

Committee: Social, Humanitarian and Cultural Committee

Issue: The Issue of Global Mass Surveillance by Governments

Student Officer: Eleni Goridari

Position: Co-Chair

PERSONAL INTRODUCTION

Dear Delegates,

My name is Eleni Goridari and it is a great honor to be serving as the co-chair of the Social, Humanitarian and Cultural Committee in the 2nd DSTMUN conference. Ever since my first MUN experience, I've always dreamt about being a student officer one day to in order to take my MUN experience to the next level. What I find most intriguing about MUN conferences is the opportunity to interact with other people, through exchanging different ideas and viewpoints, and thus learning from them not only academically, but also spiritually. Moreover, but for the MUN conferences, I wouldn't have the chance to involve myself in such debatable and up-to-date issues, which after all broadened my horizons, and increased my diplomacy skills. For this reason, I am very excited about this year's topics, and especially about the issue of mass surveillance, which is now, in the digital age, more concerning than ever. I have to remind you, that this study guide is to help you understand the basic aspects of this topic, therefore you should make your own research in order to be fully informed about it. Be aware that you need to focus on the humanitarian aspects of this issue. If you have any questions concerning mass surveillance, do not hesitate to contact me via my email: egoridari@gmail.com.

I'm looking forward to having a wonderful time, and engaging only in a fruitful debate.

Kind regards,

Eleni Goridari

TOPIC INTRODUCTION

The issue of global mass surveillance by governments is constantly becoming more pertinent to our society today, and it dates back to medieval England. Mass surveillance is monitoring a whole or a large portion of a population to monitor this group of people. It can involve anything from CCTV monitoring, e-mail interceptions, wiretapping, computer hacking etc. It is usually carried out by governments or

corporations either on behalf of a government or on their own initiative. Some mass surveillance systems can be used by many countries at the same time, while other governments develop their own systems. Its main purpose is to fight crime and prevent terrorism, however it has some undeniable drawbacks that need to be considered. Even though it is legal in most cases, it is not considered ethical as it violates some basic human rights, and therefore citizens feel monitored and vulnerable due to the number of things the government knows about them. Of course, there are some regulations, differing from country to country, protecting personal data from the “eyes” of the government, but human rights are still being infringed on. For this reason, the main controversy regarding this topic is whether government surveillance should become stricter or more liberal, depending on each country’s policy. Your aim as delegates is to propose solutions focusing on the humanitarian aspects of this topic, on how mass surveillance can continue to exist without however infringing basic human rights.

DEFINITION OF KEY TERMS

Mass Surveillance

Mass surveillance is the distributive close observation of an entire population or a substantial fraction of the entire population. Its main purpose is to protect citizens from threats such as terrorists, criminals or political subversives, and to maintain social control.

Cookies policy

Cookies are small files. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web or the client computer. This allows the server to deliver a page tailored to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next. ¹

General Data Protection Regulation (GDPR)

The General Data Protection Regulation is Europe’s new framework for data protection laws. It is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens’ data privacy and reshape the way organizations approach data privacy. ²

¹ <http://www.whatarecookies.com>

² <https://eugdpr.org>

Intelligence Agency

A governmental agency that is devoted to information gathering for purposes of national security and defence. Some of the best intelligence agencies are the Central Intelligence Agency (CIA) in USA, the Secret Intelligence Service (SIS) in the United Kingdom and the Main Intelligence Directorate (GRU) in Russia. ³

Surveillance State

A surveillance state is defined as a state which legally monitors all actions, locations, and friends of its citizens, in order to prevent crimes or in order to solve them faster. Even though it sounds as if it were a good idea, in reality it has a negative meaning, because surveillance states monitor everything and everyone, and as a result everything one says or does could be used against them. ⁴

BACKGROUND INFORMATION

Historical background

While mass surveillance in its recent form is relatively new, the concept of governments monitoring their citizens can date back to medieval England. Each country has a different historical background concerning mass surveillance, however we will be taking into account the most prominent surveillance programs and events that have occurred up until today.

Mass surveillance in world war two

As you can imagine, during World War two (1939-1945), mass surveillance was really prominent. In Germany, there was a legislation which allowed the government to imprison anyone considered enemy of the Nazis. Meanwhile, USA monitored telephone and cable transmissions of its citizens, even though it was illegal, because national security outweighed the right of privacy for the American government.

Mass surveillance during the Cold War

Mass surveillance during the Cold War (1947-1991) was an important factor for both parties to expand their power. However, in this era mass surveillance is better characterized as espionage. USA, Soviet Union and their allies, conducted espionage on each other to obtain military, government and economic secrets. The main intelligence companies participating were CIA for USA and KGB for the Soviet

³ <https://www.yourdictionary.com/intelligence-agency>

⁴ <https://piratetimes.net/what-is-a-surveillance-state-and-is-it-good-for-you>

Union. As it is known, Germany at that time was divided in half: The Western part belonged to the USA and their allies, and the Eastern part to the Soviet Union. The main body which conducted surveillance in the Eastern Part was the Ministry for State Security, known as the Stasi, and it was a secret police agency. The Stasi monitored citizens in every possible way by telephone espionage, video surveillance, photo surveillance, to even putting secret agents everywhere. Anyone who was slightly suspicious was imprisoned, questioned and tortured by the Stasi. Thus, it was the most feared and hated governmental body.

Human Rights Aspect

Due to mass surveillance, many human rights, but especially the right of privacy and the right of freedom of expression are being infringed. Almost every country is being accused of violating its citizens' rights, due to illegal personal data collection, espionage, weak judicial control on intelligence agencies etc. The main arguments that governments have are firstly, that safety should be established by all means, and secondly, if a person has nothing to fear, then they have nothing to hide. Nevertheless, many people disagree and believe that mass surveillance should be carried out to monitor terrorists and criminals, and "innocent people" should be left alone.

Benefits and Drawbacks of Mass Surveillance

While we focus mainly on the drawbacks of mass surveillance, it should be noted that there are some tremendous benefits as well.

Benefits:

- It provides safety to a country and its citizens.
- It prevents criminal and terrorist actions from happening.
- It gathers evidence to determine whether someone is innocent or guilty.

Drawbacks:

- It infringes on people's right of privacy, and in some cases on people's right of freedom of expression.
- Governments and surveillance companies can exploit people and use their personal data either to blackmail them or for their own benefit.
- Even though mass surveillance is being conducted years now, it hasn't really decreased or stopped criminal behaviors.
- People feel insecure and uncomfortable when they know someone is collecting their data.

Regulations

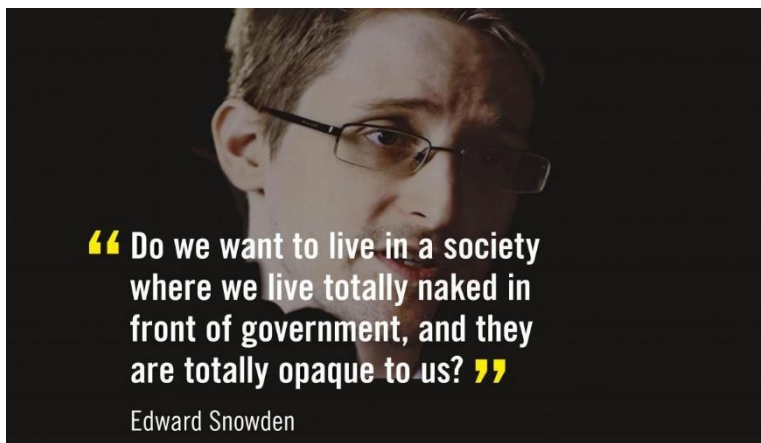
Fortunately, some countries have adopted legislations which protect the rights of their citizens. The European Union has adopted the General Data Protection Regulation which is very efficient and hopefully other countries will adopt similar legislations as well. USA doesn't have a law as efficient as GDPR, but it does have a governmental body, the American Civil Liberties Union which tries to protect the individual rights of citizens. UK has established a human rights group called Privacy International, which aims the aforementioned.

The National Security Agency (NSA) and PRISM

The National Security Agency is responsible for providing the US government with useful information and assistance in computer network operations. Its purpose is to always advise the government what's best for the country and their allies. Nevertheless, NSA's work has been strongly disputed after Edward Snowden (a former NSA subcontractor), leaked classified information about how NSA monitors citizens and what kind of illegal information it withholds. Actually, the NSA has been accused other times in the past as well, but without significant evidence. PRISM is a system the NSA uses in order to monitor the private telecommunications of nine Internet services such as Microsoft, Facebook, Google etc. The owners of these companies deny knowing anything about PRISM, but admit that its existence is not surprising. PRISM came into light after NSA's director admitted its existence in 2013.

The Edward Snowden case

One of the most important events in the history of mass surveillance is the leaking of top secret information about NSA surveillance activities in 2013, made by Edward Snowden, a former NSA subcontractor. More specifically, Snowden used to work for NSA, and his task was to collect confidential documents regarding NSA's mass surveillance techniques. The more information he discovered about NSA, the more disturbed he felt and needed to tell the world the truth. Therefore, he began copying these documents, and he slowly combined them and used them as evidence against NSA's mass surveillance. Then, he secretly met with journalists of "The



Edward Snowden's opinion about NSA's surveillance

Guardian” and “Washington Post” and revealed them his work. These newspapers released Snowden’s files on a daily basis and disclosed information about NSA and PRISM including photos, videos, social networking details etc. With this kind of information national and international debate ensued. The US government charged him with robbery of public assets, unlawful communication of domestic defence data and reluctant disclosure of classified data on communications intelligence to an unauthorized person. The latter two, are considered as an act of espionage. Some consider him a traitor and others a patriot. Since then, Snowden has been hiding and he’s now living in Russia, where his current location remains unknown.

Huawei vs USA

In February 13th of 2018 FBI, NSA and CIA urged Americans not to use Huawei products. The reason? The director of the FBI accused China of trying to spy the telecommunications of USA through 5G, a technology that Huawei uses. In December, the daughter of Huawei’s founder was arrested for suspicion of violating US sanctions against Iran by passing trade agreements on Huawei’s account with Iran. In January, USA opens a criminal investigation against Huawei and files criminal charges for suspicion of electronic fraud and industrial espionage. Then in March, Huawei accuses the US government of forbidding any American company to purchase equipment from Huawei, due to national security reasons without any evidence. In May, Trump officially prohibited the cooperation between every Chinese company with American telecommunications companies. USA has also encouraged its allies to stop using Huawei products. Moreover, Google stopped working with Huawei, thus making it more unwanted to customers. To sum it up, Trump accuses Huawei of putting USA’s national security in danger, and then prohibits it from his country, without any evidence, something that has made Huawei infamous amongst many people. Thus, Huawei is facing collateral damage from the US- China trade war.

Cambridge Analytica (CA) Issue

CA is a political data analysis-company that worked on 2016 Trump’s campaign. It has enough information for every American in order to build their personality files, which are used for psychographic targeting of ads. More specifically, CA has been accused of secretly withholding information on 50 million Facebook users without permission. The data was obtained



Cambridge Analytica fraud disclosures

through an app, which paid users to take a personality quiz, but before taking the quiz it was mandatory that users gave the app access to their Facebook accounts and to their friends also. The problem is that the Trump campaign in 2016 used ad targeting possibly with the illegally obtained information, in order to influence voters without the users' consent, something which is a clear violation to the right of privacy.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

China

Mass surveillance in China is very strict. In fact, news providers, telecommunications and all internet access are monitored by the government.

Iran

Iran is considered to be one of the worst countries regarding privacy. Citizens are not allowed to use the internet without restrictions. For example, platforms like Facebook, Twitter, Google and Youtube remain blocked. Also, every website goes under strict censorship, therefore if a site differs from the official doctrine of Islam, or the country's international and domestic policy, it is restricted. The internet censorship in Iran is politicized, as it reveals the disputes between conservatives and reformists.

Russia

In 2016, Vladimir Putin introduced some new legislations about mass surveillance which were adopted for anti-terror reasons. They require telecom companies to save their users' communication data. They will also require from internet companies to store their users' text messages. As a result, security and intelligence companies can have access to any information they request without any judicial oversight, and the amount of information that flows through the web will be limited. For this reason, some critics have characterized these legislations as "Russia's big brother laws", and many people are concerned about how their rights will be affected.

United Kingdom

Mass surveillance in the UK has existed for many centuries. Today, it is characterized as unlawful by the European Court of Human Rights (ECHR), as it is said that it infringes citizens' right of privacy. However, ECHR, stated that it wasn't the mass data collection that was illegal, but how it was collected. Given these things, the UK government is trying to alter the already existing legislations about mass

surveillance. Nevertheless, the UK's citizens, The EU and other powerful organizations such as Amnesty International, are concerned whether these new legal frameworks will be a more serious threat than the old ones, to the right of privacy, or whether they will be more liberal.

United States of America

USA is well known for its surveillance programs, as it has many intelligence agencies that have been commonly accused of spying USA's citizens. Some of the most widely-known intelligence agencies of US are CIA, NSA and FBI. Last year, the president of the United States, Donald trump signed a law which allows warrantless surveillance of the US citizens. Even before that happened, the government, was accused of infringing people's right of privacy. The public, following the Snowden disclosures has been concerned than ever about this situation, and wishes that security wouldn't come at the expense of privacy.

Central Intelligence Agency (CIA)

CIA is an American intelligence agency, and its primary goal is to collect and evaluate foreign intelligence to assist the USA's government in making decisions regarding national security. Theoretically, it is forbidden to surveil the domestic activities of US's citizens, however it has been accused several times of doing so.

ECHELON

Echelon is a global network of electronic espionage stations that is allowed to store information from telephones and the internet. Officially, Echelon doesn't exist, according to the USA and the UK, however there is strong evidence for its existence. It was set up in 1947 by a secret treaty between the US, UK, Canada, Australia and New Zealand and its aim was to eavesdrop on military and diplomatic communications. Nowadays, it can monitor every individual, and that's why people are concerned about it. The European parliament accused Echelon of spying the EU, and sharing its secrets with the UK and the US.

European Union

The European Union values the right of privacy almost more than any other country. The GDPR gives the protection of personal data and the respect for the basic privacy rights. (GDPR is further explained before and below). In fact, the European Court of Human Rights declared that the UK's mass surveillance program violates people's right to privacy.

The National Security Agency (NSA)

NSA leads the US government in cryptology and provides information assurance, and enables computer network operations. Its aim is to help the

government make a decision which is in favor for the Nation and its allies. However, NSA, especially after the Snowden revelations, has been accused of withholding illegal information about the US citizens, spying on them and infringing their right of privacy. (More details in historical background).

Federal Bureau of Investigation (FBI)

The FBI is the US national Security and Intelligence Service and its main federal law enforcement agency. It combats terrorism, cybercrime, public corruption, and other related challenges. It is involved with counterintelligence; however, it doesn't face such strong accusations as NSA.

United Nations Human Rights Council

United Nations Human Rights investigates and reports abuses happening in the whole world. It states that governments should respect the privacy of their citizens at all Costs. Its high commissioner mentioned that mass surveillance is becoming a dangerous habit rather than an exceptional measure. This UN agency has collaborated with the general assembly, and other UN affiliated organizations to solve this problem.

BLOCS EXPECTED

The issue of global mass surveillance is an issue that concerns the whole world. However due to the fact that every country has different policies, laws and regulations, there will be two blocs, each one consisting countries that have mutual policies.

Bloc A

Bloc A will consist of countries with more liberal stance on this topic. Namely, countries who try to respect their citizens' rights, have regulations protecting human rights, and have zero censorship. Such nations are members of the European Union, UK and USA.

Bloc B

Bloc B will consist of countries that reinforce very strict surveillance measures, which can sometimes lead to censorship and infringement on the right of privacy and/or freedom of speech. Such nations are China, Russia, Iran and most of the Middle East countries.

TIMELINE OF EVENTS

Date	Description of event
1939-1945	World War Two, where mainly the Nazis and the US government monitored their citizens in order to find out if someone committed treason.
1947-1991	The beginning of the World War (1947) which led the USA, Soviet Union and their allies to spy on their citizens, in order for them to see if their people had been secretly working with the enemy.
2013	Global surveillance disclosures (Edward Snowden)
February 13, 2018	The beginning of the Huawei vs USA conflict
May 25, 2018	Implementation date of GDPR

RELEVANT RESOLUTIONS, TREATIES AND EVENTS

UN resolution A/C.3/71/L.39/Rev.1

The right of privacy in the digital age.⁵

General Data Protection Regulation (GDPR)

EU'S regulation about its citizens data protection.⁶

International Principles on the Application of Human Rights to Communications Surveillance

The International Principles on the Application of Human Rights to Communication Surveillance (13 Principles), is a policy document which features 13

⁵ <https://undocs.org/A/C.3/71/L.39/Rev.1>

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

guiding principles about limiting surveillance. These principles apply to surveillance conducted within a state or extraterritorially.⁷

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

“Stop Watching Us” Movement

Stop Watching Us is a coalition of about 100 public advocacy organizations and companies. It was established in 2013 to demand the US Congress to investigate the NSA’s actions. So far, its main action has been organizing Rallies against Mass Surveillance where thousands of people participate and demand from the Congress, and generally from the US Government to be heard and to stop Mass Surveillance.

“Restore the fourth” Movement

Restore the Fourth Movement is a non-profit corporation aiming at restoring the Fourth Amendment, (the right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be size to US Constitution and ending mass surveillance. This corporation has organized several protests; it cooperates with the “Stop Watching Us” Movement, and most importantly, it has created a scoreboard which grades members of the Congress in relation to their votes on surveillance and the Fourth Amendment.

GDPR

The basic concepts of privacy protection were set in the 1950s in an European Union convention on human rights, but they didn’t mention anything about electronic storage of personal data. When computers began to be widely used (1980s), the EU created the Data Protection. As the technology was constantly developing, they introduced another convention, the Data Protection Directive, but since it was a directive and not a regulation, every country had the right to create their own versions of it. In 2012, the EU decided that they needed to propose a legislation that every country should follow, so they came up with GDPR. It was created to protect European data citizens’ rights and to guideline personal data collective companies on how to safeguard their clients’ rights.

⁷ https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

Bigger Responsibility, Bigger Repercussions



Amnesty International's action on protecting human rights in the digital age

Amnesty international is a global movement of more than 7 million people who deal with subjects of injustice. It investigates and exposes the facts in cases of abuse either by a government or by a company. One of the most important actions that it has taken against mass surveillance is a 7-point plan that not only guarantees the protection of human rights in the digital age, but also examines some important events that have happened related to mass surveillance and human rights.

POSSIBLE SOLUTIONS

There are many possible solutions to this problem, however most of them are not easy to implement. That is why, we rely on organizations such as the UN to adopt resolutions which urge states to reinforce the proper measures in order to both keep their citizens safe and not infringe their rights. Some possible solutions are:

Diversifying Communication Methods

One of the most important steps to take in order to avoid mass surveillance is diversifying communication methods, ergo using different means of communication. As a result, less data will be stored in electronic devices, and surveillance companies will find it harder to keep track of a person's information. Some ways to diversify communication methods are: going out to have a conversation in person, going to different places either with different people or alone, and incorporating new habits into one's routine.

Creating a global movement that encourages user-side encryption

In today's world, where mass surveillance is becoming more of a threat than a security system, encrypting messages, e-mails, web browsing, document transfers, and even phone calls is becoming more important than ever. Encryption is the process of encoding information to prevent anyone other than its intended recipient from viewing it. Data encryption uses an algorithm (cipher), to convert messages into random symbols. Thus, the encoded message is unreadable to anyone that doesn't have access to a special key used to decrypt the message. That is why many social media apps have encryption option. Those who use unencrypted communication tools are basically open to monitoring by hackers, or worst-case scenario by the government.

Creating secure communication tools

Everyone uses communication tools in their everyday life. The majority of people prefer using easier communication tools, however without that meaning that they are also secure. Usually, the ones that are easier to use, don't have adequate security, and vice versa. Therefore, the goal is to develop technologies that are both secure and user-friendly, and at the same time encouraging companies to adopt high security practices.

Develop guiding legal principles around surveillance and privacy

The International Principles on the Application of Human Rights to Communication Surveillance (13 Principles), is a policy document which features 13 guiding principles about limiting surveillance, and has been the basis for a pro-privacy resolution adopted by the UN. Another regulation which protects citizen's rights from surveillance is the aforementioned GDPR. States and organizations such as the UN, Transparency International, United Nations Human Rights etc., should continue adopting more legal frameworks and resolutions concerning privacy in the age where mass surveillance is continuously increasing, including punishment for those infringing them.

Raising Awareness

The first step to tackle a problem is by being informed about it. Unfortunately, many people don't know that they are being monitored or how to eliminate it. Moreover, the majority of people are irresponsible when it comes to their privacy, as they ignore reading companies and applications' privacy policy, and they rush to accept their terms and conditions. As a result, companies have a written consent that lets them read, handle and use their users' personal data without being legally prosecuted. Also, the notifications and the e-mails by companies are not only

aiming at informing people about their updated privacy policies, but also at asking for their consent.

BIBLIOGRAPHY

Aziz, Yusra. "Mass Surveillance Program Around the World." *PrivacyEnd*, 23 Feb. 2018, www.privacyend.com/mass-surveillance.

Bassine, Juliette. "Huawei vs the USA: How Did It Come to This?" *AndroidPIT*, AndroidPIT, 13 June 2019, www.androidpit.com/huawei-vs-usa-how-did-it-come-to-this.

Boerma, Lindsey. "NSA Programs May Be Legal, but Are They Ethical?" *CBS News*, CBS Interactive, 16 June 2013, www.cbsnews.com/news/nsa-programs-may-be-legal-but-are-they-ethical.

"A BRIEF GUIDE TO COMBATting MASS SURVEILLANCE." *SCQ*, 13 Dec. 2016, www.scq.ubc.ca/a-brief-guide-to-combatting-mass-surveillance.

"Cambridge Analytica Explained: The Facts, Implications, and Open Questions: GIP Digital Watch." *Cambridge Analytica Explained: The Facts, Implications, and Open Questions | GIP Digital Watch*, dig.watch/trends/cambridge-analytica.

"The Cambridge Analytica Story, Explained." *Google*, Google, www.google.com/amp/story/s/www.wired.com/amp-stories/cambridge-analytica-explainer/.

Chen, Brian X. "Why You Should Read All Those GDPR Privacy Policy Updates." *The Sydney Morning Herald*, The Sydney Morning Herald, 24 May 2018, www.smh.com.au/technology/why-you-should-read-all-those-gdpr-privacy-policy-updates-20180524-p4zh5k.html.

"CIA Vision, Mission, Ethos & Challenges." *Central Intelligence Agency*, Central Intelligence Agency, 1 Nov. 2018, www.cia.gov/about-cia/cia-vision-mission-values.

"CODE NAME VERAX: Who Is Edward Snowden, and Why Did He Risk Everything to Tell the World about PRISM?" *Truman Center*, trumancenter.org/doctrine-blog/code-name-verax-who-is-edward-snowden-and-why-did-he-risk-everything-to-tell-the-world-about-prism.

"Document." *Amnesty International*, www.amnesty.org/en/documents/act30/1795/2015/en/.

“Edward Snowden.” *Biography.com*, A&E Networks Television, 12 Apr. 2019, www.biography.com/activist/edward-snowden.

Egwuonwu, Benson. “Everything You've Ever Wanted To Know About Mass Surveillance.” *RightsInfo*, 1 Feb. 2019, rightsinfo.org/explainer-mass-surveillance-human-rights.

“Encrypted Messaging – What Is It, Why Should You Use It and What Are the Best Apps?” *Pixel Privacy*, pixelprivacy.com/resources/encrypted-messaging.

“Espionage in the Cold War.” *History Crunch - History Articles, Summaries, Biographies, Resources and More*, www.historycrunch.com/espionage-in-the-cold-war.html.

The Ethics (or Not) of Massive Government Surveillance, cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/history_worldwars.html.

“Evidence of Global Opposition to US Mass Surveillance.” *Amnesty International UK*, www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq.

“FISA 702 Amendments Renewed, Mass Surveillance in United States Continues: Golden Frog.” *Golden Frog Blog*, 22 Jan. 2018, www.goldenfrog.com/blog/fisa-702-surveillance-amendments-renewed.

“Fourth Amendment.” *Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/constitution/fourth_amendment.

“Freedom on the Net 2017.” *Iran Country Report*, 15 Nov. 2017, freedomhouse.org/report/freedom-net/2017/iran.

Global, IFSEC. “Role of CCTV Cameras: Public, Privacy and Protection - IFSEC Global: Security and Fire News and Resources.” *IFSEC Global | Security and Fire News and Resources*, IFSEC Global | Security and Fire News and Resources, 31 May 2019, www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/.

Greenslade, Roy. “How Hitler Suspended the Right to Mail and Telephone Privacy.” *The Guardian*, Guardian News and Media, 4 Dec. 2013, www.theguardian.com/media/greenslade/2013/dec/04/surveillance-adolf-hitler.

Harding, Luke. "Mass Surveillance Is Fundamental Threat to Human Rights, Says European Report." *The Guardian*, Guardian News and Media, 26 Jan. 2015, www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe.

"Home." *National Security Agency | Central Security Service*, www.nsa.gov/about/civil-liberties/about.

Lee, Timothy B. "Here's Everything We Know about PRISM to Date." *The Washington Post*, WP Company, 12 June 2013, www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-weknow-about-prism-to-date/?noredirect=on&utm_term=.d9c819eb8a8b.

Leprince-Ringuet, Daphne. "The UK's Mass Surveillance Regime Has Broken the Law (Again)." *WIRED*, WIRED UK, 13 Sept. 2018, www.wired.co.uk/article/uk-mass-surveillance-echr-ruling.

"Necessary and Proportionate." *Necessary and Proportionate*, necessaryandproportionate.org/.

News, RTÉ "European Court Rules against UK over Mass Surveillance." *RTE.ie*, RTÉ, 13 Sept. 2018, www.rte.ie/news/europe/2018/0913/993475-eu-court-uk-surveillance.

"NSA Spying." *Electronic Frontier Foundation*, www.eff.org/nsa-spying.

Pernice, Ingolf, and Jörg Pohle. "Privacy and Cyber Security on the Books and on the Ground." *Academia.edu*, www.academia.edu/37563421/Privacy_and_Cyber_Security_on_the_Books_and_on_the_Ground.

Perrone, Jane. "The Echelon Spy Network." *The Guardian*, Guardian News and Media, 29 May 2001, www.theguardian.com/world/2001/may/29/qanda.janeperrone.

"Privacy: Organizations." *Thepublicvoiceorg*, thepublicvoice.org/issues_and_resources/privacy-organizations.

"The Pros and Cons of Government Surveillance." *Rabid Geek*, www.rabidgeek.net/2016/01/08/the-pros-and-cons-of-government-surveillance.

"Redirect Notice." *Google*, Google,

www.google.com/amp/amp.tomsguide.com/us/us-huawei-ban-op-ed,news-30132.html.

Reitman, rainey. "EFF's Game Plan for Ending Global Mass Surveillance." *Electronic Frontier Foundation*, 30 Jan. 2015, www.eff.org/deeplinks/2015/01/effs-game-plan-ending-global-mass-surveillance.

Restore The Fourth, restorethe4th.com/who-we-are/.

"Stop Watching Us: Rally Against Mass Surveillance." *StopWatching.us*, rally.stopwatching.us/.

"Top World Intelligence Agencies > The Deep State Blog." *The Deep State Blog*, deepstateblog.org/deep-states-guide-to-the-worlds-largest-intelligence-agencies/.

"United Nations: Rein in Mass Surveillance." *Human Rights Watch*, 17 Apr. 2015, www.hrw.org/news/2014/07/17/united-nations-rein-mass-surveillance.

User, Super. "Why Was the GDPR Created? A History of EU Data Protection: EC2 IT." *EC2 IT Ltd*, 2 Aug. 2019, www.ec2it.co.uk/gdpr/why-was-gdpr-created-a-history-of-eu-data-protection.

Vivian. "Necessary & Proportionate." *Necessary and Proportionate*, 18 Aug. 2016, necessaryandproportionate.org/principles.

"What We Investigate." *FBI*, FBI, 3 May 2016, www.fbi.gov/investigate.

White, April. "A Brief History of Surveillance in America." *Smithsonian.com*, Smithsonian Institution, 1 Apr. 2018, www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/.

"Who We Are." *Amnesty International*, www.amnesty.org/en/who-we-are/. "Why America's Fight with Huawei Matters." *Google*, Google, www.google.com/amp/s/amp.cnn.com/cnn/2019/01/29/business/huawei-china-us-analysis/index.html.

"Why Is GDPR Important." *Visma.com*, www.visma.com/gdpr/why-is-gdpr-important.

Wilbert, Caroline. "How the CIA Works." *HowStuffWorks*, HowStuffWorks, 14 June 2006, people.howstuffworks.com/cia.htm.

Woods, Mike. "Russia Introduces Not-so-Secret Mass Surveillance." *RFI*, RFI, 3 July 2018, m.en.rfi.fr/20180702-russia-introduces-not-so-secret-mass-surveillance.

IMAGES

Google Search, Google,
www.google.com/search?biw=1366&bih=667&tbm=isch&sa=1&ei=A6tFXd6Z EZPQg wfV_pzoBg&q=gdpr&oq=gdpr&gs_l=img.3..0l5j0i30l5.128355.138833..139417...2.0..3.551.3115.0j2j2j2j1j2.....0.....1..gws-wiz-img.....10..35i39j0i67.U6Rujs3q0BQ&ved=0ahUKEwiep8vlhOfjAhUT6OAKHVU_B20Q4dUDCAY&uact=5#imgrc=EJHqx2kclKS-7M:

Google Search, Google,
www.google.com/search?biw=1366&bih=667&tbm=isch&sa=1&ei=dK1FXdupL a-HjLsP16q-wAU&q=mass%2Bsurveillance&oq=mass&gs_l=img.3.0.35i39j0i9.78937.81005..82627...1.0..4.255.1897.0j3j6.....0.....1..gws-wiz-img.....10..0i30j0i67.zQR65ja904w#imgrc=INzBD8zm7CjAHM:

Google Search, Google,
www.google.com/search?biw=1366&bih=667&tbm=isch&sa=1&ei=S0JIXdrRCJCF1fAP8LWd-A8&q=cambridge%2Banalytica%2Bscandal&oq=cambridge%2Banalytica%2Bscandal&gs_l=img.3..0i19l2j0i5i30i19j0i8i30i19l2.11225.13658..13873...1.0..1.577.2328.0j1j5j1j0j1.....0.....1..gws-wiz-img.M1U6KhTGtng&ved=0ahUKEwiao7ys_evjAhWQQhUIHfBaB_8Q4dUDCAY&uact=5#imgrc=JjWlUsd_w_uG4M: