Committee: Disarmament and International Security Committee (GA1)

Topic: Assessing the use of surveillance as a means of maintaining international and national security

Student Officer: Stefania Vasileiadou

Position: Co-Chair

Personal Introduction

Dear delegates,

My name is Stefania Vasileiadou, and I am a 1st year International Baccalaureate student at Psychico College – Hellenic American Educational Foundation. I am immensely honored to be serving as a Co-Chair in CSMUN 2021 and truly delighted to be setting off my Student Officer career in GA 1. Some would argue that MUN is merely an extracurricular, yet to me, it has grown to be far more beyond that. Not only has it helped me upgrade my academic skillset, but also evolve into a more conscientious and aware individual.

Through this study guide, I am hoping to provide you with knowledge that will incite your intellectual spirit and allow us to have a fruitful debate. Nonetheless, it is no secret that the Disarmament and International Security Committee is one that requires strong argumentative and reasoning skill as well as thorough preparation which you are expected to do leading up to the conference. While this study guide will provide you with a lot of the knowledge on the specific topic, you will also have to do a lot of independent research on your countries' policies and perspectives on the issue as well as their relations with other nations. I wish for all to utilize their diplomatic abilities to the uttermost and cannot wait to meet you in October!

Yours truly,

Stefania Vasileiadou

svasileiadou@athenscollege.edu.gr

Topic Introduction

Left in a state of reparation, soon after the end of World War II, governments started approving the implementation of Mass Surveillance systems which ultimately helped preserve the security of the states and promote societal development. Global concern regarding the universal goal of maintaining worldwide peace and security has resulted to surveillance comprising a technological tool critical to ensure not only national, but also international security.

Needless to say, technology has evolved greatly since the 1940s, and, consequently, so has surveillance. Contemporarily used even for domestic purposes, surveillance is everywhere around us. However, as practical as it may seem, surveillance also has an unseen side that has come to terrify the few that are aware of its existence; that is the threat it imposes on Human Rights. Essentially, contrary to the initial purpose of its invention, surveillance is now used in a manner that is commonly described as irrational and invasive in regard to privacy. Nowadays, although many remain under the impression that they appear uninteresting to governments, no one can live life spared of the fear of being surveilled – even the surveillance of ordinary people is valuable to governments.

Capital investments by the main supplier countries of the global Surveillance Market which permit them access to foreign datasets have led to the surfacing of many questions relating to the preservation of Human Rights. Public ignorance has caused the severity of the issue to increasingly get more bloated, with many unknowingly consenting to being monitored. The universal shift towards an automated lifestyle amply satisfies the purpose of convenience. However, what commonly goes disregarded is that the devices people are planting inside their households serve an additional purpose rather than that of their creation, that being data accumulation.

What is now critical is for a middle ground to be found, which satisfies both the objectives of maximizing security and minimizing the emerging threat to Human Rights while using surveillance. With unprecedented security attacks decreasing significantly ever since stronger surveillance was implemented and with one of the United Nations' main objectives being to “keep peace throughout the world”, it can be confirmed that the use of surveillance cannot be retracted. Universal surveillance disapproval would only lead to the establishment of unsafe anarchist societies where moderation would be eradicated, and crime and radicalization would thrive. The international community now ought to figure out how to make surveillance more ethical, as it is extremely successful in maintaining national and international security.

Definition of key terms

Surveillance

“Surveillance is the careful watching of someone, especially by an organization such as the police or the army.” [1]

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.” [2] Covert surveillance can be practiced using many different surveillance methods, namely mobile, foot, static, and technical surveillance. Equipment examples of the abovementioned include digital camera systems, location tracking apparatus, and eavesdropping device detectors.

Overt Surveillance

“Overt surveillance involves surveillance monitoring equipment that is intentionally placed so it is highly visible, fitted in plain view to deter criminal activity, provide a sense of security and give people or businesses peace of mind. If the worst happens and a crime is committed, video footage of the act can be used as evidence because when a criminal’s face is on camera, it is very hard to disprove wrongdoing.” [3]

[1] “Surveillance Definition and Meaning I Collins English Dictionary.” *Collins Dictionaries*, 2021, www.collinsdictionary.com/dictionary/english/surveillance.

[2] Military Intelligence, Section 5. “Covert Surveillance.” *MI5 - The Security Service*, 3 Mar. 2016, www.mi5.gov.uk/covert-surveillance.

[3] EV Investigations. “Overt Surveillance • Eagle View • Corporate Crime, Insurance Fraud.” *Eagle View*, 9 Apr. 2020, www.evinvestigations.com/services/detection/overt-surveillance.

Mass Surveillance

"Mass surveillance uses systems or technologies that collect, analyze, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing. Under currently available forms of mass surveillance, governments can capture virtually all aspects of our lives." [4] Mass Surveillance methods and technologies applied by governments include the tracking of citizens' movements using the Global Position System (GPS), email scanning and mobile phone tapping, etc.

Surveillance Capitalism

Surveillance Capitalism constitutes a surfacing variant of an economic and political system where capital goods belong to private individuals or enterprises. It promotes the processing of people's general data by web providers offering them free services so as to lure them in a vicious consumeristic cycle and consequently make profit. For instance, Google processes location data to offer personalized suggestions that are relevant to its users. [5]

Video Surveillance

"A system of monitoring activity in an area or building using a television system in which signals are transmitted from a television camera to the receivers by cables or telephone links forming a closed circuit" [6]

Closed Circuit Television (CCTV)

"Commonly known as video surveillance. "Closed-circuit" means broadcasts are usually transmitted to a limited (closed) number of monitors, unlike "regular" TV, which

[4] "Mass Surveillance | Privacy International." *Privacy International*, 24 Aug. 2020, privacyinternational.org/learn/mass-surveillance.

[5] "'The Goal Is to Automate Us': Welcome to the Age of Surveillance Capitalism." *The Guardian*, Guardian News and Media, 20 Jan. 2019, www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

[6] "Video Surveillance Definition and Meaning: Collins English Dictionary." *Video Surveillance Definition and Meaning | Collins English Dictionary*, HarperCollins Publishers Ltd, www.collinsdictionary.com/dictionary/english/video-surveillance.

is broadcast to the public at large. CCTV networks are commonly used to detect and deter criminal activities, and record traffic infractions, but they have other uses.” [7]

Biometrics

“The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.” [8] Biometrics is not a type of surveillance, but rather a tool for practicing surveillance.

Countersurveillance

Countersurveillance refers to premeditated measures taken by the public to deter the practice of surveillance – either that is overt or covert. Examples include the installation of a firewall in a computer system to prevent unauthorized access to a network and the use of cell phone jammers to disrupt communication in instances where one suspects they are being recorded.

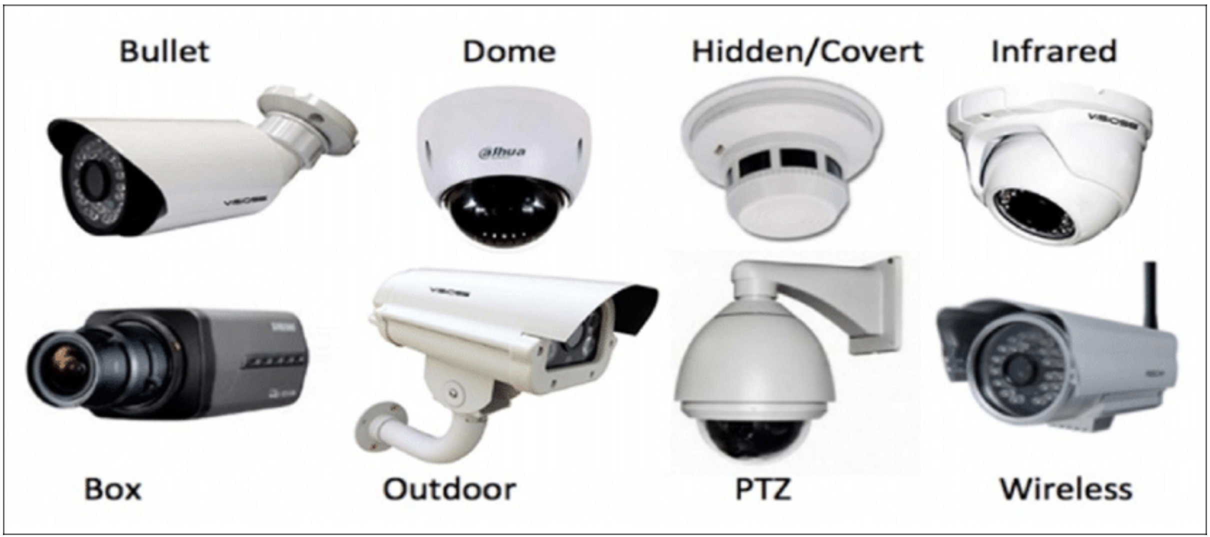

Figure 1: Different types of CCTV cameras [9]

[7] Paessler AG. “What Is CCTV? Definition and Details.” *Paessler*, 24 Apr. 2020, www.paessler.com/it-explained/cctv.

[8] “Biometrics.” *The Merriam-Webster.Com Dictionary*, www.merriam-webster.com/dictionary/biometrics.

[9] Gupta, Parul & Margam, Madhusudhan. (2017). Use of Multifaceted Electronic Security Systems in a Library Environment. Journal of Knowledge & Communication Management. 7. 116. 10.5958/2277-7946.2017.00010.9.

Background Information

Being watched has always been followed by a negative stigma. Yet when installed moderately, surveillance can also help keep people safe. Moderation is, however, slenderly separated from reaching the unsettling extreme, and this line has been crossed by many governments worldwide.

Historical Background

The Genesis of Surveillance

Primary surveillance technologies are strictly categorized as physical surveillance as they precede the creation of the World Wide Web (WWW) and its publicly available services. Social engineering, a manipulative means of collecting confidential or private information from individuals, has been argued to classify as a practice deriving from mischievous human nature. It is inherently indeterminate historically, and therefore, so is surveillance since the former is a monitoring technique. After the industrial revolution, social engineering was embedded in telephone surveillance in the form of pretexting. Pretexting enables the surveillant to create a fictional backstory or impersonate an individual or organization representee in order to phish information from someone. A common pretexting example is when someone calls an employee and pretends to be the CEO of the company at which they work at to collect confidential information from the victim.

Another early yet persistently contemporary telephone surveillance method is cell phone tapping. Known by many yet feared by few due to plausible deniability, it refers to unauthorized access to one's phone, usually to eavesdrop conversations. It is performed by bypassing the safety and security protocols built into the respective device or by physically accessing the phone lines of a home/business.

Alongside the availability of the GPS service to the general public in 1983, a new threat to privacy arose, namely location tracking. Equipped with receivers communicating with satellites, smartphones have paved the way for the easier detection of a pinpoint location, especially since most people nowadays always carry a phone everywhere they go.

Dating back to the beginning of the 20th century, audio surveillance is one of the eldest forms of surveillance. It contemporarily includes the recording and storage of audio files and has recently turned into an identification tool with the help of AI software which compares recordings with target voice samples.

Following the invention of the abovementioned came video surveillance. Surveillance was upgraded from both a national and international perspective, with Closed Circuit Television (CCTV) and Videocassette Recorders (VCRs) being the leading technologies of the late 20th century.

The Effect of Terrorist Attacks on Surveillance

The attacks on the World Trade Center (in New York City, United States) that took place on 11 September 2001 were catalytic in commencing the fight against terrorism. A setback in people's rights and freedoms could not be avoided, as the protection of national and international security had to prevail. It was not only the United States that started implementing coercive legislation, but also many other democratic nations. The urge to strengthen the precautions taken grew even larger around 2015, following the numerous terrorist attacks attributed to the Islamic State of Iraq and Syria (ISIS). The enactment of stricter laws came to threaten the right to privacy and the freedoms of expression and association by allowing intelligence agencies to monitor citizens solely under the suspicion that they are affiliated with a terrorist group.

Figure 2: Aftermath of the September 11th attacks [10]

Technical Background

Computer and Network Surveillance

Computer surveillance typically involves the monitoring of information and internet traffic. Present-day surveillance includes many computer surveillance techniques, especially in Constitutions lacking democratic values. For example, in the US, internet traffic is disposable for real-time monitoring by Federal law enforcement agencies thanks to the Communications Assistance for Law Enforcement Act. Since manual scanning of the web would be practically impossible due to the internet's vastness, surveillants have resorted to the creation of automated systems. Online surveillance computers filter information out of the internet by using certain "trigger" keywords or phrases like the ones used in the trade and sale of narcotics and weapons, monitoring certain types of online services, or chatting with suspicious people. Personal computers also constitute surveillance targets since they store

[10] Sze, Kristen. "'It Feels like It Was Yesterday': Survivor of 9/11 Terrorist Attacks Shares His Harrowing Escape from 105th Floor of the World Trade Center." *ABC7 San Francisco*, KGO-TV, 11 Sept. 2020, www.abc7news.com/911-survivor-sept-11-never-forgotten-remembering-pictures/6419324/.

personal information, such as identification card numbers, medical data, and credit card information. Examples of computer networks include TEMPEST, a form of computer surveillance involving reading electromagnetic signals from devices for the extraction of information, and a database created by the NSA called "Pinwale" that enables the reviewing and storing of email content.

Network surveillance, closely related to computer surveillance, refers to the monitoring of computer activity within a network. It usually takes place covertly, in a manner that is automatic and intrusive. Intrusive technologies secretly implant malicious software (often called spyware) in mobile phones or computers and allow outside operators to assert complete control and/or monitoring of the target's device. These technologies can be characterized as some of the most invasive surveillance methods to exist. Network surveillance can also be used for setting a limit on the access to information available to the public or to specific user-groups. Helpful in monitoring different circumvention techniques such as filtering, blocking, and bypassing and intercepting network traffic, it can provide a comprehensive analysis about the overall status of protocol monitoring and the health of a network.

Biometrics

Biometrics systems are used to identify or verify the identity of individuals by analyzing their inherent physical or behavioral characteristics. Identifiers include fingerprints, iris, face and palm prints, gait, voice, and DNA. Gathered to create biometric databases for governments to consult, they can help in border security, employment verification, the identification of criminals and the fight against terrorism. Private companies have argued that biometrics are able to enhance daily life by helping identify people with greater ease and by permitting access to places, products, and services more easily and securely as biometric identifiers cannot be replicated (with some exceptions).

Criminal Activity and Surveillance

Solving Crime

Surveillance cameras can provide authorities with footage helpful in identifying criminals and ultimately help solve criminal cases. Getting away with wrongdoing is turning increasingly impossible as AI systems can now identify people wearing headgear that covers facial features. Urban and rural safety increases while crime rates go down.

Deterring Crime

Other than satisfying the objective of identifying criminals, CCTV systems installed in public locations can also help prevent crime. Even through a clear verdict on whether cameras can deter crime only came recently, a 2019 study in Montevideo, Uruguay, found that crime was reduced by 20% in cities where cameras were installed. Not only that, but there was no crime displacement either [11]. The mentioned data is

[11] Munyo, Ignacio, and Martín Rossi. "Police-Monitored Cameras and Crime." *VOX, CEPR Policy Portal*, 30 June 2019, www.voxeu.org/article/police-monitored-cameras-and-crime.

on reported crime, therefore, what can be concluded is that the installation of cameras decreases the willingness to commit crimes.

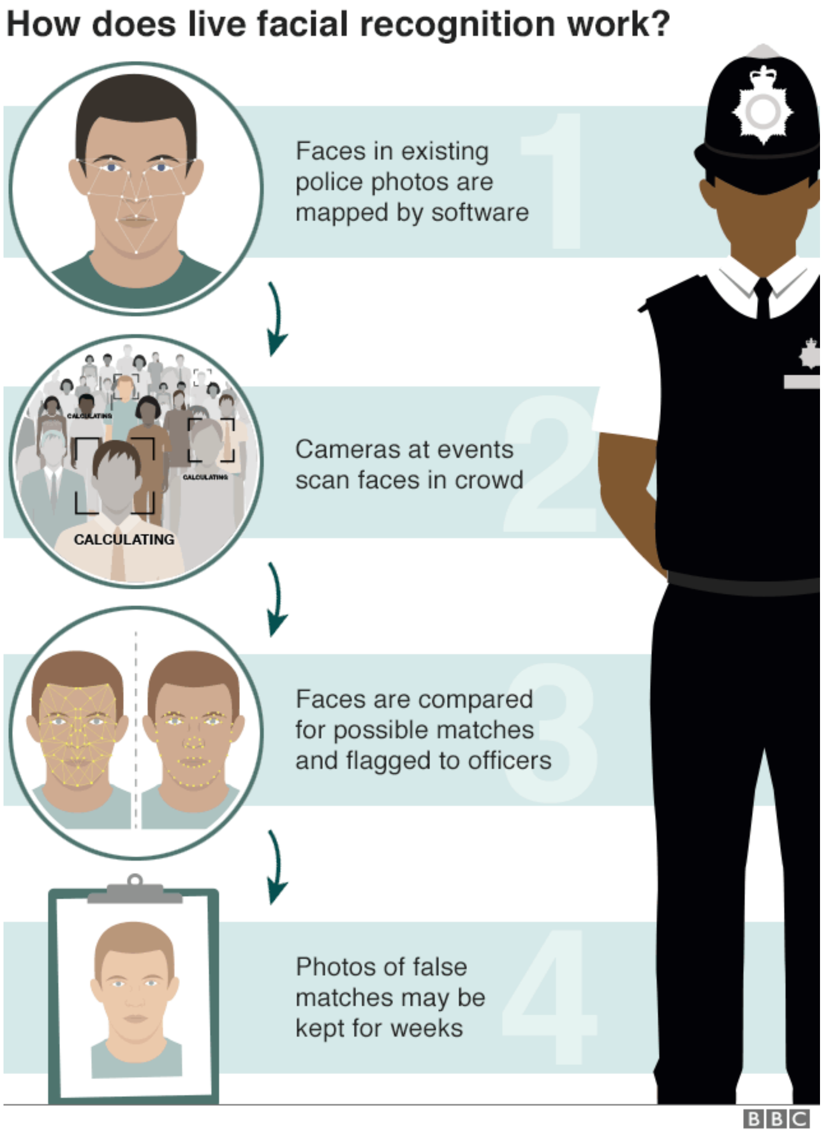
How does live facial recognition work?
1
Faces in existing police photos are mapped by software
CALCULATING
2
Cameras at events scan faces in crowd
3
Faces are compared for possible matches and flagged to officers
4
Photos of false matches may be kept for weeks
BBC

Figure 3: Live Facial Recognition Technologies Explained [12]

The Right to a Private Life

A common misconception swarming privacy and surveillance is that they cannot coexist and at the same time serve to protect the purpose of one another. Even though it is no rare occurrence for surveillance to be used in a manner that threatens

[12] "Facial Recognition Identifies People Wearing Masks." *BBC News*, BBC, 7 Jan. 2021, www.bbc.com/news/technology-55573802.

privacy, examples of the opposite persist. Surveillance can provide protection for the dependent (e.g., children and the impaired) and those who like enjoying industrial safety and the right to liberty and security, as well as help preserve democracy in pluralistic societies. However, the avoidance of authoritarianism is instrumental in achieving all the aforementioned. As soon as democracy is breached, so is the right to privacy and the freedom of association and speech. The problem grows bigger when the viewpoint is shifted from overt to covert surveillance. Covert surveillance, when practiced for an invalid reason, constitutes a criminal offense under most national legal systems. For example, in environments such as the workplace, the use of covert surveillance is deemed acceptable as it works to maintain needed control. Yet, how can unjust government surveillance be prevented? It is likely that countries with authoritarian regimes covertly surveil the public but cannot be entirely confirmed due to the lack of transparency and intel. Despite that, the existence of a few confirmed cases calls for democratic action to be taken in order to safeguard Human Rights.

Freedom of Association

Freedom of association constitutes a fundamental right every human is entitled to enjoy. It describes the right of every individual to organize or participate in groups no matter the formality of their intentions. The freedom appertains to professional organizations such as political parties, trade unions, public associations, and NGOs with employees. It simultaneously covers volunteer-based organizations as well as entities with or without a legal representative. Whenever a government commits wrongdoing, assembled protests are reasonably incited to express discordance. The succeeding response of the states contemporarily includes the deployment of technology, primarily in the form of enabled surveillance. It has previously been claimed that the sole motivation behind these actions is to maintain security and public order, yet everyone remains unconvinced. Protests are surveilled before, during, and after their execution for the collection of information and data from public and private spaces, with no regard of whether the participants are eligible to be convicted of an offense. This surveillance is carried out covertly for the most part as no official consent of those surveilled is given. It is possible that online authorities monitor social media communications and collect any relevant information secretly. Their techniques involve pretexting, confidential collaboration with social media platforms and movement-tracking applications, and hacking. Governments equip cities with fake mobile phone towers, facial recognition sentiment software, and military-grade drones supplied with technologies to ensure the complete absence of anonymity during protests.

Freedom of Speech

Ever since the commencement of the Digital Era, the public has been compelled to implement internet usage into its daily routine. The web has been turned into fertile land for opinions to be sprouted, upgrading our freedom to expression. This post-industrial advancement, however, ignited governmental backfire. Governments seek citizen approval to maintain national peace and to appear cleared of any possible wrongdoing. Whenever an individual talks unfavorably of a government or exposes any amongst its questionable actions, they become an immediate target. The problem comes to threaten journalists even more, whose job oftentimes deems them obliged to cover controversial topics. For example, FinFisher (also known as FinSpy), British surveillance software sold to governments solely for criminal investigations, has been used to monitor journalists and dissidents in countries where the rule of law is not very strong.

Major countries and organizations involved

United States of America (USA)

The Fourth Amendment to the United States constitution reads: “The right of the 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 seized" [13]. Introduced in Congress in 1789, Amendment IV and its provisions are not obeyed thoroughly and holistically. The Member Agencies of the US Intelligence Community (IC), responsible for providing national security intelligence to senior US policymakers, frequently bypass the scope of their competences. The National Security Agency (NSA) has been exposed for breaching people's privacy and is infamous for its Human Rights violations. The volume of the NSA's power is colossal, as it has seized direct access to data from Google, Facebook, and Apple, all of which have huge databases storing the personal data of billions. United States law does not recognize a privacy interest unless that is in the contents of the communications between its people; metadata, including the electronic details of online communications, our search history, and transportation record, are at the disposal of the NSA to analyze.

Augmenting universal concern, the NSA has stated that a mere collection of personal data does not count as a privacy breach, and that violations can only take place when data is examined. Moreover, contrary to rational expectation, the United States law on privacy is not contained within its territories yet has scarily come to affect non-Americans that live outside the country. For example, an infamous incident of the NSA surveilling people other than its own, is that of German Chancellor Angela Merkel getting her mobile phone tapped.

The NSA, however, is not alone in its intelligence operations – the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) are on the run too. The FBI has requested information from data troves containing Americans' email and other communications without proper justification, while the CIA has used smart devices to spy on citizens. The United States, having adopted a mainly capitalistic economic and political model, have managed to occupy a position amongst the major surveillance equipment exporters.

[13] "U.S. Constitution - Fourth Amendment: Resources: Constitution Annotated: Congress.gov: Library of Congress." *Constitution Annotated*, www.constitution.congress.gov/constitution/amendment-4/#:~:text=The%20right%20of%20the%20people,and%20the%20persons%20or%20things.

People’s Republic of China (PRC)

Evidently and provably housing some of the most surveilled cities around the world while implementing concerningly violating measures and techniques, China has contributed to its own internal corruption. Security cameras and facial recognition software are steadily increasing in number. In fact, the media mouthpiece of China’s ruling Communist Party posted a tweet claiming that the Chinese government is capable of scanning the faces of the country’s 1.4 billion citizens in just one second. Having roughly one camera for every six of its 30 million residents, it has established an expansive and pervasive surveillance network.

The implemented facial recognition systems are capable of instantly identifying people’s ethnicities and party membership. Biometric data has been weaponized against Uyghurs, a Turkic ethnic minority group mostly living in Xinjiang and currently suffering a modern genocide, as well as others suspected of disloyalty. The creation of independent Chinese media platforms, other than satisfying national media censorship objectives, allows for the uncomplicated monitoring of the population’s internet activity.

Increasing anticipated fear, China created a “social credit” system back in 2014 which ranks citizens and punishes them with slowed-down internet and flight bans if the Communist Party observes behavior that is deemed rather untrustworthy and disloyal. The social credit system is based on a series of criteria revolving around the demonstration of morals. Standing at the top of the list of the biggest surveillance technology suppliers, it has managed to make privacy a human privilege rather than a right for its people.

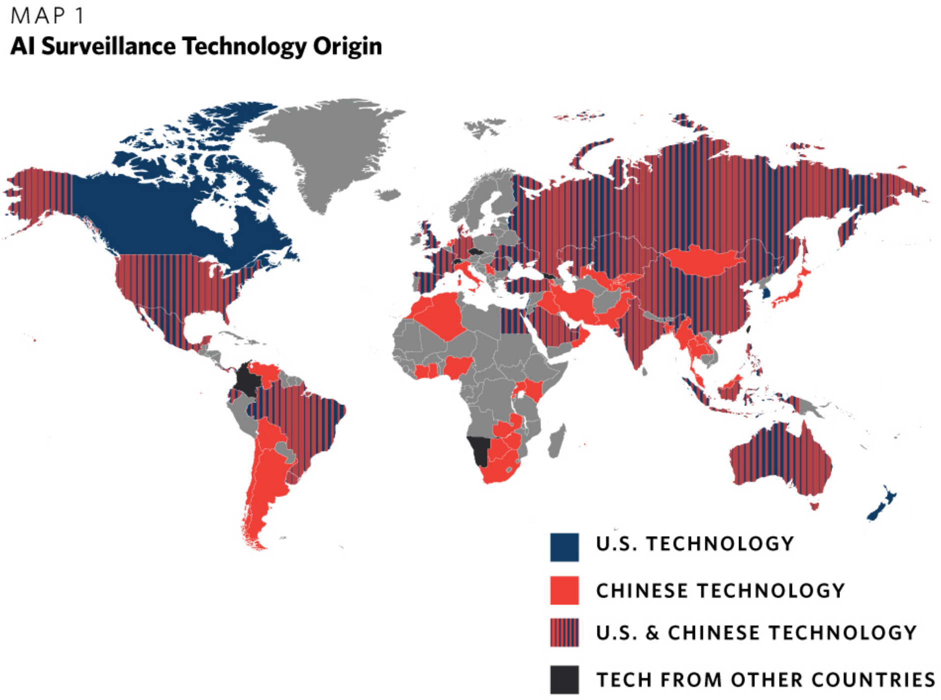
MAP 1
AI Surveillance Technology Origin
U.S. TECHNOLOGY
CHINESE TECHNOLOGY
U.S. & CHINESE TECHNOLOGY
TECH FROM OTHER COUNTRIES

Figure 4 : AI Surveillance Technology Origin [14]

The State of Israel

According to data, Israeli software company NSO (Niv, Shalev and Omri – the names of the founders) Group has sold spyware to authoritarian regimes for the goal of targeting activists, politicians, and journalists. Named “Pegasus”, the NSO’s hacking spyware is malicious and can infect both iPhones and Androids to enable operators

[14] Feldstein, Steven. “The Global Expansion of AI Surveillance.” *Carnegie Endowment for International Peace*, 17 Sept. 2019, www.carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

that allow for the extraction of messages, photos and emails, the recording of calls, and the secret activation of the microphone. A leaked list of more than 50,000 phone numbers is believed to contain information belonging to people of interest to NSO clients since 2016. Even though the existence of this data cannot verifiably reveal whether all these devices where infected by Pegasus or subject to an attempted hack, it is indicative of the volume of the NSO's targets altogether.

The Republic of Rwanda

Rwanda is built on 2 contradicting narratives; a glorious example of African development – especially when it comes to technological advancements – and a hierarchical – almost authoritarian – radicalized Patriotic Front. The Rwandan Patriotic Front (RPF) has claimed power ever since the 1994 genocide and has continuously been on the lookout for more authority ever since. The government prohibits people and the media from voicing any opinions, and has started monitoring the public through cyber-surveillance, threats, and violence. Recent installation of CCTV cameras throughout the capital's neighborhoods comprises one amongst the RPF's many mass surveillance initiatives. Dissidents have been targets of high priority and victims of deploying technology; this has been affirmed by the government's possession of the former's private communications from mobile chat applications. Rwandan authorities were recently exposed for using NSO Group's "Pegasus" spyware to likely target more than 3,500 individuals, including journalists and politicians. With democratic values steadily vanishing and the RPF's thirst for more power incessantly growing, freedom of association and speech have turned into a proper luxury for the country's people.

North Atlantic Treaty Organization (NATO)

The North Atlantic Treaty Organization (NATO) is a military alliance established on 4 April 1949 by the North Atlantic Treaty. It currently counts 30 Member States from North America and Europe and was created for the purpose of counterweighing the Soviet armies installed in central and eastern Europe after World War II. During February of 2021, NATO was processing the acquisition of the Alliance Ground

Surveillance (AGS) system. NATO AGS is a remotely piloted ground surveillance system feeding information to NATO commanders. It is owned by all allies, each of whom has direct access to both data and reports, ultimately strengthening NATO's capacity to gather and share intelligence. This high-altitude, long endurance (HALE) aircraft serves to protect ground troops and civilian populations, maintain border control and maritime safety, strengthen the fight against terrorism, help manage crises, and provide humanitarian aid during natural disasters. It works by using advanced radar sensors to continuously detect and track moving objects within areas of interest and finally provide imagery. Moreover, NATO has established a Joint Intelligence, Surveillance and Reconnaissance (JISR) system that provides the foundation for all military operations. It also provides information and intelligence access to key-decision makers in order to help them make the correct choices. It includes both virtual and electronic observation and can indicatively allow for the covert watching of Unmanned Aircraft Systems (UAS) with cameras.

Amnesty International

Amnesty International is a nongovernmental organization founded in London on 28 May 1961 by a British lawyer and human rights activist. With more than 10 million members, it strives to put an end to human rights crises around the world. Reputable for shedding light on violations made by governments, it has not let the privacy hazards imposed by surveillance go unreported. With a heavier focus on the United Kingdom and European Union, it condemns governments for their violating initiatives and exposes their tactics. Recently, during June 2021, Amnesty and another approximate 170 organizations called for a full ban on the use of biometrics for surveillance purposes. Starting petitions and organizing protests, Amnesty advocates for the release of extradited journalists sentenced to prison after unfair trials and has categorized the contemporary precariousness of the freedom of speech as an immense global threat to human values. Having been surveilled by the UK government, it also provides its members with tips on how to protect Human Rights online and informs citizens about what is to come in terms of surveillance evolution.

Timeline of events

1906	New Yorker Kelley M. Turner invents the “Dictograph”, an electric eavesdropping device of very high sound sensitivity. Ultimately playing a role in criminal prosecutions, it was used by both the police and private investigators.
1927	Russian scientist Léon Theremin invents a wireless system that can broadcast video camera footage on a television. This is later used to watch those visiting the Kremlin in Moscow.
1942	Nazi Germany’s Siemens AG builds a new CCTV system for the airfield at Peenemunde to monitor the launch of V-2 rockets. The system is primarily engineered by Walter Bruch, a field specialist, to ensure that everyone keeps a safe distance from the sight.
1950	CCTV technologies start being introduced to the world of commerce and are no longer only available the military.
1971	The global surveillance network – code-named “ECHELON” – is created after the UKUSA agreement was successfully enacted by both countries.
1972	Videocassette Recorders (VCRs) are invented and make video recording a lot easier – old video footage can be recorded over, and tapes are able to be switched out quickly. A lot of businesses start adopting security cameras.
1976	The first speech recognition device is prototyped.
1996	Axis Neteye 200, the first ever Internet Protocol (IP) camera, is invented. Remote video access is now available and accessible – no matter where one may be.
9 September 2001	Four consecutive terrorist attacks on the World Trade Center take place. A total of 2,977 people is killed and an approximate 6,000 suffers injuries. Atonement calls for stronger surveillance implementation. [15]

September 2007	The NSA, US' wiretapping agency, began user data monitoring going in and out of Microsoft under a project called "Prism".
2008	The finalization of finger image and facial quality measurement algorithms permits governmental coordination of biometric database use by the US.
25 May 2018	The European Parliament and the Council of the European Union implement the General Data Protection Regulation (GDPR).

Previous attempts to solve the issue

Anti-surveillance Movements

The "Stop Watching Us" Protest (Electronic Frontier Foundation)

On the 12th anniversary of the signing of the US Patriot Act, on the 26th of October 2013, thousands gathered on the steps of the Capitol to protest the NSA's surveillance initiatives. The message they wanted the Congress to receive was the following: "Stop Watching Us", hence the naming of the protest. The protest saw a change to reform the NSA, yet no change took place in the long run. [16]

The Surveillance Technology Oversight Project (STOP)

The Surveillance Technology Oversight Project (STOP) is a non-profit advocacy organization based in New York that aims to balance privacy and security at both a local and state level. Its goal is to transform New York into a surveillance moderacy example for the rest of the nation to follow. [17]

[15] "September 11 Terror Attacks Fast Facts." *CNN*, Cable News Network, 3 Sept. 2021, www.edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/index.html.
[16] "Stop Watching Us: Rally Against Mass Surveillance." *StopWatching.us*, www.rally.stopwatching.us/.
[17] *S.T.O.P. - The Surveillance Technology Oversight Project*, www.stopspying.org/.

Legislative Changes

The Overhauling of White House Surveillance Laws

During the first elapsed months of 2020, the US White House reached a deal to alter surveillance laws for them to not constitute such a big threat to privacy. The introduction of the bill was a true breakthrough, but not up to par with libertarian expectations. Changes would include the addition of a skeptical voice to secret court deliberations when the FBI wants to eavesdrop on Americans and the expansion of criminal penalties issues surrounding the use of the Foreign Intelligence Surveillance Act (FISA). However, the plan was eventually abandoned, as it fell victim to tweets by Donald J. Trump, opposition from the Justice Department and the collapse of a fragile temporary alliance among liberals, moderates, and conservatives.

Security Augmentation

The Patriot Act

The Patriot Act was passed by Congress and later endorsed in law by President George W. Bush in October 2001 as a direct result of the 9/11 attacks. Amending a preexisting law, the FISA, it expanded national security surveillance and introduced an array of institutional changes, such as improving coordination between government agencies. Some elements of the law were intended to resolve the sorts of problems that came before the September 11 attacks, while the creation of others was simply rooted by the executive branch's long-standing desire to increase surveillance powers. More specifically, its purpose was to deter and punish terrorist acts within and outside the country. The Patriot Act was passed by the Congress with little debate and slight scrutiny of some of the bill's problematic provisions. Yet even after 9/11, hundreds of Americans and people living within the US have been charged with jihadist terrorism or related crimes, especially during the peak of ISIS' influence, so the Act better worked as an excuse to turn regular citizens into suspects.

French Counterterrorism Bill Boosting Surveillance of Extremist Websites

On 28 March 2021, the French government announced a new counterterrorism and intelligence bill that will help in preventing attacks, especially via stronger surveillance of extremist websites. The bill was introduced just days after a French police officer was killed inside a police station in which a terrorist attack was being investigated. French Interior Minister Gerald Darmanin said the text will make French intelligence services' power to watch people's online activities stronger as extremists are "are using less and less phone lines and more and more internet connections". The efficacy of the initiative cannot be confirmed at such early stages of its application, yet past French countersurveillance and security laws have evidently been successful in thwarting attacks.

Relevant UN Resolutions, Events, Treaties and Legislation

Universal Declaration of Human Rights

The Universal Declaration on Human Rights (UDHR) is an international document adopted by the UN General Assembly on 10 December 1948 which announces 30 rights and freedoms of every citizen. Article 12 of the UDHR explicitly states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [18]

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral UN Treaty entered into force on 23 March 1976, in accordance with Article 49 of the UN Charter. Its adoption aims to preserve the integrity and equal enjoyment

[18] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf.

of civil and political rights within the territories of the Signatory States. Article 17 of the ICCPR is alike Article 12 of the UDHR. [19]

UN General Assembly Resolution on the Right to Privacy in the Digital Age

The Resolution on the Right to Privacy in the Digital Age was adopted at the 73rd session of the UN General Assembly. The council's remarks included the recognition of the importance the right to privacy bears in preventing gender-based violence, abuse and sexual harassment, cyber-bullying, and cyberstalking, especially against the female gender and minors. Relevant are Clauses 6, 9 and 14. [20]

UN Human Rights Council Resolution on the promotion, protection and enjoyment of human rights on the Internet

The Resolution on the promotion, protection, and enjoyment of human rights on the Internet was adopted on the 32nd session of the UN Human Rights Council. During the drafting of the Resolution, the Council denounced all Human Rights violations and abuses committed against individuals enjoying their fundamental freedoms on the Internet. It also requested that all States ensure civil accountability and propose effective remedies, as they ought to, according to their international obligations. In relation to our presented topic, a Preambulatory Clause pronounces: "*Noting also the importance of building confidence and trust in the Internet, not least with regard to freedom of expression, privacy, and other human rights so that the potential of the Internet as, inter alia, an enabler for development and innovation can be realized*". [21]

[19] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf.

[20] "The Right to Privacy in the Digital Age :" *United Nations*, United Nations, 26 Sept. 2019, www.digitallibrary.un.org/record/3837297?ln=en.

[21] "The Promotion, Protection and Enjoyment of Human Rights on the Internet :" *United Nations*, United Nations, 5 July 2018, www.digitallibrary.un.org/record/1639840?ln=en.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a legal framework that regulates the collection and processing of personal information belonging to citizens of the European Union (EU). Besides aiming to safeguard our data upon web usage, it also looks to introduce profit and benefit from the digital economy by both citizens and enterprises. Under the terms of GDPR, organizations are obliged to ensure that data gathering takes place legally and remains under strict conditions. Whoever collects and manages data ought to take measures that prohibit its misuse and exploitation as well as respect the rights of the data owners. [22]

Possible solutions

Multilateral and unilateral cooperation

Intergovernmental transparency and communication could help mend relations between unallied countries and discourage the execution of targeted attacks. Similarly, governmental transparency could erase surfaced concerns on the topics of privacy and liberty as well as augment civil trust. A working means of satisfying the aforementioned would be the implementation of Open Government Data (OGD). OGD enables the availability of governmental data to all, promoting transparency, accountability, and the creation of values through a set of policies.

Civilian-led monitoring

Civilian-led monitoring enables the public to monitor and record violations of International Humanitarian Law and Human Rights. With the help of internet services, the reporting of cases could be performed easily and securely. This way, civilians not intending to carry out any unlawful actions could be spared of feeling their privacy has been violated by the government. However, such an initiative would call for the establishment of stronger and more reliant governmental bodies capable of and willing

[22] General Data Protection Regulation (GDPR). 2018. *General Data Protection Regulation (GDPR) – Final text neatly arranged*. [online] Available at: <https://gdpr-info.eu/> [Accessed 9 May 2018].

to cooperate with the public. The processing of requests would have to be carried out with ease and speed to not only combat security threats, but also work for their prevention.

Legislation

Law-making is a predominantly successful way to resolve contemporary problems. Restricting and limiting the practicing of surveillance could tame the public's fiery response on the implementation of violating monitoring systems. Remembering that surveillance is highly profitable is essential, as the return to unmonitored cities would simply be catastrophic. Introduced legislation should be working to balance surveillance and security, so setting a limit on governmental authority would both eradicate unanimous concern and ensure the preservation of security.

Bibliography

Cornell Law School. "Surveillance." *LII / Legal Information Institute*, 4 Sept. 2009, www.law.cornell.edu/wex/surveillance.

"The Global Surveillance Industry." *Privacy International*, 16 Feb. 2018, www.privacyinternational.org/explainer/1632/global-surveillance-industry.

Britannica, The Editors of Encyclopaedia. "Security and protection system". *Encyclopedia Britannica*, 17 Aug. 2012, https://www.britannica.com/technology/security-and-protection-system.

Guariglia, Matthew, et al. "Surveillance Technologies." *Electronic Frontier Foundation*, 5 Mar. 2012, www.eff.org/issues/mass-surveillance-technologies.

Hvistendahl, Mara. "How China Surveils the World." *MIT Technology Review*, MIT Technology Review, 12 July 2021, www.technologyreview.com/2020/08/19/1006455/gtcom-samantha-hoffman-tiktok/.

Lutkevich, Ben. "What Is a Firewall and Why Do I Need One?" *SearchSecurity*, TechTarget, 10 Apr. 2020, searchsecurity.techtarget.com/definition/firewall.

Techopedia. “What Is a Cell Phone Jammer? - Definition from Techopedia.” *Techopedia.com*, Techopedia, 3 Nov. 2016, www.techopedia.com/definition/14888/cell-phone-jammer.

“What Are the Different Methods of Counter Surveillance?” *Esoteric Ltd*, 25 Jan. 2021, www.esotericltd.com/2020/09/11/what-are-the-different-methods-of-countersurveillance/.

“UNGA Adopts the Right to Privacy in the Digital Age.” *UNGA Adopts the Right to Privacy in the Digital Age | GIP Digital Watch*, 21 Jan. 2019, https://dig.watch/updates/unga-adopts-right-privacy-digital-age.

Carlsen, John. “When Did Security Cameras Come Out?” *ASecureLife.com*, 20 Nov. 2019, www.asecurelife.com/history-of-security-cameras/.

“Surveillance & Data Analytics.” *Centers for Disease Control and Prevention*, Centers for Disease Control and Prevention, 26 Mar. 2021, www.cdc.gov/coronavirus/2019-ncov/php/surveillance-data-analytics.html.

Aguilera, Ximena, et al. “Disease Surveillance for the COVID-19 Era: Time for Bold Changes.” *DEFINE_ME*, 14 May 2021, www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)01096-5/fulltext.

“Terrorism, Surveillance and Human Rights.” *International Federation for Human Rights*, 15 Dec. 2015, www.fidh.org/en/issues/terrorism-surveillance-and-human-rights/.

Bradford, Lowell. “How Video Surveillance Technology Has Evolved - CCTV Technology.” *Surveillance*, 23 June 2020, www.surveillance-video.com/blog/a-history-of-cctv-technology-how-video-surveillance-technology-has-evolved.html/.

Cukier, Kenneth Neil. “Surveillance Is a Fact of Life, so Make Privacy a Human Right.” *The Economist*, The Economist Newspaper, 13 Dec. 2019, www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right.

“Two Sides of the Same Coin – the Right to Privacy and Freedom of Expression.” *Privacy International*, 2 Feb. 2018, www.privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression.

Marx, Gary. “Coming to Terms: The Kaleidoscope of Privacy and Surveillance.” *The Kaleidoscope of Privacy and Surveillance*, 8 July 2015, www.web.mit.edu/gtmarx/www/thekaleidoscopeof.html#refs.

“Guidance on Covert Video Surveillance in the Private Sector.” *Office of the Privacy Commissioner of Canada*, 16 Dec. 2015, www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gd_cvs_20090527/.

Anthony, Laura. “Is It Acceptable to Covertly Monitor Staff?” *People Management*, 4 Mar. 2020, www.peoplemanagement.co.uk/experts/legal/is-it-acceptable-to-covertly-monitor-staff#gref.

Lalami, Laila. “What It Feels Like to Be Watched.” *The Nation*, 25 Oct. 2019, www.thenation.com/article/archive/surveillance-muslim-technology/.

Britannica, The Editors of Encyclopaedia. "Amnesty International". *Encyclopedia Britannica*, 23 Oct. 2019, https://www.britannica.com/topic/Amnesty-International.

“Amnesty International Home.” *Home | Amnesty International*, www.amnesty.org/en/.

“What Is Civilian-Led Monitoring?” *Ceasefire*, 18 Feb. 2019, www.ceasefire.org/what-is-civilian-led-monitoring/.

Haglund, David G.. "North Atlantic Treaty Organization". *Encyclopedia Britannica*, 18 Mar. 2021, https://www.britannica.com/topic/North-Atlantic-Treaty-Organization.

“GDPR Archives.” *GDPR.eu*, 3 Oct. 2018, www.gdpr.eu/tag/gdpr/.

Clay, Daniel and Lemarchand, René. "Rwanda". *Encyclopedia Britannica*, 10 Mar. 2021, https://www.britannica.com/place/Rwanda.

Gitinywa, Louis. “The Chilling Tale of Mass Surveillance and Spying in Rwanda.” *Global Voices Advox*, 12 May 2021, www.advox.globalvoices.org/2020/08/07/the-chilling-tale-of-mass-surveillance-and-spying-in-rwanda/.

"Israel's Coronavirus Surveillance Is an Example for Others - of What Not to Do." *Privacy International*, 1 May 2020, www.privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do.

Nato. "Alliance Ground Surveillance (AGS)." *NATO*, 16 Feb. 2021, www.nato.int/cps/en/natolive/topics_48892.htm.

Matney, Lucas. "Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life." *TechCrunch*, TechCrunch, 3 Aug. 2015, www.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=AQAAAMCLpD2SlwB818PCpiCBg-Ie1Z7wHG9BmSR0BFOnWzAqBCun89zO5bzJkv-jljJxJNPmA16DuWXO8tZbEqWaTildQWenCY8VyD1vy4WpDCHFZUKZsaeH8g36WgiaypEx1oPdFyuTxL7n694L5RGMcvkQpI_Tj99aJtDmIzkwLj8Z.

Beens, Robert E.G. "Council Post: The State Of Mass Surveillance." *Forbes*, Forbes Magazine, 24 Sept. 2020, www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=124aaaf6b62d.

Ivanescu, Isabel, and Robert Carlson. "China's Paper Tiger Surveillance State." – *The Diplomat*, For The Diplomat, 30 Apr. 2021, www.thediplomat.com/2021/04/chinas-paper-tiger-surveillance-state/.

"September 11 Terror Attacks Fast Facts." *CNN*, Cable News Network, 18 Sept. 2020, www.edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/index.html.

Global, IFSEC. "Role of Cctv Cameras : Public, Privacy and Protection." *IFSEC Global I Security and Fire News and Resources*, IFSEC Global I Security and Fire News and Resources, 30 July 2021, www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/.

“Facial Recognition Identifies People Wearing Masks.” *BBC News*, BBC, 7 Jan. 2021, www.bbc.com/news/technology-55573802.

Fox, Lewis Lambert. “Avoiding Internet Surveillance: How to Protect Your Privacy.” *NordVPN*, 24 Mar. 2021, www.nordvpn.com/blog/avoid-internet-surveillance/.

Davis, Ben. “What Are the Benefits of Government Surveillance?” *Mvorganizing.org*, 1 May 2021, www.mvorganizing.org/what-are-the-benefits-of-government-surveillance/#What_are_the_benefits_of_government_surveillance.

“What Is Social Engineering? Examples & Prevention Tips.” *Webroot*, 27 Sept. 2011, www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering.

Stanley, Pat. “How to Tell If Your Cell Phone Is Tapped in 2021.” *Best Cell Phone Spy Apps*, 25 May 2021, www.bestcellphonespyapps.com/how-to-tell-if-your-cell-phone-is-tapped/.

“Foot Surveillance.” *Blast Theory*, 4 May 2017, www.blasttheory.co.uk/kidnap/surveillance/detect/foot.htm.

“Remembering 9/11: 'The Death Toll Was Too Staggering To Whisper'.” *NewYork-Presbyterian*, 5 Oct. 2020, www.healthmatters.nyp.org/remembering-9-11-the-death-toll-was-too-staggering-to-whisper/.

“Mobile Surveillance System And Nvr.” *Neousys Technology*, 5 June 2018, www.neousys-tech.com/en/discover/mobile-surveillance-system-and-nvr.

Bertagna, Patrick. “How Does a Gps Tracking System Work?” *EETimes*, 10 Oct. 2010, www.eetimes.com/how-does-a-gps-tracking-system-work/.

“Covert Surveillance Solutions throughout the UK and Overseas.” *CTR Private Investigations*, 30 Apr. 2021, www.ctrinvestigations.co.uk/services/covert-surveillance/.

“Static Surveillance.” *Insight Investigations*, 24 Dec. 2020, www.investigate.uk/surveillance/static/#:~:text=Static%20surveillance%20is%20commonly%20used,specific%20persons%20watched%20and%20followed.&text=24%20

hours%20manned%2C%20or%20electronic%2C%20surveillance%20can%20be%20maintained.

"Msa Technical Surveillance Countermeasures." *MSA Security*, 2 Mar. 2016, www.msasecurity.net/msa-technical-surveillance-countermeasures.

"Open Government Data." *OECD*, www.oecd.org/gov/digital-government/open-government-data.htm.

Kemp, Kathryn W. "'The Dictograph Hears All': An Example of Surveillance Technology in the Progressive Era." *The Journal of the Gilded Age and Progressive Era*, vol. 6, no. 4, 2007, pp. 409–430., doi:10.1017/S153778140000222X.

Edwards, Jeff. "A Brief History of Network Monitoring." *WhatsUp Gold*, Whatsupgold, 2 June 2021, www.whatsupgold.com/blog/a-brief-history-of-network-monitoring.

Mayhew, Stephen. "History of Biometrics: Biometric Update." *Biometric Update*, 20 July 2018, www.biometricupdate.com/201802/history-of-biometrics-2.

"Snmp." *Net*, 22 May 2020, www.net-snmp.org/about/history.html.

Schmidt, Kevin. "Chapter 1. Introduction to SNMP and Network Management." *O'Reilly Online Learning*, O'Reilly Media, Inc., 15 Dec. 2002, www.oreilly.com/library/view/essential-snmp-2nd/0596008406/ch01.html.

"REST APIs." *IBM*, IBM Cloud Education, 6 Apr. 2021, www.ibm.com/cloud/learn/rest-apis.

"Msa Technical Surveillance Countermeasures." *MSA Security*, 2 Mar. 2016, www.msasecurity.net/msa-technical-surveillance-countermeasures.

REST API Monitoring, 9 Sept. 2016, www.manageengine.com/products/applications_manager/rest-api-monitoring.html.

"Freedom of Association." *Human Rights House Foundation*, 13 Aug. 2019, www.humanrightshouse.org/we-stand-for/freedom-of-association/.

Siatitsa, Ilia. "Freedom of Assembly under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications." *International Review of* *the Red Cross*, 1 Mar. 2021, http://international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-913.

Prokscha, Antonio. "Russia: Journalists Covering Navalny's Imprisonment Detained." *International Press Institute*, 7 Apr. 2021, www.ipi.media/russia-journalists-covering-navalnys-imprisonment-detained/.

Kirchgaessner, Stephanie, et al. "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon." *The Guardian*, Guardian News and Media, 18 July 2021, www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

"Human Rights Council Adopts Nine Texts: Establishes Mechanism to Protect Africans and People of African Descent against Excessive Use of Force by Law Enforcement Officers, Renews Mandate on Belarus." *OHCHR*, 13 July 2021, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27306&LangID=E.

"Summary: International Covenant on Civil and Political Rights (ICCPR)." *CCLA*, 27 Oct. 2015, ccla.org/summary-international-covenant-on-civil-and-political-rights-iccpr/.

"Rwanda: Surveillance Revelations Opportunity to REFORM Legal and Encryption Environment." *ARTICLE 19*, 26 July 2021, www.article19.org/resources/rwanda-surveillance-revelations-opportunity-to-reform-legal/.

Palmer, Danny. "What Is GDPR? Everything You Need to Know about the New General Data Protection Regulations." *ZDNet*, ZDNet, 17 May 2019, www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

Arthur, Charles. "Nsa Scandal: What Data Is Being Monitored and How Does It Work?" *The Guardian*, Guardian News and Media, 7 June 2013, www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

“UKUSA Agreement Release.” *National Security Agency Central Security Service > News & Features > Declassified Documents > UKUSA*, 25 June 2010, www.nsa.gov/news-features/declassified-documents/ukusa/.

Fandos, Nicholas, and Charlie Savage. “House Reaches Deal to Overhaul Surveillance Laws.” *The New York Times*, The New York Times, 11 Mar. 2020, http://www.nytimes.com/2020/03/10/us/politics/surveillance-laws-fisa.html.

Nato. “Joint Intelligence, Surveillance and Reconnaissance.” *NATO*, 9 Oct. 2020, www.nato.int/cps/en/natohq/topics_111830.htm.

Kobie, Nicole. “The Complicated Truth about China's Social Credit System.” *WIRED UK*, 7 June 2019, www.wired.co.uk/article/china-social-credit-system-explained.

Ivanescu, Isabel, and Robert Carlson. “China's Paper TIGER Surveillance State.” *The Diplomat*, The Diplomat, 30 Apr. 2021, thediplomat.com/2021/04/chinas-paper-tiger-surveillance-state/.

Ma, Alexandra and Katie Canales. “China's 'Social Credit' System RANKS Citizens and Punishes Them with Throttled Internet Speeds and FLIGHT Bans If the Communist Party Deems Them Untrustworthy.” *Business Insider*, Business Insider, 9 May 2021, www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

Davies, Dave. “Facial Recognition and beyond: Journalist Ventures inside China's 'Surveillance State'.” *NPR*, NPR, 5 Jan. 2021, www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta.

Lang, Marissa. “CIA Uses Smart Devices to Spy on Citizens, WikiLeaks Reveals.” *GovTech*, GovTech, 30 Apr. 2021, www.govtech.com/security/cia-uses-smart-devices-to-spy-on-citizens-wikileaks-reveals.html.

“Mass Surveillance.” *Amnesty International UK*, 20 Mar. 2015, www.amnesty.org.uk/issues/mass-surveillance.

Roth, Kenneth. “The NSA's Global Threat to Free Speech.” *Human Rights Watch*, 28 Oct. 2020, www.hrw.org/news/2013/11/18/nsas-global-threat-free-speech.

“Surveillance. Types of Surveillance: Cameras, Telephones Etc.” *Word Systems*, 2 June 2016, wsystems.com/surveillance-types-of-surveillance-cameras-telephones-etc/.

“Communications Surveillance.” *Privacy International*, 8 Feb. 2018, privacyinternational.org/explainer/1309/communications-surveillance.

Laperruque Jake Laperruque Jake Laperruque is Senior Counsel with The Constitution Project at POGO., Jake. “What to Expect for the PATRIOT Act Reauthorization.” *Project On Government Oversight*, 11 Feb. 2020, www.pogo.org/analysis/2020/02/what-to-expect-for-the-patriot-act-reauthorization/.

Schwartz, Adam, et al. “Biometrics.” *Electronic Frontier Foundation*, 1 Dec. 2011, www.eff.org/issues/biometrics.

Techopedia. “What Is Network SURVEILLANCE? - Definition from Techopedia.” *Techopedia.com*, Techopedia, 1 Mar. 2016, www.techopedia.com/definition/31668/network-surveillance.

Lutkevich, Ben. “What Is a Firewall and Why Do I Need One?” *SearchSecurity*, TechTarget, 10 Apr. 2020, www.searchsecurity.techtarget.com/definition/firewall.

Wires, News. “France Unveils New COUNTERTERRORISM Bill That Boosts Surveillance of Extremist Websites.” *France 24*, France 24, 28 Apr. 2021, www.france24.com/en/europe/20210428-france-presents-counter-terrorism-bill-to-boost-surveillance-of-extremist-websites.

“Terrorism in America after 9/11.” *New America*, www.newamerica.org/international-security/reports/terrorism-in-america/terrorism-cases-2001-today.

Ellen Nakashima, Mike DeBonis. “House Effort to PASS Surveillance Overhaul Collapses after Trump Tweets and Pushback from DOJ.” *The Washington Post*, WP Company, 28 May 2020, www.washingtonpost.com/national-security/house-effort-to-pass-surveillance-overhaul-collapses-after-trump-tweets-and-pushback-from-doj/2020/05/27/a3f224f8-a047-11ea-81bb-c2f70f01034b_story.html.

"What Is Personal Data?" *European Commission - European Commission*, 27 Nov. 2019, ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

Sidell, Elle Poole. "What Does Google Do With Your Data?" *Avast*, Avast, 23 Aug. 2021, www.avast.com/c-how-google-uses-your-data.

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

Perlroth, Nicole. "Software Meant to Fight Crime Is Used to Spy on Dissidents." *The New York Times*, The New York Times, 31 Aug. 2012, www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html.

"USA Patriot Act." *Office of the Director of National Intelligence*, www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2116-usa-patriot-act.