, with $1.5 million going to the FTC and $1 million going to the New Jersey DCA. However, $300,000 of this was discharged, at a later date, leaving the final settlement at $2.2 million [13]

Morgan Stanley, an investment bank and financial services provider, has also been through a similar case. A lawsuit alleging unlawful treatment of personal data was filed against the banking behemoth in 2020. The plaintiffs claim in court documents that Morgan Stanley neglected to adequately “clean” equipment from its data centre between 2016 and 2019.

This led to a technical bug in the system that may have exposed the personal information of about 15 million users. After the equipment was deactivated, Morgan Stanley resold it to other parties, which made the situation even more difficult. The financial

[12] Enzuzo. "8 Biggest Data Privacy Lawsuits & Class Action Settlements." *Enzuzo*, 20 Aug. 2023, www.enzuzo.com/blog/data-privacy-lawsuits. Accessed 22 Aug. 2024.

[13] Enzuzo. "8 Biggest Data Privacy Lawsuits & Class Action Settlements." *Enzuzo*, 20 Aug. 2023, www.enzuzo.com/blog/data-privacy-lawsuits. Accessed 22 Aug. 2024.

institution first proposed to pay $120 million to settle the lawsuit; however, this amount was later lowered and verified to be $60 million. [14]

The rapid proliferation of digital surveillance technologies raises concerns that these systems could, in some cases, reify or even amplify discrimination. These biases are then carried over into the algorithms that power advanced surveillance systems—such as those based on Artificial Intelligence (AI) and facial recognition. Such technologies are often used in ways that over-police the marginalized, sometimes even leading to racial profiling or unwarranted malfeasance on poor populations. The use of surveillance in this way is not only an infringement on confidentiality but will also increase social justice, impartial treatment, and ethicality.

The methods of digital surveillance pose a great risk in terms of data breaches, in which extensive amounts of personal data are gathered and stored by not only governments but also by private entities. Consequences could be serious in case these repositories fall under attack, particularly in identity theft and even exposing sensitive personal information. Public awareness of the dangers of present monitoring tactics has increased as a result of high-profile incidents involving large firms or government database breaches. These occurrences serve as a reminder of the need for strong cybersecurity and the moral obligation of organisations to secure the data they gather to lower the possibility of harm to persons.

The issue of privacy and surveillance during pandemics

The concern for privacy and surveillance has been present throughout history, a phenomenon exacerbated during pandemics. Modern technology makes encroachment on personal freedoms much easier. Biometric data and other personal information are used under the excuse of protecting public health, raising major concerns. Tracking systems became essential in the management of public health even during the COVID-19 pandemic because they aided in monitoring the spread of the virus and determining the risks associated with infection on a personal level.

[14] Enzuzo. "8 Biggest Data Privacy Lawsuits & Class Action Settlements." *Enzuzo*, 20 Aug. 2023, www.enzuzo.com/blog/data-privacy-lawsuits. Accessed 22 Aug. 2024.

Geospatial tracking and modelling provided insight into outbreak patterns; the use of wearable devices and remote monitoring provided more health data—all far from just the physiological markers that wearables tracked in the past. Apart from these benefits, however, the systems came with their fair share of privacy and ethical challenges.

Data security in relation to user consent was pertinent to uphold public trust and, as such, effectiveness. The integration of these technologies has pointed out the possibilities of digital tools for public health but also underlined the necessity of a balance between innovation and safeguarding privacy. While these systems were put in place to reduce the spread of the virus, they have also raised concerns about the probability of AI surveillance being misused for other purposes than managing public health. There is a fear of such technology being used to track the movement of healthy people or collect sensitive information from the well and seriously sick, therefore violating the privacy of the personal nature.

This has created a decline in public trust as the introduction of AI-based surveillance during the pandemic expresses people's increasingly profound concerns as to whether such benefits would outweigh the privacy risks brought by technologies. Researchers have argued that AI surveillance, in this sense, is a form of biopolitics, meaning that forms of surveillance are utilised in pursuit of influencing public opinion and behaviour, further enhancing government control and oversight in ways that might compromise individual liberties. Experts have offered technological solutions to these ethical concerns through data de-identification, anonymisation, and differential privacy to safeguard personal information.

The issue of privacy and surveillance during conflict

Many military organisations and governments have used large-scale digital surveillance in the process of monitoring threats, keeping track of enemy movement, and ensuring security during armed conflict. This may involve the interception of communications, online activity tracking, and surveillance of social media. These practices could mean personal privacy violations, not only for combatants but also for civilians. The indiscriminate collection of data raises concerns about the erosion of privacy rights and opens up chances of abuse, in that most personal information is collected without consent or any form of oversight. For example, the Planning Tool for Resource Integration, Synchronisation, and Management (PRISM) is a clandestine national security electronic surveillance program operated by the United States National Security Agency (NSA) which

was disclosed in June 2013. The NSA has used it to collect data upstream from some of the US's largest internet firms, including Google, Facebook, Apple, and Microsoft. The powers stem from the Protect America Act of 2007, [15] and were reauthorised by legislation called the FISA Amendments Act of 2008. [16] Whereas PRISM targeted foreigners outside the U.S., with the exception of a few narrowly defined categories such as U.S. communications routed through American servers, officials found that the program was also collecting tens of millions of pieces of data by Americans. That included emails, synchronized video calls, and live feeds of other types of digital conversations.

The revelations of the scope and nature of PRISM sparked a broad public outcry over privacy rights by government agencies — including attempts to limit abuses through legislation on mass surveillance, or judicial action such as the BigBrotherAwards, an international debate about governmental security versus national consideration of civil liberties, and what information would be considered sensitive/secret for which governments Digital surveillance during armed conflict may inadvertently affect civilians. In this case, surveillance technologies gather data about people not directly involved in the conflict and might, therefore be used to harm or mistakenly target some. Sometimes, the data compiled from communications and location tracking misinterprets or provides impetus to execute a course of action that results in civilian casualties. These are the unintended effects that bring forth the moral dilemma that lies between military objectives and the protection of civilians.

The types of digital surveillance and their potential uses

Digital surveillance can come in many shapes and forms, covering its various uses. First of all, internet and network surveillance. Internet and network surveillance is the process of monitoring and analyzing data as it moves over networks. This is a type of surveillance through which authorities or organizations can inspect data packets closely with tools like Deep Packet Inspection (DPI) in search of specific content. Metadata collection gathers information regarding communications, such as who contacted whom and when. This type of surveillance is in wide application in cybersecurity, law enforcement, and intelligence. Advantages include enhanced security and cyber threat detection and

[15] Protect America Act of 2007." Congress.gov, Library of Congress, 5 Aug. 2007, www.congress.gov/bill/110th-congress/senate-bill/1927. Accessed 24 Aug. 2024.
[16] FISA Amendments Act of 2008, H.R. 6304, 110th Congress, 2nd Session. Congress.gov, Library of Congress. https://www.congress.gov/bill/110th-congress/house-bill/6304 .

prevention. On a negative note, there are a lot of privacy concerns in that it mostly includes monitoring people secretly, and state or corporate abuse or overreach.

Another key type of digital surveillance is social media surveillance. It uses tools and software to track, analyze and harvest data from social media platforms and profiles. It can be used to track public sentiment, individual activities, and monitor trends. It can also be a significantly important tool for the early identification of threats or even targeted advertising. In terms of advantages, social media surveillance has the ability to provide valuable insight concerning public opinion and early detection of potential risks. On the other hand, this type of digital surveillance can pose significant threats to the privacy of individuals, it facilitates the manipulation of public discourse, while at the same time creating a "non-safe" environment which may be characterized by censorship.

Another significant type of digital surveillance is location tracking. It involves the utilization of many technologies like the Global Positioning System (GPS), in pursuit of monitoring the real-time location of individuals or devices. It is commonly used in logistics, law enforcement, or even by apps on commonly used devices like smartphones. Location tracking can ensure advanced safety, efficient navigation and the ability to locate missing people or assets. However, it raises serious privacy concerns, as location tracking can result in a breach of a person's privacy, which can ultimately mean potential misuse of data by unauthorized parties. Legally, this aforementioned breach is addressed by numerous documents, for example, the Personal Data Protection Act (PDPA).[17]

Lastly, biometric surveillance is also important. It uses technology like fingerprinting and facial recognition to identify individuals. It can be used to enhance security, law enforcement, and access control. It can enhance security by quickly identifying individuals in various situations, from airports to crime scenes. Concerning its disadvantages, biometric surveillance can include significant privacy violations, especially if data is collected without consent or used for purposes beyond its original intent.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Islamic Republic of Iran

Iran's position is characterized by a complex balance between interests concerning national security and informational control. Digital surveillance was undertaken as a form of

[17] Taiwan. Ministry of Justice. Labor Standards Act. 1 Jan. 2018, https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021. Accessed 24 Aug. 2024

protection against threats or even political instability. This includes monitoring internet traffic, activities on social media, and communications; filtering and blocking access to several websites and platforms. Domestically, these measures are defended as necessary for the preservation of societal morals and principles of Islamic life. Internationally, however, such practices have received wide criticism from human rights activists, among others, on the grounds that they usually amount to violations of privacy, freedom of expression, and access to information.

Russian Federation

Russia's federation position towards digital surveillance is underpinned by the values of national security, social stability, and the protection of state sovereignty. Far-reaching systems of digital control are employed for the monitoring of activity on the internet, social media and even communications, ostensibly to preserve public order, and protect the nation from external interference. These surveillance practices are often seen as necessary for the maintenance of law and order, bearing in mind national interests. At the same time though, on an international level, these practices have raised significant concerns. It is argued that such surveillance can lead to the suppression of dissent and narrow access to information.

United Kingdom

In terms of digital surveillance, the United Kingdom (UK) is working towards keeping a balance between maintaining national security and privacy protections for its citizens. The UK government makes heavy use of digital surveillance for counterterrorism and domestic policing, under frameworks like the Investigatory Powers Act.[18] These measures are justified on the grounds that they serve public safety in a dangerous and integrated world. Some are doing this under the color of law but current legal thinking that otherwise un-intrusive blanket coverage is justified, though being disputed as overly preemptive and intrusive to civil liberties. Surveillance is carefully conducted under the rule of law to protect both national security and individual rights, but the debate over how that balance should be struck continues.

[18] Participation, Expert. "Investigatory Powers Act 2016." *Legislation.Gov.Uk*, Statute Law Database, www.legislation.gov.uk/ukpga/2016/25/contents. Accessed 31 Aug. 2024.

United States of America

The issue is complex for the United States of America (U.S.A), where there are public sensitivities to privacy and campaigns against domestic electronic surveillance in all of its forms. In the time following 9/11, with programs similar to PRISM and laws such as the USA PATRIOT Act, U.S. surveillance powers grew exponentially. They are seen as counterterrorism and a form of safeguarding the national interest. However, they have generated controversy on the grounds of privacy, arguing that mass surveillance can suppress freedoms and a means to promote "government overreach". Although surveillance is seen as a necessity for national security, this balance between security and personal liberties remains tenuous.

Amnesty International

Amnesty International, founded on the 28th of May 1961, consistently argues for the safeguarding of privacy and civil liberties in response to evolving digital surveillance capabilities. The group has stated that mass surveillance, existing without supervision can be a major human rights violation as it obstructs free speech and the right to privacy.[19] Amnesty International advocates for transparency, accountability, and strong safeguards to be established so that surveillance practices do not violate human rights. The organisation underlines that while security is essential, it should not be established at the expense of individual liberties and human dignity.

Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF), founded on the 6th of July 1990, is the first organization defending civil liberties in the digital world. The EFF contends that even basic levels of digital surveillance, much less mass monitoring programs, imperil rights to privacy and anonymity under international law. The organisation encourages the creation of policies and tools that combat indiscriminate surveillance, transparency, and accountability concerning monitoring programs, but also judicial oversight. The EFF works on the basis that digital rights ought to be protected in the ever-changing world of surveillance technologies.

Human Rights Watch

[19] Surveillance: The Legal and Human Rights Framework. 2015, https://www.amnesty.org/en/documents/pol30/2048/2015/en/. Accessed 24 Aug. 2024.

Human Rights Watch (HRW), founded in 1978, is deeply concerned about the human rights implications of digital surveillance, particularly the potential for such practices to violate privacy, freedom of expression, and other civil liberties. These violations fall under documents like the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICPR). The HRW highlights how surveillance can be used to target activists, journalists, and political dissidents, often in ways that undermine democratic principles and human rights. The organization calls for stronger legal protections, oversight mechanisms, and international standards to prevent abuse and ensure that surveillance is conducted in a manner that respects human rights. HRW advocates for a balance between security needs and the protection of individual freedoms, warning against the dangers of unchecked surveillance.

TIMELINE OF EVENTS

Date	Description of Event
10 December 1948	The Universal Declaration of Human Rights[20] was created in the 3rd GA Session.It was signed by 48 member states to establish a common standard of fundamental human rights to be universally protected, including rights such as equality before the law, freedom of expression, and the right to education.
1950	European Court of Human Rights (ECHR) Judgments[21]
28 May 1961	The creation of Amnesty International.
23 March 1976	The International Covenant on Civil and Political Rights[22] (ICCPR) was signed by 74 member states at the 21st GA session to commit its signatories to respect the civil and political rights of individuals, including the rights to life, freedom of speech, freedom of assembly, electoral rights, and the right to a fair trial.

[20] "Universal Declaration of Human Rights." United Nations, www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed 31 Aug. 2024.

[21] López Ribalda and Others v. Spain." European Court of Human Rights, Council of Europe, 17 October 2019, https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22López%20Ribalda%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-158649%22]}. Accessed 25 Aug. 2024.

[22] /nternational Covenant on Civil and Political Rights | Ohchr, www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Accessed 31 Aug. 2024.

9 December 1978	The Human Rights Watch was established.
12 October 1990	Establishment of the Electronic Frontier Foundation
18 December 2013	UN General Assembly Resolution 68/167[23] was drafted. It was signed by 193 member states on the 68th session of the GA, with the main objective of protecting the right to privacy in the digital age.
20 May 2013	Edward Snowden Revelations.
30 June 2014	Report of the UN High Commissioner for Human Rights.[24]It was created on the 27th GA session with the goal of addressing the right to privacy in the digital age
26 March 2015	UN Human Rights Council Resolution 28/16[25]. It was drafted during the 28th session of the Human Rights Council, with the goal of supporting the rights to privacy
8 March 2016	Report of the UN Special Rapporteur on the right to privacy. [26]Drafted on the 31st session of the GA, was to outline the mandate of the newly appointed Special Rapporteur on the Right to Privacy, Joseph Cannataci.

[23] A/RES/68/167, undocs.org/A/RES/68/167. Accessed 31 Aug. 2024.

[24] OHCHR | Report of the High Commissioner for Human Rights on Civil Society, www.ohchr.org/en/calls-for-input/report-high-commissioner-human-rights-civil-society. Accessed 31 Aug. 2024.

[25] *A/HRC/RES/28/16*, undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F28%2F16&Language=E&DeviceType=Desktop&LangRequested=False. Accessed 31 Aug. 2024.

[26] Special Procedures: Special Rapporteur on the Right to Privacy." Office of the High Commissioner for Human Rights, https://www.ohchr.org/en/special-procedures/sr-privacy. Accessed 25 Aug. 2024.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Universal Declaration of Human Rights

The Universal Declaration of Human Rights (UDHR)[27] is a milestone document in the history of human rights. It includes 30 articles that cover freedoms like speech, privacy, and the freedom to take refuge in another country. The UDHR is a key document in the landscape of international human rights law.

The link to digital surveillance is clear; there are two articles in the UDHR directly related to both privacy (Article 12) and freedom of expression rights (Article 19). Invasive or unregulated digital surveillance practices can potentially violate those rights. The increasing ability of governments and corporations to monitor what people are doing online means that there are dangers associated with these activities, as it signals an erosion of certain basic rights. It is critical to preserve the principles present in the UDHR by keeping surveillance practices from further violating human rights online.

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR)[28] is an international treaty signed by the UN General Assembly in 1966 (21st session) committing the Member States that signed the Covenant to respect the values of individual liberty. Examples include the right to privacy, freedom of speech, and freedom from arbitrary detention. In addition, Article 17 of the ICCPR specifically prohibits arbitrary or unlawful interference with a person's privacy in his family life, home, and correspondence. The ICCPR provisions are therefore important in the digital surveillance context because they establish a legal framework that states must follow to ensure that, when carrying out their surveillance activities, these rights and freedoms are protected.

---

[27] Universal Declaration of Human Rights." United Nations, https://www.un.org/en/about-us/universal-declaration-of-human-rights. Accessed 25 Aug. 2024

[28] "International Covenant on Civil and Political Rights." United Nations Human Rights Office of the High Commissioner, 16 Dec. 1966, www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Accessed 20 Aug. 2024.

UN General Assembly Resolution 68/167 (2013)

The UN General Assembly Resolution 68/167[29], adopted in December 2013 addresses the right to privacy in the digital age, concerned with how surveillance is conducted digitally and its implications on privacy rights. It highlights the importance of states meeting their international law obligations in protecting privacy, even when confronted with security concerns. The resolution urges a review of surveillance practices to ensure they are not violating human rights. It reaffirms that the protection of individual rights can only be achieved if oversight mechanisms are in place for such activities.

UN Human Rights Council Resolution 28/16

Based on the concerns of Resolution 68/167, in 2015 the UN Human Rights Council passed the UN Human Rights Council Resolution 28/16[30]. This resolution was based on the concerns of Resolution 68/167. It highlights the need for all Member States to ensure respect for freedom of expression, privacy, and human rights online in their digital communications. It calls upon them to specifically examine laws and practices that govern surveillance activities, ensuring conformity with international obligations surrounding human rights. The resolution also reinstates the important role of vigilance and discussion when it comes to privacy in the digital age, including indirectly supporting the work of the UN Special Rapporteur on Privacy.

Report of the UN Special Rapporteur on the right to privacy (2016)

The report, presented by the UN Special Rapporteur on Privacy[31], is associated with state surveillance and its implications for the right to privacy. It highlights overzealous surveillance and demands greater safeguards to enshrine individuals' privacy rights. It recommends that surveillance activities should be carried out in a manner compliant with

---

[29] A/RES/68/167, undocs.org/A/RES/68/167. Accessed 31 Aug. 2024.

[30] *A/HRC/RES/28/16*, undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F28%2F16&Language=E&DeviceType=Desktop&LangRequested=False. Accessed 31 Aug. 2024.

[31] Special Procedures: Special Rapporteur on the Right to Privacy." Office of the High Commissioner for Human Rights, https://www.ohchr.org/en/special-procedures/sr-privacy. Accessed 25 Aug. 2024.

transparency, oversight, and accountability in order for human rights protection to coexist alongside security imperatives.

Report of the UN High Commissioner for Human Rights (2014)

The report on Human Rights in the digital age [32] highlights concerns raised by the UN High Commissioner for Human Rights, Michelle Bachelet, regarding the effect of digital surveillance on privacy and other human rights. The report stresses that surveillance if carried out at all, must meet principles of necessity and proportionality to be compatible with international human rights law.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

European Court of Human Rights (ECHR) Judgements

The European Court of Human Rights (ECHR)[33] has issued a number of judgments concerning digital surveillance. They emphasize the need to balance national security measures with individual privacy rights. For example, in the case of Big Brother Watch v. the United Kingdom (2018)[34], the court ruled that the UK's surveillance programs violated the EU Convention on Human Rights,[35] particularly Article 8, which grants the right to respect for private life. The role of the European Court of Human Rights (ECHR) in advancing the ethical implications of digital surveillance is critical as it interprets and applies privacy rights under the European Convention on Human Rights. So far, it has acted as a vital brake on state surveillance powers to ensure that the state applies full consideration of necessity and proportionality while safeguarding the freedoms of individuals. Cases such as Big Brother

[32] United Nations High Commissioner for Human Rights. Report of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age. United Nations, 30 June 2014. A/HRC/27/37.

[33] "López Ribalda and Others v. Spain." European Court of Human Rights, Council of Europe, 17 October 2019, https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22López%20Ribalda%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22],%22itemid%22:[%22001-158649%22]}. Accessed 25 Aug. 2024.

[34] Big Brother Watch v. United Kingdom." Global Freedom of Expression, Columbia University, https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/. Accessed 25 Aug. 2024.

[35] Convention for the Protection of Human Rights and Fundamental Freedoms." Council of Europe, 4 November 1950, https://70.coe.int/pdf/convention_eng.pdf. Accessed 25 Aug. 2024.

Watch v. United Kingdom provide important test cases that address the balance of national security and privacy considerations that inform states' implementation of surveillance measures and establish considerable evidence in the interpretation of the Convention. That said, the ECHR is limited in a couple of important ways—enforcement and pace of legislative and technological change. While the challenging dimensions of the ECHR need to be taken into account, and noted, the review and findings of the ECHR are nevertheless crucial and relevant in advancing ethical considerations for contemporary digital surveillance dilemmas; it has the demonstrated capability of providing improved awareness of transparency, oversight, and respect for human rights in response to rapidly evolving technology in practice.

Edward Snowden Revelations

In late May 2013, the Guardian reported that telephone records of millions of Americans were collected by the National Security Agency (NSA). Edward Snowden, a former Central Intelligence Agency (CIA) systems analyst, leaked classified documents, revealing the collection of these records. The revelations became the catalyst for public debate concerning privacy, government overreach, and the ethics of surveillance. Even though they sparked a number of legislative reforms such as the USA FREEDOM Act, which aimed to limit certain surveillance practices, they did not manage to resolve the fundamental problems connected to digital surveillance, seeing as the underlying infrastructure of surveillance remains intact and governments are resuming the development of new technologies that circumvent existing regulations. These revelations[36] showed that NSA surveillance activities were not limited to the United States but targeted U.S. citizens and foreign leaders or governments. The leaks generated an enormous amount of public debate about privacy and civil liberties, which in turn led to calls for reform in surveillance practices and human rights concerns relative to national security. His activities also raised tension over international relations and became a factor in the review of international cooperation in intelligence gathering—a turning point in the ever-developing debate about privacy and state surveillance.

[36] Snowden, Edward. "NSA Files: Decoded – The Full Story of How the World Was 'Turned Upside Down'." The Guardian, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded?ref=quillette.com.

The Guardian and The Washington Post Reports

The Guardian and The Washington Post were critical in determining whether digital spying had become a problem or an accepted element of society. Their discoveries have uncovered very disturbing state data mining, as well as the amount of intelligence the government is keeping hidden behind closed doors. These revelations have demonstrated exactly how widespread and indiscriminate surveillance is, bringing some of the hazards to privacy and civil rights to light for a public that most likely had no idea what was going on. Their discoveries have shed light on these tactics, sparking public debates about the ethics of digital surveillance as well as requests for more privacy protections and greater openness in government operations. While they have helped to publicize the problem and drive regulatory changes. This growth of surveillance technology is compounded by the way digital communication unfolds on a global, decentralized level, and it presents an issue that existing models to protect privacy struggle with.

POSSIBLE SOLUTIONS

Legislative measures internationally

Legislation on an international level can address the ethical implications of digital surveillance. Generally, it can create a legal base by creating a unified front against violations of privacy. It can set privacy standards that member states will be encouraged to adhere to and therefore provide a consistent level of privacy protection globally. Without the presence of these international standards, individuals or even organizations in countries with weaker legislation on the matter become vulnerable to cases of data breaches and data misuse and exploitation. At the same time, by establishing these international standards, legislation on a national level can be harmonized. Currently, the global landscape is characterized by a patchwork of different national privacy protection laws, every one of them with different rules and requirements. Thus, by establishing these aforementioned standards, member states can follow the lines of the international community, creating uniformity.

Collaboration of organizations

Collective efforts leveraging the power of organizations, legislators, and technology companies will contribute to a secure digital world that respects user privacy. It is critical that organisations use clear policies around data profiling to perform the practice responsibly, equitably, and transparently. This may entail using fair algorithms, and explaining to users how their data is being harnessed. Regular check-ups can prevent any unfair action and will secure transparency. This approach leads to increased user trust and preservation of ethical principles, by reassuring the users for the safety of their data and encouraging a more ethical approach. But in addition to that, there are also some disadvantages, like the high cost of deployment and technical complexity in designing artificial intelligence that is fairly balanced with business when profiling is restricted.

Technical protection

Finally, to ensure user data security through, for instance, encryption, multi-factor authentication, and regular updates, technology firms must create systems with high-end security capabilities. However this comes with its share of disadvantages, such as the expensive nature of formulating these protective actions by companies when it comes to the privacy question, like the high costs associated with coming up with these security measures borne from developing new software programs, there could be backlash if people did not want to be responsible for their own privacy, etc., or even being overconfident with our own protection, which might make us careless when handling personal data.

BIBLIOGRAPHY

ForumCosmos. “Ethical Considerations in Data Privacy and Security.” Medium, 13 July 2023, medium.com/@armaanakhan91/ethical-considerations-in-data-privacy-and-security-1874a10061f0. Accessed 16 July 2024.

Internet Encyclopedia of Philosophy, iep.utm.edu/surv-eth/. Accessed 16 July 2024.

Saheb, Tahereh. “‘ethically Contentious Aspects of Artificial Intelligence Surveillance: A Social Science Perspective’ - Ai and Ethics.” *SpringerLink*, Springer International Publishing, 19 July 2022, link.springer.com/article/10.1007/s43681-022-00196-y. Accessed 16 July 2024.

ForumCosmos. “Ethical Considerations in Data Privacy and Security.” Medium, Medium, 13 July 2023, medium.com/@armaanakhan91/ethical-considerations-in-data-privacy-and-security-1874a10061f0.

Consent | English Meaning - Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/consent. Accessed 19 July 2024.

Data Breach | English Meaning - Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/data-breach. Accessed 19 July 2024.

Wiretapping | English Meaning - Cambridge Dictionary, dictionary.cambridge.org/dictionary/english/wiretapping. Accessed 19 July 2024.

Santiago, David. “History and Evolution of Video Surveillance Technology.” 3Sixty Integrated, 2 Aug. 2023, www.3sixtyintegrated.com/blog/2023/07/26/history-video-surveillance/. Accessed 02 Aug. 2024.

“The 9/11 Effect and the Transformation of Global Security.” Council on Foreign Relations, www.cfr.org/councilofcouncils/global-memos/911-effect-and-transformation-global-security. Accessed 02 Aug. 2024.

Hartig, Hannah. “Two Decades Later, the Enduring Legacy of 9/11.” Pew Research Center, 2 Sept. 2021, www.pewresearch.org/politics/2021/09/02/two-decades-later-the-enduring-legacy-of-9-11/. Accessed 02 Aug. 2024.

The Informed Consent Challenge." Electronic Frontier Foundation, www.eff.org/issues/informed-consent. Accessed 2 Aug. 2024.

Smith, Richard. “The Limitation Principle in Data Protection Laws.” International Journal of Law and Information Technology, vol. 24, no. 1, 2016, pp. 22-45. Oxford Academic, academic.oup.com/ijlit/article/24/1/22/583212. Accessed 2 Aug. 2024.g

Data Protection and Privacy." European Commission, ec.europa.eu/info/law/law-topic/data-protection_en. Accessed 2 Aug. 2024.

"Surveillance and Discrimination: The Impact of Technology on Marginalized Communities." Journal of Information Technology & Politics, vol. 15, no. 1, 2018, pp. 1-20. Taylor & Francis Online, www.tandfonline.com/doi/full/10.1080/19331681.2018.1469118. Accessed 2 Aug. 2024.

"Global Data Breach Statistics." Breach Level Index, breachlevelindex.com/. Accessed 2 Aug. 2024.

"The Impact of Digital Surveillance on Human Rights." *Human Rights Watch*, 11 Dec. 2018, www.hrw.org/report/2018/12/11/big-data-and-human-rights-impact-privacy-and-surveillance. Accessed 2 Aug. 2024.

"Digital Surveillance and Human Rights." *Amnesty International*, www.amnesty.org/en/what-we-do/digital-surveillance/. Accessed 2 Aug. 2024.

"The Use of Digital Technology in Armed Conflict." *International Committee of the Red Cross (ICRC)*, www.icrc.org/en/document/technology-war-and-humanitarian-law. Accessed 2 Aug. 2024.

"The Impact of Digital Surveillance on Civilian Protection." Journal of Conflict and Security Law, vol. 20, no. 3, 2015, pp. 405-426. Oxford Academic, academic.oup.com/jcsl/article/20/3/405/5852848. Accessed 2 Aug. 2024.

"Bias in Surveillance Technologies." Electronic Frontier Foundation (EFF), www.eff.org/issues/surveillance. Accessed 2 Aug. 2024.

“How AI Can Perpetuate Discrimination in Surveillance.” MIT Technology Review, 16 July 2020, www.technologyreview.com/2020/07/16/ai-surveillance-bias/. Accessed 2 Aug. 2024.

“Surveillance and Accountability in Armed Conflict.” Oxford University Press, vol. 30, no. 4, 2019, pp. 321-340. Oxford Academic, academic.oup.com/ijlit/article/30/4/321/5555830. Accessed 2 Aug. 2024.

"Guidelines on Digital Surveillance and Human Rights." UN Human Rights Council, www.ohchr.org/en/documents/tools-and-resources/guidelines-digital-surveillance. Accessed 2 Aug. 2024.

The Long-Term Impact of Digital Surveillance in Conflict Zones." Brookings Institution, 15 Sept. 2021, www.brookings.edu/research/the-long-term-consequences-of-digital-surveillance/. Accessed 2 Aug. 2024.

“Surveillance Data and Its Long-Term Implications.” International Journal of Human Rights, vol. 24, no. 8, 2020, pp. 1127-1145. Taylor & Francis Online, www.tandfonline.com/doi/full/10.1080/13642987.2020.1831580. Accessed 2 Aug. 2024.

Tait, Robert. “Iran: Authorities Step up Online Surveillance of Dissidents.” The Guardian, 4 Apr. 2023, www.theguardian.com/world/2023/apr/04/iran-authorities-step-up-online-surveillance-of-dissidents. Accessed 3 Aug. 2024.

“Iran’s Internet Censorship and Surveillance.” *Human Rights Watch*, 24 Feb. 2021, www.hrw.org/news/2021/02/24/irans-internet-censorship-and-surveillance. Accessed 3 Aug. 2024.

“Digital Authoritarianism: Iran’s Use of Surveillance Technology.” *Freedom House*, freedomhouse.org/report/digital-authoritarianism/iran. Accessed 3 Aug. 2024.

“Surveillance and Repression in Iran.” *Amnesty International*, www.amnesty.org/en/latest/news/2022/11/surveillance-and-repression-in-iran/. Accessed 3 Aug. 2024.

“Russia's Surveillance State: Domestic Controls and the Kremlin's Digital Influence Abroad.” *Council on Foreign Relations*, 1 Sept. 2023, www.cfr.org/russias-surveillance-state. Accessed 3 Aug. 2024.

Soldatov, Andrei, and Irina Borogan. “Russia’s Digital Surveillance State.” *Foreign Affairs*, 5 Apr. 2022, www.foreignaffairs.com/articles/russia/2022-04-05/russias-digital-surveillance-state. Accessed 3 Aug. 2024.

“The Evolution of Russia's Surveillance State.” *Human Rights Watch*, 17 Mar. 2021, www.hrw.org/news/2021/03/17/evolution-russias-surveillance-state. Accessed 3 Aug. 2024.

“Russia: Digital Surveillance and the Right to Privacy.” *Amnesty International*, www.amnesty.org/en/latest/news/2022/09/russia-digital-surveillance-right-to-privacy/. Accessed 3 Aug. 2024.

“Investigatory Powers Act.” *UK Government*, www.legislation.gov.uk/ukpga/2016/25/contents/enacted. Accessed 3 Aug. 2024.

“The USA PATRIOT Act: Preserving Life and Liberty.” *U.S. Department of Justice*, www.justice.gov/archive/ll/highlights.htm. Accessed 3 Aug. 2024.

“Edward Snowden: Leaks That Exposed US Spy Programme.” *BBC News*, BBC, 17 Jan. 2014, www.bbc.com/news/world-us-canada-23123964. Accessed 11 Aug. 2024.