Committee: Disarmament and International Security - DISEC

Issue: Controlling the use of government surveillance on people using pretexts

Student Officer: Vassiliki Vassiliou

Position: Deputy President

PERSONAL INTRODUCTION

Dear Delegates,

My name is Vassiliki Vassiliou, and I am an 11th grade student at the American College of Greece, Pierce. In this year's ATSMUN, I will be serving as a Deputy President of the Disarmament and International Security Committee (DISEC) and it truly is my utmost honor to do so. I began attending Model United Nations conferences about a year ago and, since then, I have fallen in love with the MUN world. The combination of politics, international affairs, and human rights utterly captivated me from the very beginning of this journey and, due to that, since my first conference, I have attended almost every one that I could. I really hope this conference is an eye opening, productive and educational experience for all of you! Even though this will be an online conference due to the pandemic regulations and I will not be able to meet you all in real life, I am sure this experience will be rewarding!

This study guide will assist you in thoroughly understanding the topic of: "Controlling The use of government surveillance on people using pretexts" in order for you to be able to prepare your own solutions and participate in the fruitful debate on the resolutions. You are highly encouraged to carry out your own research too. After the "Bibliography" section there will be another section with helpful links that will surely assist you in doing so.

If any questions or problems arise, please do not hesitate to contact me. (vassiliouvassiliki70@gmail.com)

I am very excited to meet you all and I wish you the best of luck with your preparation!

Best Regards,

Vassiliki Vassiliou

INTRODUCTION

Due to the continuous integration of the digital aspect in our day-to-day life, the containment of government surveillance has become practically impossible. Social engineering, a form of psychological manipulation, is frequently used by governmental services to obtain personal data that can contribute to maintaining national security and public safety. A commonly used form of social engineering is pretexting.

Pretexting is a term used to describe impersonation and the creation of fake scenarios. By impersonating persons with authority, the attacker gains the victim's trust and takes advantage of them. As this is an example of covert surveillance, the victim is unaware of the fact that they are being interrogated by government officials. It is evident that, this form of surveillance is an ultimate breach of the Universal Declaration of Human rights (UDHR) as the individual's right to privacy is not respected.

Despite the unethicality of the pretexting technique, pretexting is the most commonly used social engineering method amongst investigators. The authorization process for both Directed and Intrusive surveillance is brief resulting in minor consequences for the violation of individuals' rights.

Regardless of the intensity and the urgency of the worldwide issue of cybersecurity, the number of legislations protecting personal data is devastatingly low. Even the Data Protection Acts that have been created are not part of the authorization of covert surveillance and therefore are regularly breached. More specifically, the only Act that contributes to the process, as of now, is the Regulation of Investigatory Powers Act of 2000 (RIPA).

As long as governmental network transparency simply does not exist, the issue of human rights abuses in the digital world will remain timely.

DEFINITION OF KEY TERMS

The pretext technique

Pretexting is an investigating technique used to manipulate people to divulge hidden information. The attacker engages with the victim through the creation of a fake scenario and the impersonation of someone else (usually of a person in a position of power).

Pretext

"Pretext is a pretended reason for doing something that is used to hide the real reason[1]."

Surveillance

"Surveillance is the continuous observation of a place, person, group, or ongoing activity in order to gather information[2]."

Social Engineering

"Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps.[3]"

Social Credit System

The social credit system is a diverse network of initiatives aiming to secure trust within a community. The system gathers personal data through both governmental and private bodies and later shares it with algorithms that process it accordingly. These algorithms are also referred to as the "personal credit platform". The social credit system is often called a « blacklist » as after the data is collected, individuals are divided into two categories, the trustworthy ones and the ones that are not. The citizens with the highest trustworthiness scores are awarded and the ones with the lowest are punished by the government.

Covert Surveillance

Surveillance is covert if it's done in a way that tries to ensure the subject is unaware it is, or could be, taking place. There are two types of Covert Surveillance: Directed and Intrusive.

---

[1] "Pretext." *Cambridge Dictionary* . https://dictionary.cambridge.org/dictionary/english/pretext

[2]("Surveillance | Definition of Surveillance at Dictionary.Com")https://www.dictionary.com/browse/surveillance

"What Is Social ENGINEERING: Attack Techniques & PREVENTION Methods: Imperva." *Learning Center*, 29 Dec. 2019, www.imperva.com/learn/application-security/social-engineering-attack/#:~:text=Social%20engineering%20is%20the%20term,in%20one%20or%20more%20steps.

Directed Surveillance

It is the 'monitoring of targets' movements and conversations. Authorization for Directed Surveillance can only be granted when it is considered proportionate and necessary under the Regulation of Investigatory Powers Act of 2000 (RIPA), The most common reasons why this type of surveillance is used is for ensuring public safety, national security and public health.

Intrusive Surveillance

It is covert surveillance that is carried out in relation to anything taking place on residential premises or private vehicles. Due to the unethicality of this action, intrusive surveillance can only be authorized when the reason behind it is either ensuring national security or ensuring the economic well-being of the country.

BACKGROUND INFORMATION

History of government surveillance

The exact timeframe of the beginning of government surveillance is a topic frequently debated on, but the majority of scientists date it back to the creation of the "Five Eyes". The "Five Eyes" is an alliance between England, the United States, Canada, Australia and New Zealand that was created during the Cold War (1947) to monitor the Soviet Union. Up to the present, the "Five Eyes" have created the largest mass surveillance system named ECHELON and signed the UKUSA agreement, one that allows the monitoring of citizens and the constant collection of personal data that can later be shared using "security reasons" as a pretext.

Government surveillance is defined as the constant observation and monitoring of citizens through artificial intelligence, in ways such as biometrics and social security analysis, as well as through social engineering. CCTV technologies, one of the most common surveillance methods, were introduced back in 1959 while the first speech detector was prototyped years later in 1976. Currently, the main surveillance method used by governments to monitor individuals is computer and network surveillance.

Social engineering is a manipulation technique used to collect personal data by controlling the victim. More specifically, social engineering is covert surveillance that consists of methods such as baiting, phishing and, the only method used by governments, pretexting.

The pretexting technique is defined as the creation of fake scenarios and the impersonation of a person with authority in order to gain the victims' trust and obtain their personal data. Pretexting is frequently used by governmental services such as investigating agencies. Pretexting was one of the early stages of social engineering in cybersecurity as it was introduced in 1974 by the FBI.

Throughout the past two years, the Covid 19 pandemic has been used as a pretext or, in other words, as an excuse for the large and constant expansion of digital government surveillance. New technologies such as tracking systems, facial recognition systems, cell-phone apps and, most importantly, public health systems that collect personal data to alleviate the spread, have all led to the absolute reduction of privacy and to the destruction of democratic societies. Additionally, studies show that almost all short-term emergency measures will become timely after the coronavirus pandemic and therefore it is necessary that we act immediately.

The underlying reason behind government surveillance and its unethicality

The main reason why governments began using surveillance to monitor their citizens is to ensure national security. As mentioned before, government surveillance began after the Second World War to control opponents just like it is still used to monitor foreign enemies and to prevent terrorist attacks. This became evident after the well-known terrorist attack on the 11th of September 2001, when mass surveillance expanded rapidly. Governments took legislative measures, adapted new surveillance programs and increased the authority of secret intelligence agencies such as the FBI or the NSA. Since then, the constant controlling of citizens' actions, conversations and surroundings has been considered justifiable and reasonable, thus individuals have given up their privacy for security. It is important to mention that it is widely believed that pretexting was actually documented for the first time in human history during the Trojan horse attack, when the Greeks hid inside a giant horse and presented it as a gift from Athena in order to manipulate the city of Troy and utterly destroy it.

Even though we cannot argue that surveillance has not prevented terrorist attacks since global statistics do show the opposite, it is still extremely important to highlight that the possibility of terrorist attacks happening, does not in any way justify the consent violation of individuals' human rights. Innocent citizens have become goverments' targets since their private lives are fully exposed to government officials. Numerous modern-day philosophers

such as Yuval Noah Harari argue that democracy cannot withstand covert or overt surveillance as it opposes its values of free speech, free will and social justice.

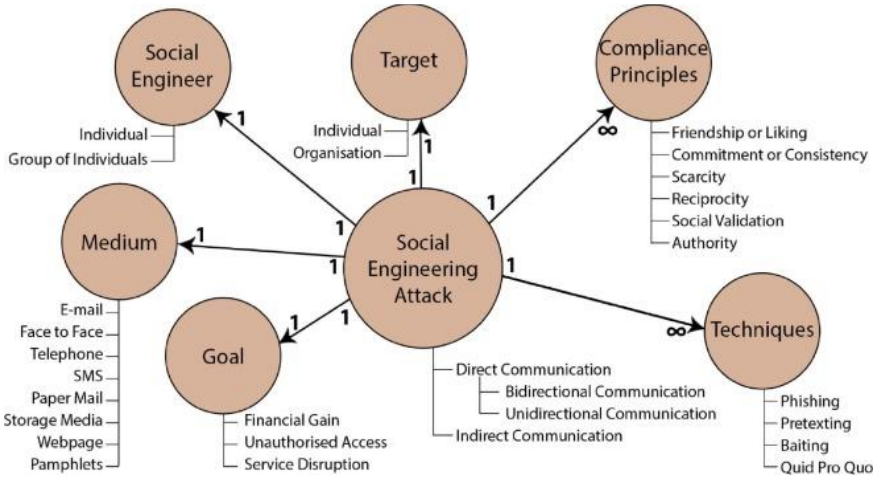

Figure 1: Brief Explanation of Social Engineering Attacks

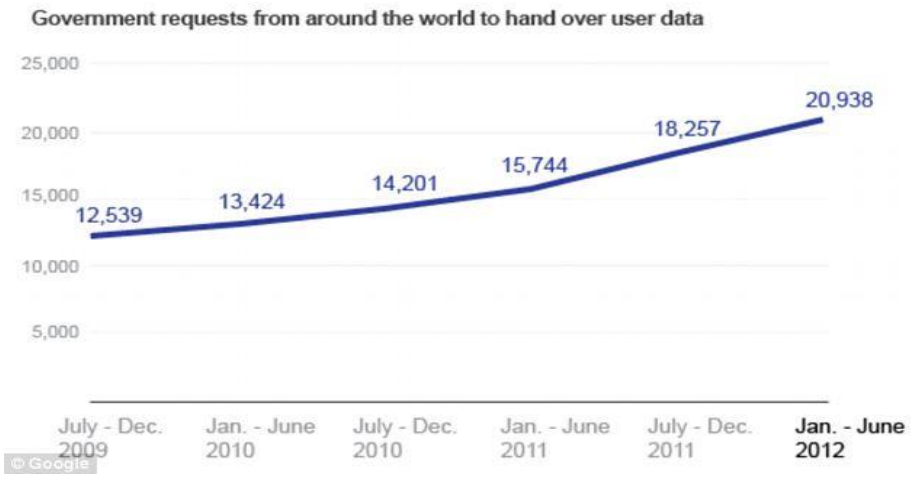

Figure 2: The rise of governmental surveillance between 2009 and 2012, the main time period of government surveillance's growth

ECHELON

Echelon is a surveillance program whose members are the "Five eyes". The "Five Eyes" consist of five English-speaking countries: the United States of America, the United Kingdom, Australia, Canada and New Zealand. The surveillance program was created back in 1946 when the United Kingdom-United States Agreement on security was signed by the aforementioned countries. Even though ECHELON started out as a surveillance system to

monitor and analyze the cyber communications of the Soviet Union and its allies during the cold war, it has now become the largest mass surveillance and industrial espionage network to ever exist. "In February of 2000, 60 Minutes published a report detailing the existence and scope of ECHELON. Mike Frost, a former spy for Canada's NSA-equivalent, CSE, told the host just how large the program's reach really was, ``Echelon covers everything that's radiated worldwide at any given instant." Echelon operated in secret until 1980 when it started being referenced by authors. Until then, the public was completely unaware of both ECHELON and the "Five Eye" cooperation itself. ECHELON is constantly collecting internet and communications data of both civilians and government officials with almost no restrictions. Approximately, monitoring spyware has been installed in more than 50 thousand computer networks globally by the Five Eyes. The ECHELON surveillance program is widely known for its "keyword search". More specifically, there are certain keywords that might refer to terrorist activities, to which the program responds when collecting data from citizens' communications. A noteworthy incident that highlights the program's threat to privacy is the following: Back in 1999, during a call with her friend, a woman mentioned how her son "bombed last night", referring to his performance at a school play. Due to the fact that the word "bomb" is one of the aforementioned keywords, the woman was noted down as a possible terrorist and later had to be investigated.[4]

Existing benefits and potential advantages of government surveillance's use if it becomes regulated and contained

Despite the current devastating situation of government surveillance and control, it is necessary to mention the benefits of surveillance as long as it becomes regulated. As

[4] Matney, Lucas. "Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life." *TechCrunch*, TechCrunch, 3 Aug. 2015, techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJ21NIiLL_hiyzOLTuUeNVDJkdiny3FlITXzJjxbFS38nQEH48u4HMQmr10ReAeCtuJw9x7muidH8mSsz9GCx2Iqc1mMeNgrkclIKgjfwpgrxB7Y1l1JCkpR_6L_JBx_7tMoYJbBYu_r4k2ilFCvDeuSbNEEesEjkLLX9CqIpt41.

mentioned before, the main purpose of surveillance and the reasoning behind its creation is the protection of citizens from violent forces, or, in a simplified manner, terrorism. Until now, hundreds of terrorist attacks have been prevented through the use of both communication and camera surveillance. Crime rates have been reduced and national security has increased as data collection surveillance can easily provide law enforcement with the information that is necessary for investigations to occur. Thousands of citizens have publicly vocalized their appreciation towards government surveillance as it creates a constant feeling of safety, an almost non-existent feeling in today's world.

As long as the necessary measures are taken in order to ensure that government surveillance does not violate individuals' right to privacy and citizens are aware of and consent to the collection of their personal data, government surveillance can actually be extremely beneficial for public security and health.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

China

China's mass surveillance network is the largest surveillance network in the world. Despite the continuous camera, biometric, data mining and telephone surveillance, China's government has also developed a social credit system. The system monitors and analyzes the social behaviors of individuals and consequently rated their trustworthiness. For the system to operate, the individuals are identified through facial recognition and the collected data is stored in their personal credit platform. The trustworthiness scores of the citizens are regularly updated. Participation in the Chinese social credit system was voluntary for years until it became mandatory in 2020. Since then, Sesame Credit has been used by citizens in order for individuals with higher trustworthiness scores to be awarded with a wealthier and more convenient life than the ones with lower credit scores. [5]

United States of America

The United States mass surveillance network growth begun during World War I and World War II but continued all throughout the Cold War period. In order to maintain national safety by silencing political dissent, secret intelligence agencies such as NSA, CIA and the FBI

[5] "Mass Surveillance in China." *Wikipedia*, Wikimedia Foundation, 7 May 2021, en.wikipedia.org/wiki/Mass_surveillance_in_China#Social_credit_system.

were created. The United Kingdom-United States Agreement on surveillance of 1946 between the five eyes contributed to the constant attempts to prevent digital communications and to the rise of government surveillance rates. After the 9/11 attack, domestic surveillance rapidly grew in order to prevent cyberterrorist attacks. The US government uses computer, camera and telephone surveillance in an attempt to ensure public security and for cyber-crime to be prevented. Additionally, the Fourth Amendment, an Amendment that protects the privacy rights of individuals, rights that the pretexting investigation technique completely and utterly disregards, became part of the United States Constitution back in March 1792.

Israel

Israel's involvement in mass surveillance is mainly through the Niv, Shalev and Omri (NSO) group, an Israel-based platform that develops Pegasus. Pegasus is a spyware that provides governments with access to individuals' personal data, location and digital devices. In their website its stated that "NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe." [6] Their actions are a perfect example for the term 'Covert Surveillance" that, as stated before, violates individuals' right to privacy. Additionally, the NSO group has repeatedly denied giving out their partners' names.

Russian Federation

Since the Covid-19 outbreak, Russia's surveillance state has been rapidly becoming more and more severe. Facial recognition surveillance has become one of the main methods of monitoring Russian citizens. In fact, due to insufficient protection of the data, it is accessible for a very low price in the black market, meaning that individuals' human right to privacy is completely and utterly violated. These facial recognition systems can recognize an individual from up to 50 meters away without them facing the camera as it analyzes a person's walk, body movements, voice, and tattoos. Russia is one of the top 5 countries with the largest number of CCTV cameras per 1000 people (93) and it is estimated that 33% of them are installed by the state. During the pandemic, these systems have been used in order

[6] *Nsogroup.com*, www.nsogroup.com/.

to recognize and fine individuals who violate the emergency safety rules. Furthermore, Russian authorities also use a cellphone app called Social Monitoring in order to enforce quarantine rules and other Covid 19 policies. Additionally, within the next 3 years, Russia is planning on creating a fingerprint bank that collects data from both Russians and foreigners.

The United Kingdom

In 2018, during a ruling held at the Grand Chamber of the European Court of Human Rights, 17 judges agreed that the British surveillance system violated the European Convention on Human Rights that protects European individuals' right to privacy as the UK government did not sufficiently nor efficiently protect citizens' personal data. The information collected by monitoring individuals' calls, text messages and emails was easily accessed by outsiders. Additionally, the UK is the leading of the top countries with the largest number of CCTV cameras per 1000 people. More specifically, in the United Kingdom there are 153 cameras per 1000 citizens. Despite that, The RIPA is an Act of Parliament of the United Kingdom that governs the use of covert surveillance by public bodies including bugs, video surveillance and interceptions of private communications and private agents. The Act distinguishes between interception of private communications and communications data directed surveillance and intrusive surveillance as the authorization process differs for all. The Act states that to use covert techniques it needs to be necessary, proportionate, lawful and compatible with the Human Rights Act.[78].

[7] "Regulation of Investigatory Powers Act 2000." *JUSTICE*, 15 June 2015, justice.org.uk/regulation-investigatory-powers-act-2000/.

[8] Council, Hinckley & Bosworth Borough. "Regulation of Investigatory Powers Act (RIPA)." *Overview | Regulation of Investigatory Powers Act (RIPA) | Hinckley & Bosworth Borough Council*, Hinckley & Bosworth Borough Council, 20 Dec. 2010, www.hinckley-bosworth.gov.uk/info/10020/strategies_plans_and_policies/609/regulation_of_investigatory_powers_act_ripa.

Country	# of CCTV Cameras	# of People	# of CCTV Cameras per 100 People
United States	50 000 000	327,167,430	15.28
China	200 000 000	1,392,730,000	14.36
United Kingdom	5 000 000	66,488,990	7.5
Germany	5 200 000	82,927,920	6.27
Netherlands	1 000 000	17,231,020	5.80
Australia	1 000 000	24,992,370	4
Japan	5 000 000	126,529,100	3.95
Vietnam	2 600 000	95,540,400	2.72
France	1 650 000	66,987,240	2.46
South Korea	1 030 000	51,635,260	1.99

Figure 3: Some of the most surveilled countries in the World and the number of CCTV cameras per 100 people.

Electronic Frontier Foundation (EFF)

The Electronic Frontier Foundation is a non-profit organization created in 1990 in order to protect human rights in the digital world during the rise of cyber surveillance. “EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.” The EFF has taken several legislative measures to control cyber-Surveillance and has had multiple legal victories such as: Bern v. US Department of Justice, MGM v. Grokster, Steve Jackson Games v. Secret Service Case service, and the list goes on. They have organized events and put out numerous press releases resulting in the creation of a vast network of concerned users and volunteers.

Amnesty International (1961)

Amnesty International is a non-governmental organization that fights against global abuses of human rights. In order to ensure public safety, they investigate and expose the abuses, they lobby governments and organizations with authority in order to ensure that they are respecting international law and, most importantly, acting accordingly to the ‘Declaration of Human Rights’. They investigate and expose the facts, whenever and wherever abuses happen. Throughout their journey since the creation of the organization in 1961, they have gained millions of followers that volunteer and advocate for human rights. Amnesty International heavily focuses on the fight against government surveillance and its human rights violations. They have managed to uncover governments’ breaches of international

treaties aiming to protect individuals' rights to privacy and have exposed their actions through hundreds of articles. They advocate for the preservation of the human right to privacy through protests and publications as well as signing petitions and advising individuals on how to protect their personal data. They have also focused on biometric surveillance and have called for a ban of their use along with almost 200 more organizations. [9]

Privacy International (PL)

Privacy International is a London-based non-profit charity created in 1990, aiming for the protection of individuals' rights to privacy. Privacy International acts in various ways such as through conducting research studies, advocacy and the creation of public campaigns, assisting organizations with the same goals and taking legislative measures. Until now, they have changed the surveillance state of 20 different countries and have won 10 court cases against harmful surveillance practices.

TIMELINE OF EVENTS

Date	Description of Event
1792	The 4th Amendment was added to the Constitution of the United States.
1940	The UKUSA Agreement was jointly enacted by the United Kingdom and the United States
1946	The ECHELON surveillance program was created by the Five Eyes.
1948	The Universal Declaration of Human Rights (UDHR) was created.

[9] "Latest." *Amnesty International*, 3 July 2021, www.amnesty.org/en/latest/.

1964	The United Kingdom-United States Agreement (UKUSA) on surveillance was signed by the five eyes.
1971	The global surveillance network was created.
1998	Data Protection Act was implemented
2000	The Regulation of Investigatory Powers Act (RIPA) was created.
2017	The United Nations Human Rights Council resolution on `'The right to privacy in the digital age "was ratified by all member states.
2018	The General Data Protection Regulation (GDPR) was introduced.
2018	Creation of the Data Protection Act, an act that surpassed the 1998 Data Protection Act

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

General Assembly Resolution 217A: Universal Declaration of Human Rights, Article no.12; "The right to privacy" (December 10, 1948)

The Universal Declaration of Human Rights is a General Assembly Resolution created after the second World War which guarantees the rights of every individual. Article 12 states that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

UN Human Rights Council Resolution on "The right to privacy in the digital age'; Article no.34 (March 23, 2017)

This HRC Resolution was created and adopted at the 73rd session of the UN General Assembly. Its main purpose is to ensure that "all individuals in the world share an inalienable right to protect their identities". It raises concern over the current violation of human rights by surveillance and highlights the importance of an individuals' privacy in regards to their safety. The resolution was adopted without a vote.

UN's International Covenant on Civil and Political Rights (ICCPR, December 16, 1966); Article 17

The ICCPR is a multilateral treaty created by the UN on 23 March 1976. The counties that have ratified this Covenant are obliged to protect and respect basic human rights. Article 17 of the ICCPR states that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, not to unlawful attacks on his honor and reputation." The covenant consists of many more Articles that can assist individuals and organizations to advocate against the abuse of power and the violation of human rights due to surveillance. Article 19, for instance, states that "Everyone shall have the right to hold opinions without interference.

Side event on cyberspace and international peace and security held by the United Nations Institute for Disarmament Research (UNIDR) on October 5, 2016, during 71st Session of the General Assembly First Committee (DISEC)[10]

During the side event, three experts on security in the digital world discussed cybersecurity and its impact on economic, scientific, social, and political grounds, in detail. Throughout this event, the aforementioned experts raised concerns over the current surveillance situation worldwide and discussed its disadvantages.

[10] "The UN, Cyberspace and International Peace & Security-Side Event-October 5th – UNODA." *United Nations*, United Nations, www.un.org/disarmament/ar/update/the-un-cyberspace-and-international-peace-security-side-event-october-5th/.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The telephone records and privacy protection Act of 2006

This Act states that « utilizing pretexting to buy, sell, or obtain phone records » is a federal offense. It is one of the two Acts existing that specifically direct pretexting. The Act Doubles fines and imposes an additional five-year prison term for violations occurring in a 12-month period. It prohibits investigators from "(1) making false or fraudulent statements to an employee of a covered entity or to a customer of a covered entity; (2) providing false or fraudulent documents to a covered entity; or (3) accessing customer accounts of a covered entity through the Internet or by fraudulent computer-related activities without prior authorization[11]".

The Gramm-Leach-Bliley Act

This Act passed in November 1999 and is part of the 106th United States Congress. It states that « Soliciting others to obtain financial information via pretext » is illegal. Additionally, it makes it necessary for companies to inform the customer about the collection of their personal data.

The European Convention on Human Rights (ECHR)

The ECHR came into force on the 3rd of September, 1953 aiming to protect Human rights and Fundamental Freedoms. Article 18 of the ECHR provides a right to respect for an individual's « private and family life, his come and his correspondence ». Additionally, Article 1 makes the perseverance of individuals' human rights mandatory and, as privacy is a human right, it declares its respect necessary.

General Data Protection Regulation (EU, 2018)

The General Data Protection Regulation is part of the European Union Law and aims to protect individuals' personal data and privacy. It controls how data will be transferred both in and out of Europe. It was created back on 14 April 2016 but was implemented two years later, on 25 May, 2018. The GDPR consists of the right to be informed, the right to access, the right to erasure, the right to data portability and the right to rectification.

Data Protection Act (United Kingdom Act of Parliament,2018)

The Data Protection Act came into effect on the 1st of January, 2021 but was created back in 2018 and is part of the UK parliament. The DPA controls how European citizens' personal information is used by organizations, businesses and, most importantly, the government. It is fundamental for the provision of the human right to privacy.

Data Protection Act, 1998

The DPA is an Act designed to protect citizens' personal data. It regulates how and when personal information can be obtained and used in order to ensure security. This Act was later surpassed by the previously mentioned Data Protection Act of 2018.

POSSIBLE SOLUTIONS

The remodification of Covert Surveillance's Authorization Process

As it has already been mentioned in the topic's introduction, the only Act that a covert surveillance attack has to be in accordance with in order to be authorized, is the Regulation of Investigatory Powers Act of 2002. (RIPA) Taking into consideration that monitoring and psychologically manipulating someone without consent or a warning violates numerous regulatory instruments such as the Universal Declaration of Human Rights, the HRC "The right to privacy in the digital age" Resolution, the 4th Amendment, the European Convention on Human rights and the Data Protection Act, the authorization process should be much more complicated and the consequences for breaching the aforementioned treaties and policies much more severe. Additionally, the authorization under the RIPA should not be used as a defense against claims of interference with an individual's right to privacy under Article 8 of the European Convention on Human Rights.

Despite that, it is important to recognize that government surveillance is extremely important for national security and public health, and the only reason why we owe to control it is to protect innocent citizens that unjustifiably and unreasonably get convicted for crimes that they did not commit. Lastly, even if someone does plead guilty to all their offenses, their human rights should still be respected as stated in the International Covenant on Civil and Political Rights (ICCPR).

Impeachment of unlawful investigators

Despite the severe unethicality of social engineering, pretexting is the most commonly used social engineering technique amongst investigators. The violation of individuals' human rights should under no circumstances be excused and the consequences that the person responsible should bear, must be harsh. It is necessary that private investigations are constantly controlled by either UN bodies or non-governmental organizations in order to ensure that all is conducted in accordance with international treaties. The violation of treaties should be severely punished through either fining or even imprisonment. In order for democratic regimes to withstand the surveillance epoch, the abuse of power shall not be disregarded.

Establishment of a related United Nations body

Such a body would have complete authority over the actions of governments regarding covert surveillance, and will be able to inhibit their execution. Furthermore, its existence would be necessary as it is essential that governments and governmental corporations such as investigation agencies are constantly monitored as their authority does not award them with the right to violate international policies and regulations regarding human rights. Such a body shall specifically focus on controlling ECHELON as even if it is the largest surveillance network worldwide and has been accused for numerous breaches of international treaties, its monitoring is non-existing. Additionally, it must introduce conventions that will regulate the use of new technologies such as tracking systems, facial recognition systems and cell-phone apps that collect personal data. The issue of covert surveillance and, more specifically, pretexting, is not touched upon sufficiently by the UN, thus the creation of treaties and policies has not occurred yet. This could also be a subsidiary body of a pre-existing one such as the Human Rights Council, as it deals with human rights violations. It is mandatory that the required measures are being taken to counter the constant violation of individuals' human rights. Due to the Covid 19 pandemic, the emergency safety measures are estimated to continue existing for the next few decades and therefore the urgency of the current surveillance issue will rapidly increase.

HELPFUL LINKS:

https://www.carlisle.gov.uk/Council/Council-and-Democracy/Regulation-of-Investigatory-Powers-Act"About Eff." Electronic Frontier Foundation, 11 May 2021, www.eff.org/about.-RIPA

Privacy in the Digital Age. www.article19.org/data/files/HRC.34.L.7.Rev1_Privacy_in_the_digital_age_1.pdf.

"I Think I'm under Surveillance." *Liberty*, 6 Mar. 2020, www.libertyhumanrights.org.uk/advice_information/i-think-im-under-surveillance/. .

"Privacy International: About Privacy International." *Privacy International | About Privacy International*, privacyinternational.org/about.

Luxmoore, Matthew. "As Russia Lifts Lockdowns, Expanded Surveillance Network May Remain." *RadioFreeEurope/RadioLiberty*, As Russia Lifts Lockdowns, Expanded Surveillance Network May Remain, 12 June 2020, www.rferl.org/a/as-russia-lifts-lockdowns-expanded-surveillance-network-may-remain/30665176.html

Mouton, Francois, et al. "Social Engineering Attack Examples, Templates and Scenarios." *Computers & Security*, Elsevier Advanced Technology, 21 Mar. 2016, www.sciencedirect.com/science/article/pii/S0167404816300268.

Matney, Lucas. "Uncovering Echelon: The Top-Secret Nsa/Gchq Program That Has Been Watching You Your Entire Life." *TechCrunch*, TechCrunch, 3 Aug. 2015, techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/.

BIBLIOGRAPHY

FBI Monograph: Pretext and Cover Techinques . 6 May 2008, www.governmentattic.org/docs/FBI_Pretexts_and_Cover_Techniques_May-1956.pdf

HRC.34.L.7.Rev1 Privacy in the Digital Age. 22 Mar. 2017, www.article19.org/data/files/HRC.34.L.7.Rev1_Privacy_in_the_digital_age_1.pdf

politics, NickMy passions are, et al. "Countries With the Best Data Privacy Laws: ExpressVPN Blog." *Home of Internet Privacy*, 17 Nov. 2020, www.expressvpn.com/blog/10-countries-with-top-data-privacy-laws/

.Diggelmann, Oliver, and Maria Nicole Cleis. "How the Right to Privacy Became a Human Right." *OUP Academic*, Oxford University Press, 7 July 2014, academic.oup.com/hrlr/article/14/3/441/644279#:~:text=The%20final%20wording%20with%20'privacy,UDHR%20on%2010%20December%201948

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

"Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles - Article 12." *OHCHR*, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23907&LangID=E

"Pretexting." *Pretexting - an Overview | ScienceDirect Topics*, www.sciencedirect.com/topics/computer-science/pretexting

"Fourth Amendment." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., www.britannica.com/topic/Fourth-Amendment#:~:text=Fourth%20Amendment%2C%20amendment%20(1791),seizures%20of%20individuals%20and%20property

Guide on Article 8 of the European Convention on Human Rights. 31 Dec. 2020, www.echr.coe.int/documents/guide_art_8_eng.pdf

"Universal Declaration of Human Rights." *United Nations*, United Nations, www.un.org/en/about-us/universal-declaration-of-human-

rights#:~:text=Drafted%20by%20representatives%20with%20different,all%20peoples%20and%20all%20nations

"Surveillance and Society: NGOs." *Research Guides*, guides.lib.uci.edu/c.php?g=473354&p=3250086.

PRETEXT SEARCHES AND THE FOURTH AMENDMENT: UNCONSTITUTIONAL ABUSES OF POWER. scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3859&context=penn_law_review

Willingham, Brian. "Brian Willingham." *Diligentia Group*, Brian Willingham Https://Diligentiagroup.com/Wp-Content/Uploads/2021/01/DG_mainlogo-Navy@2x.Png, 17 Sept. 2020, diligentiagroup.com/legal-investigation/what-is-pretexting-and-is-it-legal/

Crocker, Cindy Cohn and Andrew. "The Long Fight to Stop Mass Surveillance: 2018 in Review." *Electronic Frontier Foundation*, 3 Jan. 2019, www.eff.org/deeplinks/2018/12/long-fight-stop-mass-surveillance-2018-review

"Fourth Amendment." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., www.britannica.com/topic/Fourth-Amendment#:~:text=Fourth%20Amendment%2C%20amendment%20(1791),seizures%20of%20individuals%20and%20property

Mouton, Francois, et al. "Social Engineering Attack Examples, Templates and Scenarios." *Computers & Security*, Elsevier Advanced Technology, 21 Mar. 2016, www.sciencedirect.com/science/article/pii/S0167404816300268

Burgess, Matt. "What Is GDPR? The Summary Guide to GDPR Compliance in the UK." *WIRED UK*, www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018#:~:text=The%20full%20GDPR%20rights%20for,automated%20decision%20making%20and%20profiling

"What Is Social Engineering: Attack Techniques & Prevention Methods: Imperva." *Learning Center*, Imperva, 29 Dec. 2019, www.imperva.com/learn/application-security/social-engineering-attack/

"I Think I'm under Surveillance." *Liberty*, 6 Mar. 2020, www.libertyhumanrights.org.uk/advice_information/i-think-im-under-surveillance/

Covert Surveillance. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

"Scam." *Cambridge Dictionary*, dictionary.cambridge.org/dictionary/english/scam

"The UN, Cyberspace and International Peace & Security-Side Event-October 5th – UNODA." *United Nations*, United Nations, www.un.org/disarmament/ar/update/the-un-cyberspace-and-international-peace-security-side-event-october-5th/

Rosen, Rebecca J. "Google: 'Government Surveillance Is on the Rise'." *The Atlantic*, Atlantic Media Company, 13 Nov. 2012, www.theatlantic.com/technology/archive/2012/11/google-government-surveillance-is-on-the-rise/265164/

"Mass Surveillance in China." *Wikipedia*, Wikimedia Foundation, 7 May 2021, en.wikipedia.org/wiki/Mass_surveillance_in_China#Social_credit_system

Barshad, Amos, et al. "Inside Israel's Lucrative - and Secretive -Cybersurveillance Industry." *Rest of World*, 9 Mar. 2021, restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/

Matney, Lucas. "Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life." *TechCrunch*, TechCrunch, 3 Aug. 2015, techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJ21NIiLL_hiyzOLTuUeNVDJkdiny3FlITXzJjxbFS38nQEH48u4HMQmr10ReAeCtuJw9x7muidH8mSsz9GCx2Iqc1mMeNgrkclIKgjfwpgrxB7Y1l1JCkpR_6L_JBx_7tMoYJbBYu_r4k2ilFCvDeuSbNEEesEjkLLX9Cqlpt41

"ECHELON." *Wikipedia*, Wikimedia Foundation, 9 June 2021, en.wikipedia.org/wiki/ECHELON

Nsogroup.com, www.nsogroup.com/

"France: New Security Law Risks Dystopian Surveillance State." *Amnesty International*, www.amnesty.org/en/latest/news/2021/03/france-new-security-law-risks-dystopian-surveillance-state/

Council, Hinckley & Bosworth Borough. "Regulation of Investigatory Powers Act (RIPA)." *Overview | Regulation of Investigatory Powers Act (RIPA) | Hinckley & Bosworth Borough Council*, Hinckley & Bosworth Borough Council, 20 Dec. 2010, www.hinckley-bosworth.gov.uk/info/10020/strategies_plans_and_policies/609/regulation_of_invest

"Regulation of Investigatory Powers Act 2000." *JUSTICE*, 15 June 2015, justice.org.uk/regulation-investigatory-powers-act-2000/

igatory_powers_act_ripa.

"Latest." *Amnesty International*, 3 July 2021, www.amnesty.org/en/latest/

"Social Credit System." *Wikipedia*, Wikimedia Foundation, 8 July 2021, en.wikipedia.org/wiki/Social_Credit_System.

.