Forum: Disarmament and International Security Committee

Issue # 1: The question to the right of privacy regarding mass surveillance

Student Officer: Santiago Rojas, Renee Purcait, Jorge Saa, Carla Saliot

Position: Chair of Disarmament and International Security Committee

---

Introduction

Mass surveillance exposes individuals to excessive and indiscriminate monitoring leading to an obvious and blatant violation of both the right of privacy and the freedom of speech. Society is profoundly perturbed that electronic surveillance may intercept digital communication and amasse personal data without any defined protocole to use it, store it, share it or destroy it. It has been proven that mass surveillance decomposes the freedom of intellectuals, it hurts the connections between societies, and it gives path to imperfect and illegal portrayal of people while compiling useful information that can be employed to manipulate people, predict their behavior or simply be sold. While mass surveillance is needed to prevent terrorist attacks, catch the most wanted criminals or even track contact cases during pandemies, it has to be done within a legal framework that complies with human rights and safeguards our basic privacy and liberties. Information is power, and compiling all kinds of information on everybody may result in a very dangerous game if used unethically.

Definition of Key Terms

Global Surveillance:

Can be defined as the close observation and monitoring of entire populations across nations. It is ordinarily carried out with the complex collection of data from cell phones, laptops, search history, social media, and telecommunication applications.

Artificial Intelligence and Machine Learning:

A surging branch of computer science where computers are built to perform tasks that would require human intelligence. Artificial Intelligence is developed through the process of machine learning which allows the computer to learn and improve from experience automatically.

Biometrics:

A type of metrics related to physical human traits and characteristics used to verify identity. Physiological traits, eyes, fingerprints, voice recognition, and behavioral characteristics are examples of the most common biometrics used in today's society.

Right to Privacy:

The right to not have personal matters nor affairs publicly disclosed or publicized and to be left alone. Furthermore, it refers to the right of being left alone, and the right to the protection by the law from privacy attacks or interferences.

Big data:

A term in computer science is used to describe data that is so large, fast, and complex that it becomes too difficult for traditional management tools to manage it or store it. For example, The New York Stock Exchange generating one terabyte of new trade data every day would be considered big data.

Communication Surveillance:

The process of a third party intercepting communication during the course of its dispatch. This may include monitoring, copying, recording, storing, or diverting the transmission.

General Overview

Instead of restricting surveillance to individuals with a fair suspicion of wrongdoing, mass surveillance employs programs or technology that capture, analyze, or produce data on an infinite or large number of people. Governments can monitor nearly any part of our lives using modern modes of mass surveillance. Mass surveillance may expose an entire community or a large portion of it to indiscriminate monitoring, resulting in a systemic violation of people's right to privacy and all the protections that privacy provides.

The storage, processing, generation, interpretation, use, retention, or storage of information about numerous people, regardless of whether they are guilty of wrongdoing, is referred to as mass surveillance.

The issue with mass surveillance from a legal standpoint is that it is neither strictly appropriate nor proportionate in a democratic society. There are alternatives available that are less invasive. Mass surveillance allows for arbitrary state influence and control over individuals by routinely tracking people's lives. The presumption that all information could be useful to counter a hypothetical danger underpins mass surveillance, which is incompatible with democratic ideals and principles that aim to restrict the information a state knows about its citizens in order to moderate its control. Mass surveillance further obstructs the division of powers because the executive branch is able to carry out its activities without the two other branches of government - legislative and judicial -

providing adequate oversight. Since the right to surveillance is authorized in bulk rather than for each instance of infringement, mass surveillance forces lack effective independent authorisation. It generates mistrust that is incompatible with democratic ideals and standards, in which everyone is presumed guilty unless proven innocent in the eyes of the law.

Mass surveillance has a negative impact on other human rights and freedoms, as unjustified invasions of privacy prohibit the enjoyment of other rights and frequently serve as a gateway to violations of other human rights.

Some Types of Mass Surveillance

FBI monitoring of email and electronic communications: consists of a system implemented by the FBI that uses a special list of key-words to look for possible and suspicious references that might call the FBI's attention. It is used to find and track drug traffickers, terrorists, fugitives, etc.

License-plate cameras at intersections: cameras located in intersections that take pictures of "offending cars" and its license plate to send a traffic ticket to the owner. These cameras were placed to easily punish every person who skipped a red light or committed any other type of traffic transgressions.

Surveillance cameras in public places: these cameras are placed in areas that have some history of having criminal activities, subway stations, or areas that are regularly crowded. These cameras record every single activity of people who are in these places without them even knowing.

Geolocation tracking on cell phones: The GPS tracking system that smartphones use are great to always keep track of where you are and where your family members and friends are at. This tracking system also allows government officials

to know where you are at all times. The government has the authority to track all of your steps and moves using your phone GPS when you are connected to wifi or your smartphone data.

Biometric Identification: biometric identification consists of scanning different parts of your body as a way of authentication. Instead of writing your password you can just show your face or place a fingerprint to be allowed to get in a place, to your phone etc.

Terrorism

Mass surveillance technology is of significant advantage to insights offices and law requirement authorities in spite of the fact that the Parliamentary Gathering of the Board of Europe has addressed their viability in terms of counter-terrorism anticipation. The utilization of modern insights innovations empowers government authorities to memorize an awesome bargain from metadata. Such innovations can filter through endless sums of information and organize it into categories. For example, in dissecting little bank exchanges to distinguish suspicious cash exchanges, counterfeit insights programs may construct a complex preview of how account holders oversee their cash which may encourage the discovery of cash washing or fear based oppressor financing exercises. Undoubtedly, the collection of metadata can uncover more data almost an individual's conduct, inclinations and social connections

The General Assembly expressed their concern with respect to the potential negative results of such mass information observation capability and procedures. In expansion to encourage States to secure the correct protection of people when they are both on and offline. They called on all States to survey their enactment, methods and hones overseeing communications

reconnaissance, the collection of individual information, and the interferences of individual communications.

Mass Surveillance Revelations

In 2013, Edward Snowden, former computer intelligence consultant, uncovered that GCHQ was furtively interfering with millions of people's private communications, indeed when those individuals were clearly of no insights intrigued. The data collected and put away by the government can uncover the foremost insinuating viewpoints of a person's private life – where they go, who they contact, which web destinations they visit and when.

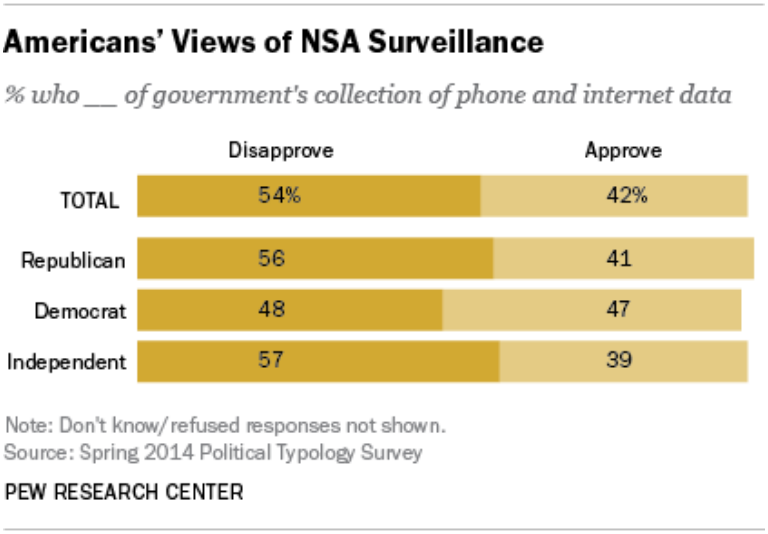
In 2014, the highly secretive Uk court ruled that these technologies may in rule comply with the UK's human rights commitments. This was the finding hence challenged within the European Court of Human Rights, which incompletely ruled against the UK in 2018. In any case, the judgment did not go far enough, and the amalgamation brought the case to the Amazing Chamber.

Major Parties Involved and Their Views

United States

As a member of the "Five Eyes Alliance", an alliance comprised of five members which would share intelligence obtained through mass surveillance, the United States has a strong belief that mass surveillance is worth the privacy breach. Not only do they believe in mass surveillance, but they exercise it through their National Security Agency (NSA) and acquire data from devices such as cellphones and computers from 193 different countries and share this information with security agencies of member countries of the "Five Eyes Alliance"(Amnesty International UK). However, a majority of the country's population (54%) disapproves of this surveillance on behalf of the NSA (Gao).

U.S. Citizens' Views Regarding Surveillance from the NSA



United Kingdom

The United Kingdom (UK) is another member of the "Five Eyes Alliance" and believes that mass surveillance should be possible, regardless of the arguments made against it due to the privacy breach (Amnesty International UK). However, in recent years, the European Union (EU) Court has declared the actions of the UK to be illegal and illegitimate. This is because, according to the 2016 Investigatory Powers Act (IPA) and the Privacy and Electronic Communications Regulations (PECR), a member state of the EU "cannot legally require a service provider to indiscriminately retain traffic and location data for national security purposes." (Afifi-Sabet). Nevertheless, the nation has been actively using telecommunications companies to collect personal data destined for national security. This then provides an argument for which Brexit should occur due to this "unfair trial" against the United Kingdom.

Canada

Just like the United States and the United Kingdom, Canada is a member of the "Five Eyes Alliance" (Amnesty International UK). It also believes in the power of mass surveillance and on using it for national security. In fact, the Canadian

government has its own Communications Security Establishment (CSE) Act which is updated constantly. This act has become very important for the government as, in 2012, the government was able to spy on Canadians using public WiFi networks at the airports. This generated great controversy within the nation, however the government was excused by saying that they were only collecting metadata, data that is still legal according to the CSE. However, many Canadians and experts have expressed that, in fact, metadata can reveal a lot about an individual (International Civil Liberties Monitoring Group).

China

The Chinese government is an example of a continuous and a highly developed system of mass surveillance. The Chinese government has invested into the installation of security cameras and, in the past years, the implementation of Artificial Intelligence Facial Recognition. Mass surveillance is so important in China that 16 out of the 20 most surveilled cities in the world are in China, with the most surveilled being the city of Taiyuan. This city has 117.02 cameras per 1,000 citizens (Bischoff). In fact, China has used mass surveillance in a way that has allowed them to place around 1 million people into what they call "re-education centers" in the region of Xinjiang alone (Campbell).

North Korea

North Korea is another government that is highly involved with the usage of mass surveillance. The government of North Korea "has absolute and systematic control of all forms of telecommunications." The North Korean government has a division called 'Bureau 27' which monitors and detects mobile phones. This is to the point at which a person caught attempting to make an international phone call would be arrested (Amnesty International UK). At the same time, due to the situation of its frontiers, the government has developed an "Intelligent Unmanned Surveillance CCTV" system that, supposedly, could monitor a specific person with a 99.5% accuracy. This technology was being developed to have greater control over its residents (CIVICUS).

Timeline of Events

Date	Description of event
1946	With World War II over, the Five Eyes Alliance is created. This alliance consists of security agencies from the United States, the United Kingdom, Australia, Canada and New Zealand (Privacy International).
2001	The terrorist attacks of 911, shock the world and push governments worldwide into using mass surveillance to prevent such threats from entering their countries and from planning such attacks in the near future. This makes the United States reinforce the role of the National Security Agency (NSA) by having the agency ask private companies to send telephone and internet metadata to them (Electronic Frontier Foundation).
2005	The New York Times exposes spying from the NSA and U.S. President George Bush confirms these statements (Risen and Lichtblau).
2013	Edward Snowden, former NSA contractor, reveals the NSA's practices and it's mass surveillance methods. He also reveals that the agency monitors internet and phone communications in 193 countries. Snowden states, "We've got agencies looking through webcams into people's bedrooms, and they're collecting billions of cell phone location records a day. They know where you got on the bus, where you went to work, where you slept, and what other cell phones slept with you." (Amnesty International UK).
2016	The Canadian Security Intelligence Service (CSIS) is taken to court for illegally storing and analyzing metadata. This is due to the fact

	that, according to the Canadian government, metadata can only be stored if it has anything to do with national security threats, investigations or international affairs (Murphy).
2019	Chinese telecommunications companies, such as Huawei, are banned from the United States for national security purposes. This is due to the U.S. government fearing that such companies are constantly spying on its citizens through their technology. By doing this, the Chinese companies would surveill the U.S. population and acquire data that would then be transferred to the Chinese government (Keane).
2020	The European Union Court of Justice condemns the United Kingdom's methods of mass surveillance as illegal due to its violations to the Privacy and Electronic Communications Regulations (PECR). This is because the government of the UK was collecting information from telecommunications companies which is legal according to the UK. Nevertheless, it is illegal according to EU laws (Afifi-Sabet).
2021	The European Commission (EC) makes a proposal for a new law regarding artificial intelligence (AI) and mass surveillance. This new law would restrict the use of some of the biometric mass surveillance cases and methods (European Digital Rights).

UN involvement, Relevant Resolutions, Treaties and Events

The OHCHR (The Office of the United Nation High Commissioner for Human rights) acknowledges the right of privacy and the consequences of online mass surveillance.

"States should be transparent about the nature and extent of their internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use," Mr. Emmerson said. Mr. Emmerson is a special rapporteur on the promotion and protection of human rights and fundmetal freedoms while countering terrorism.

On June 14th 2014, the United Nations Human Right Council Assembly, adopted the resolution A/HRC/ 27/37concerning the protection of rights privacy in connection with mass surveillance.

The United Nation High Commissioner for Human Rights, Navi Pillay, on his report on July 16th 2014 emphasized the fact that "mass surveillance is emerging as a dangerous habit rather than an exceptional measure". According to him, the measures taken if really needed and have to be in proportion with a legitimate claim to a risk.

Past action

The Parliamentary Assembly of the Council of Europe

The Parliamentary Assembly of the Council of Europe presented their concerns of using "mass surveillance" through a resolution published in 2015. Furthermore, the assembly has come to express their deep concerns on the possibility that the surveillance technology, that was developed by the United States and its allies, would end up in authoritarian regimes and endanger the fundamental human rights of its citizens. The assembly also stated that the use of mass surveillance tools does not appear to improve nor contribute to the prevention of terrorist attacks. As a result of such concerns and more, the resolution urged members and observers to encourage the use of encryption tools for individuals to ensure

further privacy and to "enact laws that make any collection of data without the consent of the person involved subject to judicial review, while making no distinction between data and metadata." They also suggested agreeing on a multilateral "intelligence codex". This would further prevent the participant states of the agreement from spying on each other, thus protecting the citizens of those states.

Global Network Initiative

The Federal Government of the United States emphasized the need for a public debate for balancing the use of communication surveillance and privacy. As a non-governmental organization to prevent internet censorship, the Global Network Initiative or the GNI has urged governments and the United States for transparency regarding their laws and regulations. Furthermore, the Global Network Initiative has stated the need to inform the public and keep close ties for representatives of the public for greater visibility on communication surveillance.

"Encrypt Everything"

In 2013, former Google CEO, Eric Schmidt proposed that the solution to government surveillance was to "encrypt everything. Seeing as the data collection and monitoring of the National Security Agency (NSA) was exposed recently, Eric Schmidt proposed this idea with the hope that it could "open up countries with strict censorship laws," and give the public a "voice."

Snowden Treaty

Formally titled, "The International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistleblowers," Edward Snowden and his team proposed this treaty on September 24, 2015. In Snowden's campaign for a new global treaty against mass surveillance, Edward

Snowden argued that mass surveillance violates international law on privacy in the Universal Declaration of Human Rights. The treaty would further expand on this topic and propose the termination of mass surveillance and a mechanism that would monitor and improve compliance.

In the past years, several organizations and communities, in general, have brought attention to their discomforts towards mass surveillance, and although in several cases their best form of action is urging and suggesting, the work of bringing awareness and giving a voice to the public is crucial and beneficial. Several ideas proposed still are possibilities to be considered and possibly acted upon. Encryption is a powerful solution that is not being completely utilized as of today. The Snowden Treaty on the other hand presented radical ideas that experts deem to fail for such extreme measures and proposals.

Possible Solutions

Promoting the implementation of encryption worldwide has been an effective solution to combat mass surveillance. When a message is encrypted it can't be seen or manipulated by any user who is not authorized, protecting your privacy and any sensitive information you may have.

Creating measures to control Mutual Legal Assistance Treaties (MLAT's) to make sure they are following the guidelines, protecting human rights of privacy, and that they provide all the information on how the data collected will be used. Creating a law to limit the use of information gathered during MLAT's.

The establishment of new mandates for Special Rapporteurs on the right of privacy, seeking advisory for an opinion from the International Court of Justice and the to educate citizens on the issue.

Sustainable Development Goal (SDG)

Sustainable Development Goal number 16 is "**Peace, Justice and Strong Institutions**". This connects to the issue at hand due to the fact that reaching an agreement between the government and the people on mass surveillance would clearly strengthen governmental as well as private institutions. This would be since it could increase the trust between the people and these institutions. Addressing this issue would also bring peace of mind to the citizens that are being surveilled as it would allow them to protect their own human rights. These include but are not limited to freedom of speech and expression and, right to liberty and security. Overall, discussing this issue will strengthen human civilization as a whole by understanding different perspectives and what they imply.

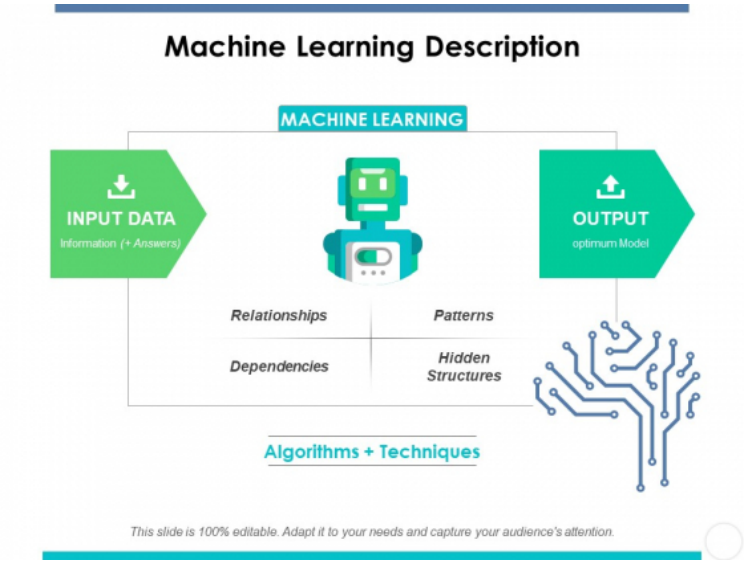
Appendix

I. The history of mass surveillance in the United States.

https://www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=4c12b845b62d

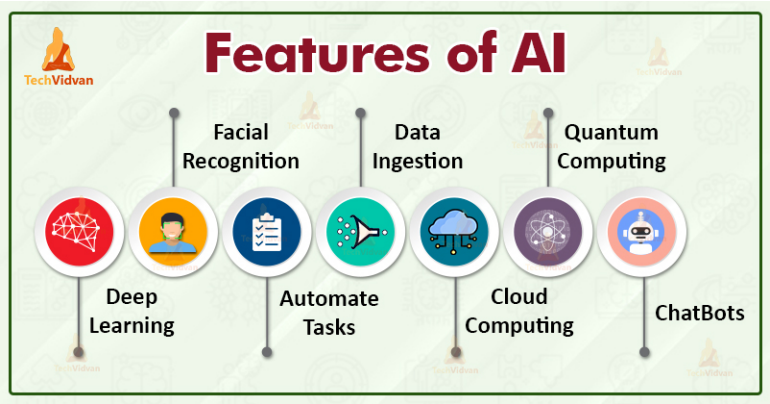
II. An in-depth explanation of Machine learning.

https://www.expert.ai/blog/machine-learning-definition/



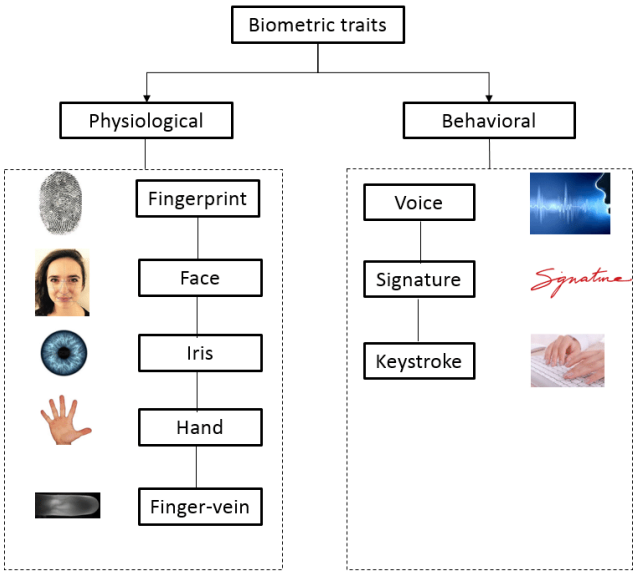
III. An in-depth explanation of Artificial Intelligence

https://builtin.com/artificial-intelligence



IV. Description and exposition of what biometrics and biometric data is.

https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html



V. The International Covenant on Civil and Political Rights, a multilateral treaty adopted by the United Nations General Assembly.

https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

VI. The Parliamentary Assembly statement of Mass Surveillance.

https://ccdcoe.org/incyder-articles/mass-surveillance-endangers-human-rights-and-does-not-prevent-terrorist-attacks-says-council-of-europe/

VII. Statement from Ben Emmerson, a United Nation Human Rights expert on online mass surveillance.

https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200&LangID=E

VIII. United National General Assembly report on "the right to privacy in the digital age.
A/HRC/27/37 A/HRC/27/37 United Nations A/HRC/27/37 …

IX. A detailed report on the background of mass surveillance and the importance that it has for governments.

https://www.southampton.ac.uk/~mwra1g13/msc/comp6048/government-mass-surveillance.html

X. Article discussing the negative repercussions that mass surveillance might have on society.

https://www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it

XI. A United Nations briefing on the "right to privacy on the digital age"

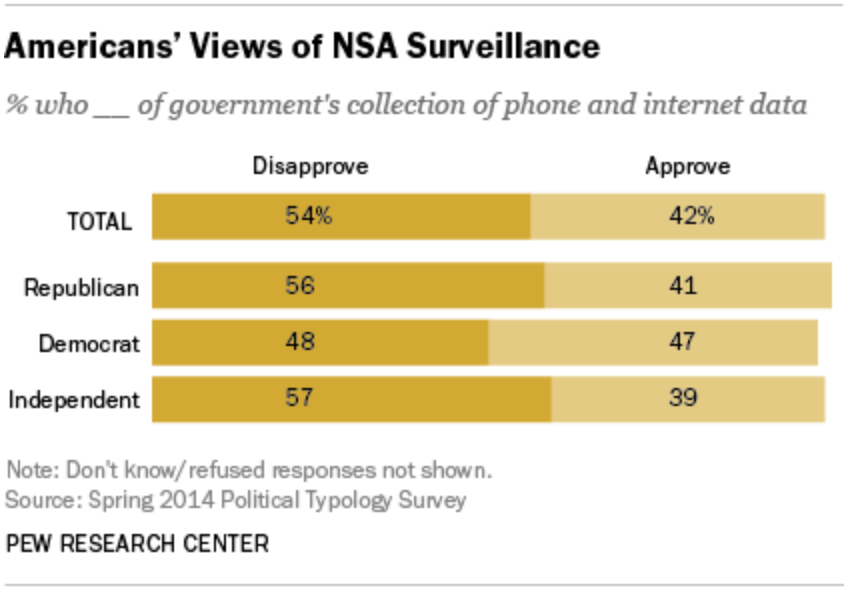
https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age

XII. Article by Amnesty International arguing against mass surveillance.

Evidence of global opposition to US mass surveillance | Amnesty International UK

XIII. Report of the American citizens point of view in relation to mass surveillance, national security, and privacy.

What Americans think about NSA surveillance, national security and privacy | Pew Research Center



XIV. A report on the European Union Court declaration of "UK 'mass surveillance' regime"

UK 'mass surveillance' regime is illegal, EU court declares | IT PRO

XV. Global Network Initiative (GNI) statement on mass surveillance and the importance of free expression.

https://globalnetworkinitiative.org/gni-statement-on-communications-surveillance/

Bibliography

Afifi-Sabet, Keumars. "UK 'Mass Surveillance' Regime Is Illegal, EU Court Declares." *IT PRO*, IT Pro, 7 Oct. 2020, www.itpro.co.uk/security/privacy/357351/uk-mass-surveillance-regime-is-illegal-eu-court-declares.

Beens, Robert E.G. "Council Post: The State of Mass Surveillance." *Forbes*, Forbes Magazine, 24 Sept. 2020, www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=4c12b845b62d.

"Bill c-59: Mass Surveillance and Cyber Powers." *International Civil Liberties Monitoring Group*, International Civil Liberties Monitoring Group, iclmg.ca/issues/bill-c-59-the-national-security-act-of-2017/bill-c-59s-mass-surveillance-and-cyber-powers/.

Bischoff, Paul. "Surveillance Camera Statistics: Which City Has the Most Cctv Cameras?" *Comparitech*, Comparitech, 8 June 2021, www.comparitech.com/blog/vpn-privacy/the-worlds-most-surveilled-cities/.

Campbell, Charlie. "What China's Surveillance Means for the Rest of the World." *Time*, Time, 21 Nov. 2019, time.com/5735411/china-surveillance-privacy-issues/.

"Does Mass Surveillance by Governments Matter?" *Does Mass Surveillance by Governments Matter?*, www.southampton.ac.uk/~mwra1g13/msc/comp6048/government-mass-surveillance.html.

"Evidence of Global Opposition to US Mass Surveillance." *Amnesty International UK*, Amnesty International , 6 Oct. 2020,

www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq.

"Five Eyes: Privacy International." *Five Eyes | Privacy International*, Privacy International, privacyinternational.org/learn/five-eyes.

Gao, George. "What Americans Think about NSA Surveillance, National Security and Privacy." *Pew Research Center*, Pew Research Center, 17 Aug. 2020, www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/.

"General Assembly Backs Right to Privacy in Digital Age | | UN NEWS." *United Nations*, United Nations, 19 Dec. 2013, news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age.

"International Covenant on Civil and Political Rights." *United Nations Human Rights Office of the High Commissioner*, United Nations, 16 Dec. 1966, www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

Keane, Sean. "Huawei Ban Timeline: Chinese Company Settles Patent Lawsuits with Verizon." *CNET*, CNET, 13 July 2021, www.cnet.com/news/huawei-ban-timeline-xiaomi-removed-us-boycott-list-chinese-companies/.

"Mass Surveillance ENDANGERS Human Rights and Does Not Prevent Terrorist Attacks, SAYS Council of Europe." *CCDCOE*, ccdcoe.org/incyder-articles/mass-surveillance-endangers-human-rights-and-does-not-prevent-terrorist-attacks-says-council-of-europe/.

Munn, Nathan. "How Mass Surveillance Harms Societies and Individuals - and What You Can Do about It." *Canadian Journalists for Free Expression*,

Canadian Journalists for Free Expression, 8 Nov. 2016, www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it.

Murphy, Jessica. "CSIS under Scrutiny for Programme That Illegally Kept Metadata." *BBC News*, BBC, 5 Nov. 2016, www.bbc.com/news/world-us-canada-37875696.

"New AI Law Proposal Calls out Harms of Biometric Mass Surveillance, but Does Not Resolve Them." *European Digital Rights (EDRi)*, European Digital Rights (EDRi), 22 Apr. 2021, edri.org/our-work/new-ai-law-proposal-calls-out-harms-of-biometric-mass-surveillance-but-does-not-resolve-them/.

"North Korea Develops New Systems To Increase Surveillance And Block Outside Information." *Monitor Tracking Civic Space*, Civicus, 23 Jan. 2020, monitor.civicus.org/updates/2020/01/23/north-korea-develops-new-systems-increase-surveillance-and-block-outside-information/.

"North Korea, the Surveillance State." *Amnesty International UK*, Amnesty International UK, 12 Jan. 2018, 07:31 am, www.amnesty.org.uk/north-korea-surveillance-state-prison-camp-internet-phone-technology.

"Online Mass Surveillance: 'Protect Right to Privacy Even When Countering Terrorism' – UN Expert." *United Nations Human Rights Office of the High Commissioner*, United Nations, www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200&LangID=E.

Risen, James, and Eric Lichtblau. "Bush Lets U.S. Spy on Callers without Courts." *The New York Times*, The New York Times, 16 Dec. 2005,

www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

"Timeline of NSA Domestic Spying 1791-2015." *Electronic Frontier Foundation*, Electronic Frontier Foundation, 29 Sept. 2017, www.eff.org/nsa-spying/timeline.

United Nations General Assembly, 2014, *The Right to Privacy in the Digital Age*.

van der Kleut, Jennifer. "Biometrics and Biometric Data: What Is It and Is It Secure?" *Norton*, Norton, 8 Feb. 2019, us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html.

"What Is Artificial Intelligence? How Does Ai Work?" *BuiltIn*, 2021, builtin.com/artificial-intelligence.

"What Is the Definition of Machine Learning?" *Expert.ai*, 26 May 2021, www.expert.ai/blog/machine-learning-definition/.