Committee: Human Rights Council (HRC)

Issue: The issue of state surveillance breaching the individual right to privacy

Student Officer: Christina Antonakou

Position: Deputy President

PERSONAL INTRODUCTION

Dear Delegates,

My name is Christina Antonakou, I am 16 years old and a 10th grader at Pierce (The American College of Greece). It is my utmost honor and pleasure to serve as a Deputy President of the Human Rights Council (HRC) of ACGMUN 2024. This will be my 6th conference however my first one serving as a Student Officer.

MUN and I did not get off to a good start. I was intimidated and wondered what I had put myself into, but once I stepped into my first conference room, I was left speechless by how everything was much simpler than I thought it would be. MUN is not just a conference, but a new path in which you will meet new people and create experiences that will mark you for life. My advice to you is to be a mini expert on all the topics. I do know that by the time our conference arrives, you will have gotten that a lot, but it is indeed one of the most crucial parts of MUN. The first step is to read this Study Guide. This guide aims to give you insight on the topic at hand, but it should not be your only source of information. You should also engage in personal research, according to the policy of your delegation.

Through this study guide, I aim to introduce you to the topic of "The issue of state surveillance breaching the individual right to privacy" and offer you critical information on the issue that will help you draft resolutions. Acknowledging that it is not an easily comprehensible topic, if you have any questions, please do not hesitate to contact me at my personal email, cantonakou@gmail.com.

With that being said, I welcome you all to the 7th ACGMUN!

TOPIC INTRODUCTION

"The issue of state surveillance breaching the individual right to privacy", is a vital problem which affects us all, mainly caused by the rapid evolution of technology. Although it started developing in the nineteenth century, it wasn't until the twentieth century that the barrier between surveillance and privacy was threatened. Major breakthroughs of surveillance technology, particularly after World War II, encouraged the acceptance of widespread physical surveillance by not only the government but private citizens as well.

Surveillance involves monitoring another person or group. It may involve recording individuals, listening to private conversations (as when a telephone conversation is bugged), or even using canines to locate harmful substances such as narcotics and explosives.

Surveillance can lead to a complete disregard for an individual's right to privacy. Right now, the ability of governments and companies to keep people's lives under surveillance has never been more capable, especially with the use of artificial-intelligence algorithms. Because of that reason, new laws have been ratified to impose limits on the ability of authorities to place individuals under surveillance against their will or without their knowledge. Governments can only interfere with citizens' rights when it is specifically allowed by law and done for a good reason, like national security or public safety.

Because there will never be a society in which every individual will abide by every law, authorities will keep investigating to ensure a degree of social conformity. Though such investigations do not fall under the category of state surveillance, except if that process violates someone's, or everyone's privacy. Last, this topic has been taken into consideration by the UN after numerous cases and aims to protect the right to respect one's private life. This includes protecting the privacy of messages, phone calls, and emails. For instance, A/HRC/51/17[1] highlights the threats that state surveillance consists of.

[1] OHCHR. (n.d.). United Nations .https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

DEFINITION OF KEY TERMS

Mass Surveillance

"Mass surveillance uses systems or technologies that collect, analyze, and generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing."[2]

Personal data

"Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data"[3]

Surveillance

"The word surveillance is binary in nature, derived from the French verb -to watch over-. As in, watching over an individual or individuals to keep them safe, but also watching over them to ensure that they meet a certain standard of behavior. Conceptually, surveillance both enables and constrains. It is used both to protect and to control."[4]

Privacy

"The state of being alone and not watched or interrupted by other people**."**[5]

Surveillance state

"A country whose government invests vast amounts of resources in deploying surveillance technology to monitor not only its visitors but also its own citizens."[6]

[2] Mass surveillance. (n.d.). Privacy International. https://privacyinternational.org/learn/mass-surveillance

[3] What is personal data? (n.d.). European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

[4] Surveillance is a fact of life, so make privacy a human right. (2019, December 13). The Economist. https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

[5] Privacy. (n.d.). Oxford Learner's Dictionaries | Find definitions, translations, and grammar explanations at Oxford Learner's Dictionaries. https://www.oxfordlearnersdictionaries.com/definition/english/privacy (2023, September 22).

[6] What is a surveillance state? PrivacyEnd. https://www.privacyend.com/surveillance-state/

BACKGROUND INFORMATION

The USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001[7], was signed by the former president, George W. Bush in response to the September 11 attacks, with the aim to strengthen U.S. national security, especially as it related to foreign terrorism. The legislation was designed to expand the powers of the government to surveil and investigate suspected terrorists; it is controversial due to its authorization of indefinite detention without trial of immigrants, and because of the permission given to law enforcement to search property and records without the owner's consent or knowledge. The Congress passed the final legislation on October 11, 2001, but there was an "improvement and reauthorization act" in 2005.

Pegasus Spyware

Pegasus[8] is a spyware, and a highly intrusive surveillance tool which is able to access a user's mobile data. It turns smartphones into a surveillance device, accessing the camera and microphone, geolocation data, e-mails, messages, photos, videos, passwords, and applications. It is developed by an Israeli company which globally markets it. It is known that it was sold to at least 14 European Union countries. Pegasus has been used for illegitimate purposes by governments, including against journalists, political opponents, human rights defenders. While certain governments fight that the use of Pegasus-type spyware should be limited to exceptional situations for genuine and serious threats to national security or specific and defined serious crimes, we are far from achieving that.

Predator spyware

Predator spyware is a phone hacking software developed by Cytrox, based in Skopje, North Macedonia. Predator shares similar features with Pegasus spyware. Predator can access one's messages, calls, photos, passwords, camera and microphone. It can add a certificate authority (CA) to smartphones, tricking the device into trusting malicious apps and websites. It has been used to surveil political opponents and government critics, not just criminals and foreign agents. Several countries have suffered due to the Predator's epidemic, such as Greece and Egypt.

[7] What is the USA Patriot web. (n.d.). Department of Justice | United States Department of Justice. https://www.justice.gov/archive/ll/highlights.htm

[8] The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU member states for the acquisition and use of Pegasus and equivalent surveillance spyware | Think tank | European Parliament. (2022, May 12). https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740151

The Edward Snowden case

Edward Snowden is a former contractor for the National Security Agency (NSA)[9]. He was working at an underground facility in Hawaii in 2013, when he witnessed the mass collection of NSA's electronic data on American citizens. As he has said, NSA was not just watching existing terrorists but everyone; just in case they became terrorists. This was not something that affected people only in transatlantic countries, but Americans as well. Snowden copied files of the NSA's top-secret surveillance programs and fled the U.S., while also sharing the highly classified information with several Western journalists in prestigious newspapers. Due to that incident, Americans understood how governments and private companies collect personal data.

In 2015, the Congress rewrote the law that allowed the NSA to view and investigate everyone's records. The U.S.A. Freedom Act[10] now prohibits the huge collection of phone records by American citizens. According to a former president, this action did not only result in the change of laws but the inclusion of transparency to help build confidence among the American people that their privacy and civil liberties are being protected by the government.

Figure 1: Edward Snowden[11]

Heatmaps

Heatmaps are a method of representing data from websites graphically, where values are depicted by color, making it easy to visualize complex data, analyze it and understand it. Heatmaps are mainly created with the use of specialized heatmapping software. They are a way for the owner of a website to understand what users do on

[9] National Security Agency | Central Security Service.https://www.nsa.gov

[10] Freedom Act. (n.d.). U.S. https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.htm

[11] Supervising surveillance: International law and the surveillance state. (2020, November 11). Harvard International Review. https://hir.harvard.edu/global-surveillance-state/

their website -where they click, how far they scroll- and be in control of it. A variety of color schemes can be used when creating heatmaps, most likely a rainbow. Usually, warmer colors -reds and oranges- represent more used sections, while cooler colors -blues and purples- represent less frequently used sections of the website. Heatmaps take any number of forms, like click maps, scroll maps, mouse-tracking maps. There are also eye-tracking website heatmaps in which a sensor technology is used to track the movement of users' eyes when they are using a specific website. This type of technology can monitor eye movement, blinking, and pupil dilation to analyze where on a page a user's attention is focused.

Figure 2: "A heatmap of user interactions on a checkout page."[12]

Five Eyes alliance

The Five Eyes (FVEY) alliance is a web of global intelligence, a secret association that continues to redefine geopolitical landscapes. It is compromised by five English-speaking countries, the United States, the United Kingdom, Canada, Australia, and New Zealand. This alliance has established an unprecedented era of surveillance and shares information that shapes the world's approach to national security.

It was established in Word War II and based on the 1946 UKUSA Agreement[13], intended as a cooperative arrangement for sharing signals intelligence (SIGINT)[14].

[12] What is a Heatmap? + how to create, analyze & use Heatmaps. (2023, March 24). Build a More Perfect Digital Experience | FullStory. https://www.fullstory.com/heatmap/

[13] National Security Agency/Central security service > helpful links > NSA FOIA > declassification & transparency initiatives > historical releases > UKUSA. (n.d.). National Security Agency | Central Security Service. https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/

[14] National Security Agency/Central security service > signals intelligence > overview. (n.d.). National Security Agency | Central Security Service. https://www.nsa.gov/Signals-Intelligence/Overview/

Except the Five Eyes, there are also extended alliances known as the Nine Eyes and Fourteen Eyes. The Nine Eyes alliance includes the original Five Eyes countries along with France, the Netherlands, Denmark and Norway. The Fourteen Eyes further extends the Nine Eyes by including Belgium, Sweden, Spain, Germany and Italy. There is also the Forty One Eyes alliance with a great expansion of the Fourteen Eyes, including the addition of the allied coalition in Afghanistan. These alliances enhance global surveillance capabilities, but also entertain debates concerning privacy and the boundaries of national security.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

People's Republic of China

China is currently a global leader in the space of state surveillance, as it has -among many others- the second-largest surveillance camera company in the world. Even dominant countries such as the US have blocked Chinese military companies from accessing its technologies. The Chinese government has been putting a lot of effort into state surveillance, as it has managed to build a new social contract with its citizens: "they give up their data in exchange for more precise governance that, ideally, makes their lives safer and easier (even if it doesn't always work out so simply in reality)".[15] It is important to note that the pandemic has accelerated the use of surveillance tech in China, whether the technology itself can stay the same with the equipment that is already used, or with its expansion -always acknowledging that other countries will follow China's lead. Though, the Chinese government is now proposing that by collecting every Chinese citizen's data extensively, it can find out what the people want (without giving them votes) and build a society that meets their needs.

[15] Yang, Z. (2022, October 10). The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect. MIT Technology Review. https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/

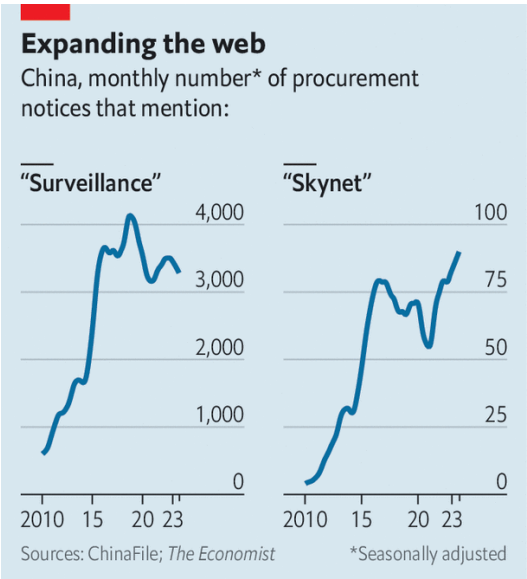

Figure 3: China's Surveillance Network [16]

Federal Trade Commission (FTC)

"The Federal Trade Commission enforces a variety of antitrust and consumer protection laws affecting virtually every area of commerce, with some exceptions concerning banks, insurance companies, non-profits, transportation and communications common carriers, air carriers, and some other entities. The agency leverages its resources and targets its enforcement efforts at practices that cause the greatest harm to consumers." [17] The Federal Trade Commission is currently exploring rules to cease harmful commercial surveillance and weak data security. Commercial surveillance is the act of collecting, analyzing, and profiting from information about people, by selling this collected information of consumers to the market, by algorithms and automated systems. Mass surveillance has increased the risks of data breaches, manipulation, and other abuses. Firms are able to collect personal data on individuals at a massive scale. Companies reportedly survey consumers while they are connected to the internet –every aspect of their online activity, their family and friends' networks, browsing and purchase histories, location and physical movements, and a wide range of other personal details. While very little is known about the automated systems that analyze data companies collect, research suggests that these algorithms are subject to errors, bias, and inaccuracy. As a result, commercial surveillance practices may discriminate against consumers based on characteristics like race, gender, religion, and age, eliminating their ability to obtain housing, credit, employment, or other critical needs.

[16] China's enormous surveillance state is still growing. (2023, November 23). The Economist. https://www.economist.com/china/2023/11/23/chinas-enormous-surveillance-state-is-still-growing

[17] What the FTC does. (2020, January 9). Federal Trade Commission. https://www.ftc.gov/news-events/media-resources/what-ftc-does

Federal Trade Commission Act

In the last two decades, the FTC has used its existing authority under the FTC Act to bring hundreds of enforcement actions against companies for privacy and data security violations, even though it may not be enough for such dilemma. On August 11, 2022, the Federal Trade Commission (FTC) issued an Advanced Notice of Proposed Rulemaking (ANPRM) announcing that the agency wants to create new regulations on commercial surveillance and data security. The ANPRM explained that, even if the Commission does not ultimately abide by all the regulations, comments on these issues would sharpen its enforcement work and may inform Congress and other policymakers. The ANPRM also announced a public forum, which was held on September 8, 2022, in which panelists and members of the public made remarks on the topics addressed in the ANPRM. The ANPRM was approved by the Commission by a 3-2 vote. The dissenting commissioners reasoned that Congress is the proper body to adopt nationwide consumer data and privacy rules and not the FTC, simply because if the FTC completes the rulemaking process and adopts commercial surveillance and data security laws, the regulations may be subject to legal challenge.

Russian Federation

The Russian Federation has a long history of state surveillance, starting with Komitet Gosudarstvennoy Bezopasnosti (KGB) back in the Soviet Union, followed by the Federal'naya Sluzhba Bezopasnosti (FSB) and many others.

Roskomnadzor

Roskomnazdor is an agency based in Russia, which started in 2008 as a bureaucratic backwater with a few dozen employees who regulated radio signals, telecom and postal delivery. Its role expanded as concerns grew about the internet, which was under less state control than television and radio, leading to more activity from independent and opposition media. Russia, along with authoritarian countries like China and Iran, consistently use technology as a tool of repression. Since the agency was established in 2008, Mr. Putin has turned it into a way to make Russia an even more powerful state. Roskomnadzor has also worked to unmask and surveil people behind anti-government accounts and provided detailed information on online activities to security agencies, according to documents.

United States of America (USA)

The American Telephone and Telegraph Company (AT&T), the National Security Agency (NSA) and the Electronic Frontier Association (EFF) have played critical roles regarding the United States' position on state surveillance. The US government, assisted by AT&T and other telecommunications carriers, has engaged in massive, illegal surveillance of domestic communications and has recorded millions of

Americans since 2001. It was first revealed in December 2005, that the NSA has been intercepting Americans' phone calls and Internet communications. EEF fought back and resulted in the Jewel v. NSA[18] case, in which EEF sued the NSA and the rest of the government agencies that were engaged in state surveillance.

United Kingdom (UK)

Numerous reports in 2013 revealed sharing collaborations between Government Communications Headquarters (GCHQ) and the United States' National Security Agency. Big Brother Watch, English PEN, Open Rights Group and Dr Constanze Kurz went to the Court in 2013 following Edward Snowden's revelations that UK intelligence agencies were running a mass surveillance and communications interception programme named TEMPORA, while receiving data from other US programmes like PRISM and UPSTREAM, invading UK citizens' privacy. The European Court of Human Rights has stated that the UK's regime for the surveillance of electronic communications and web activity violates the public's right to privacy. At the end of 2016, the UK government passed the Investigatory Powers Act[19], which put limits upon the country's hacking powers. "It provides a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies."[20]

TIMELINE OF EVENTS

Date	Description of event
March 5, 1946	UKUSA Agreement
November 4, 1952	Formation of National Security Agency
April 18, 1961	Vienna Convention on Diplomatic Relations
December 7, 2000	Charter of Fundamental Rights of the European Union
October 11, 2001	PATRIOT Act
2013	Edward Snowden Case
August 11, 2022	ANPRM creating new regulations on commercial surveillance
September 8, 2022	Public Forum on ANPRM

[18] Jewel v. NSA. (2019, 29). United States Courts. https://www.uscourts.gov/cameras-courts/jewel-v-nsa

[19] Nast, C. (2017, May 8). What is the IP act and how will it affect you? WIRED UK. https://www.wired.co.uk/article/ip-bill-law-details-passed

[20] Investigatory powers act. (n.d.). NCSC. https://www.gchq.gov.uk/information/investigatory-powers-act

RELEVANT UN RESOLUTIONS, TREATIES AND EVENTS

- Human Rights Council report on the right to privacy in the digital age, 26 September 2019 **(A/HRC/48/31)** [21]

  In the present report, the High Commissioner analyzes how the use of artificial intelligence and technology by States negatively affects citizens' right to privacy and their civil rights. Following an overview of the international legal framework, the High Commissioner provides examples of consequences on the right to privacy. The High Commissioner then addresses the challenges, while providing a set of recommendations for States regarding the design and implementation of safeguards to cease harmful outcomes.

- Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development : joint written statement / submitted by the Citizens' Coalition for Economic Justice and the People's Solidarity for Participatory Democracy, 30 August 2013 **(A/HRC/24/NGO/44)**[22]
- The right to privacy in the digital age : report of the United Nations High Commissioner for Human Rights, 3 August 2018 **(A/HRC/39/29)**[23]

  The present report is identifying and clarifying principles, standards and best practices concerning the protection of the right to privacy in the digital age.

- The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014 **(A/HRC/27/37)**[24]

  This report discusses the protection and promotion of the right to privacy in the context of domestic surveillance and the collection of personal data, including on a mass scale.

[21] The right to privacy in the digital age: report (2021). (n.d.). United Nations Human Rights. https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021

[22] Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development :. (n.d.). United Nations Digital Library System. https://digitallibrary.un.org/record/782634?ln=en

[23] The right to privacy in the digital age : report of the United Nations High Commissioner for Human Rights. *(n.*d.). United Nations Digital Library . https://digitallibrary.un.org/record/1640588?ln=en

[24] The right to privacy in the digital age :. (n.d.). United Nations Digital Library System. https://digitallibrary.un.org/record/777869?ln=en

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

European Union, Charter of Fundamental Rights of the European Union

The European Union has taken into consideration dilemmas such as state surveillance, specifically with the ratification of "Charter of Fundamental Rights of the European Union". This Chart aims to strengthen the protection of fundamental rights like privacy, while facing a wide range of social progress, scientific and technological developments. Article 7 of the Charter guarantees all individuals in the European Union the respect for private and individual life, while Article 8 guarantees the protection of their personal data. It also requires that such data be processed fairly for specific purposes. Article 47 secures the right to an effective remedy, including a fair and public hearing within a reasonable timeframe. [25]

International Principles on the Application of Human Rights to Communications Surveillance

A set of principles, stated by the UN Human Rights Council, was put forward in 2014, and it is named "International Principles on the Application of Human Rights to Communications Surveillance". It calls upon all States to ensure that laws, regulations, and activities related to Communications Surveillance adhere to international human rights law and standards. The document has been adopted by hundreds of companies, organizations, experts, and elected officials have signed the principles document. However, it is not an effective international treaty that has a chance at solving global issues upon state surveillance. "This document attempts to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Sur- veillance technologies and techniques."[26]

Article 41 of the Vienna Convention on Diplomatic Relations

Article 41 of the Vienna Convention on Diplomatic Relations[27], requires all foreign officers to respect the laws of the country in which they are posted, which means that surveillance conducted by diplomats is illegal. Article 41 does not refer to non-diplomat citizens, but establishes the precedent that unfettered surveillance ought to be regulated.

[25] Charter of Fundamental Rights pf the European Union
https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[26] Necessary and Proportionate. https://necessaryandproportionate.org/files/en_principles_2014.pdf

[27] United Nations - Office of Legal Affairs.
https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

POSSIBLE SOLUTIONS

Reviewing and strengthening governments' policies and laws

One of the main problems regarding the right to privacy is that laws and policies do not entirely protect citizens. In the past, there have been cases that went into court but could not face any legal consequences due to the paucity of laws that protect victims in such cases. Adopting legislative and regulatory frameworks that adequately prevent the violation of basic human rights and protect each citizen's privacy, could eliminate the unlawful and unnecessary government surveillance.

Tackling the vast development of Artificial Intelligence (AI)

Living in the digital age, states are increasingly integrating AI systems in the executive branch as seen by law enforcement, national security, criminal justice and border management agencies. It is highly probable that the usage of AI is a cause for concern, as its technology can create softwares and machines far beyond our control. States ought to recognize the need to protect and reinforce all human rights in the development and use of AI as a central objective, and ensure equal respect and enforcement of all human rights online and offline.

Organizations' supervision

Another approach on tackling the issue of state surveillance, is to call for a specific UN organization to deal with the issue and peacefully find solutions that states will abide by. Such organizations are, United Nations Sciences and Technology Organization (UNSTO)[28] and Office of the United Nations High Commissioner for Human Rights (OHCHR)[29].

Thus, it would be effective to have a NGO[30] to supervise, as they can work on a large scale or very locally to promote social and political change, like Electronic Frontier Foundation (EEF)[31] or Privacy International[32] which will ensure the protection of citizens and the right usage of state surveillance tools; either digital or other techniques, and that they will not invade an entity's private life except if it is a matter of national security.

[28] UNSTO. https://www.unsto.org

[29] OHCHR. https://www.ohchr.org/en/ohchr_homepage

[30] How privacy organizations build a better society | Internxt blog. (2023, May 16). Internxt. https://blog.internxt.com/how-privacy-orgs-improve-society/

[31] Electronic Frontier Foundation. https://www.eff.org

[32] Privacy International. https://privacyinternational.org

BIBLIOGRAPHY

General Bibliography

Camões - Repositório Institucional da Universidade Autónoma de Lisboa. https://repositorio.ual.pt/bitstream/11144/5433/1/00EN-vol13-n1-art012.pdf

Does surveillance law provide security or threaten privacy? (2021, May 20). https://www.qmul.ac.uk/lac/our-legal-blog/items/does-surveillance-law-provide-security-or-threaten-privacy.html

The kaleidoscope of privacy and surveillance. (n.d.). MIT - Massachusetts Institute of Technology. https://web.mit.edu/gtmarx/www/thekaleidoscopeof.html

Surveillance ethics. (n.d.). Internet Encyclopedia of Philosophy | An encyclopedia of philosophy articles written by professional philosophers. https://iep.utm.edu/surv-eth/#H2

History of privacy timeline / safecomputing.umich.edu. (n.d.). U-M Safe Computing / safecomputing.umich.edu. https://safecomputing.umich.edu/privacy/history-of-privacy-timeline

Does the government guarantee a right to privacy? (2012, September 30). ThoughtCo. https://www.thoughtco.com/right-to-privacy-history-721174

ALA | Constitutional origin of the right to privacy. (2009, July 20). American Library Association | Awards, publishing, and conferences: ALA membership advocates to ensure access to information for all. https://www.ala.org/ala/washoff/contactwo/oitp/emailtutorials/privacya/05.htm

FTC explores rules cracking down on commercial surveillance and lax data security practices. (2022, September 7). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices

FTC Considers Adopting Commercial Surveillance and Data Security Rules. (n.d.). https://crsreports.congress.gov/product/pdf/LSB/LSB10839

The ethics (or not) of massive government surveillance. (n.d.). Computer Science. https://cs.stanford.edu/people/eroberts/cs201/projects/ethics-of-surveillance/history_worldwars.html

Mass surveillance began with World War I. (2014, August 4). University of Wisconsin Press Blog. https://uwpress.wisc.edu/blog/2014/08/its-about-blackmail-not-national-security/

A decade on, Edward Snowden remains in Russia, though U.S. laws have changed. (2023, June 4). NPR https://www.npr.org/2023/06/04/1176747650/a-decade-on-edward-snowden-remains-in-russia-though-u-s-laws-have-changed

Surveillance is a fact of life, so make privacy a human right. (2019, December 13). The Economist. https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

What is personal data? (n.d.). European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

Privacy. (n.d.). Oxford Learner's Dictionaries | Find definitions, translations, and grammar explanations at Oxford Learner's Dictionaries. https://www.oxfordlearnersdictionaries.com/definition/english/privacy (2023, September 22).

What is a surveillance state? PrivacyEnd. https://www.privacyend.com/surveillance-state/

Mass surveillance. (n.d.). Privacy International. https://privacyinternational.org/learn/mass-surveillance

Does the government guarantee a right to privacy? (2012, September 30). ThoughtCo. https://www.thoughtco.com/right-to-privacy-history-721174

"Olmstead v. United States." Oyez, www.oyez.org/cases/1900-1940/277us438 Accessed 24 Nov. 2023.

Green v. United States, 355 U.S. 184 (1957). (n.d.). Justia Law. https://supreme.justia.com/cases/federal/us/355/184/

First Amendment. (2010, September 21). Encyclopedia Britannica. https://www.britannica.com/topic/First-Amendment

What the FTC does. (2020, January 9). Federal Trade Commission. https://www.ftc.gov/news-events/media-resources/what-ftc-does

The right to privacy in the digital age: report (2021). (n.d.). United Nations Human Rights. https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021

Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development :. (n.d.). United Nations Digital Library System. https://digitallibrary.un.org/record/782634?ln=en

The right to privacy in the digital age : report of the United Nations High Commissioner for Human Rights. *(n.d.).* United Nations Digital Library . https://digitallibrary.un.org/record/1640588?ln=en

The right to privacy in the digital age :. (n.d.). United Nations Digital Library System. https://digitallibrary.un.org/record/777869?ln=en

Yang, Z. (2022, October 10). The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect. MIT Technology

Review. https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/

What is a Heatmap? + how to create, analyze & use Heatmaps. (2023, March 24). Build a More Perfect Digital Experience | FullStory. https://www.fullstory.com/heatmap/

'They are watching': Inside Russia's vast surveillance state (Published 2022). (2022, September 23). The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html

Charter of Fundamental Rights pf the European Union https://www.europarl.europa.eu/charter/pdf/text_en.pdf

National Security Agency | Central Security Service. https://www.nsa.gov

Richards, N. M. (2023, March 24). *The dangers of surveillance*. Harvard Law Review. https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

Necessary and Proportionate. https://necessaryandproportionate.org/files/en_principles_2014.pdf

NSA spying. (n.d.). Electronic Frontier Foundation. https://www.eff.org/nsa-spying

Ali. (n.d.). European court of human rights declares UK's mass surveillance regime unlawful. DPG Law. https://dpglaw.co.uk/european-court-of-human-rights-declares-uks-mass-surveillance-regime-unlawful/

Jewel v. NSA. (2019, 29). United States Courts. https://www.uscourts.gov/cameras-courts/jewel-v-nsa

Haan, K. (2023, September 1). What is the Five Eyes alliance? Forbes Advisor. https://www.forbes.com/advisor/business/what-is-five-eyes/

National Security Agency/Central security service > signals intelligence > overview. (n.d.). National Security Agency | Central Security Service. https://www.nsa.gov/Signals-Intelligence/Overview/

Five Eyes. (n.d.). Privacy International. https://privacyinternational.org/learn/five-eyes

What is the USA Patriot web. (n.d.). Department of Justice | United States Department of Justice. https://www.justice.gov/archive/ll/highlights.htm

USA Patriot Act. (2011, November 3). Encyclopedia Britannica. https://www.britannica.com/topic/USA-PATRIOT-Act

The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU member states for the acquisition and use of Pegasus and equivalent

surveillance spyware | Think tank | European Parliament. (2022, May 12). https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740151

Pegasus. (n.d.). MEMO. https://www.middleeastmonitor.com/20220910-israels-predator-spyware-rivals-nsos-pegasus/

Pictures and Graphs Bibliography

China's enormous surveillance state is still growing. (2023, November 23). The Economist. https://www.economist.com/china/2023/11/23/chinas-enormous-surveillance-state-is-still-growing

What is a Heatmap? + how to create, analyze & use Heatmaps. (2023, March 24). Build a More Perfect Digital Experience | FullStory. https://www.fullstory.com/heatmap/

Supervising surveillance: International law and the surveillance state. (2020, November 11). Harvard International Review. https://hir.harvard.edu/global-surveillance-state/