Forum: Human Rights Council

Issue: Examining human rights implications of mass surveillance in the digital age

Student Officer: Mumu Liu

Position: President

Introduction

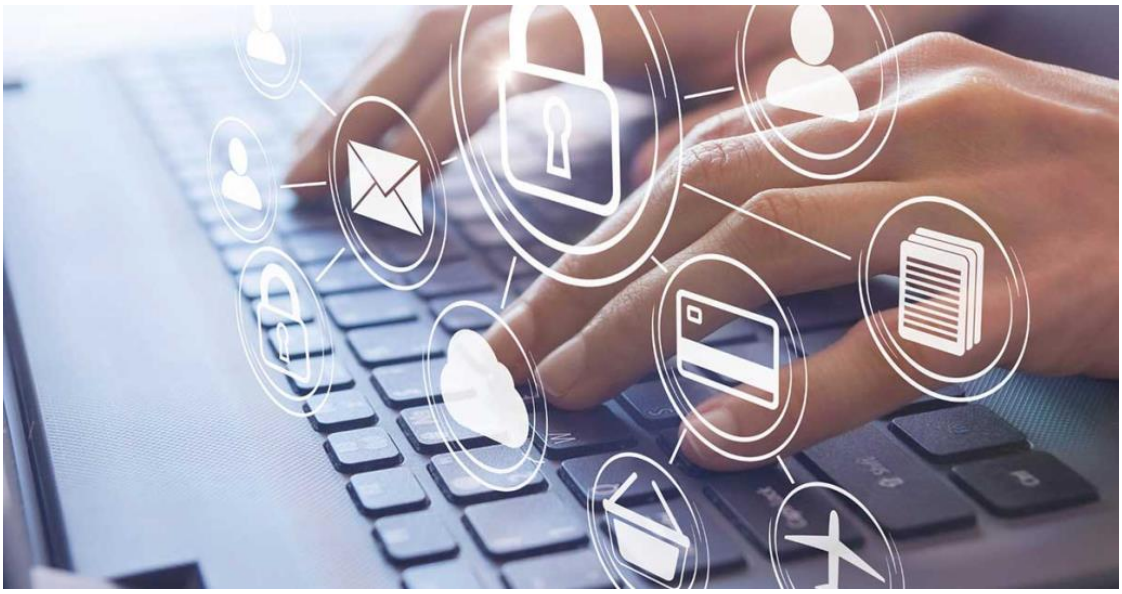

Figure 1. Cybersecurity demonstration model

Contemporarily, due to the excessive development of electronics and virtual networks, more data have become available online. While online data benefits knowledge assimilation, more monitoring technologies has been developed to further watch the safety situation of society. Nevertheless, consistent exposure of individuals has led to significant consequences as the monitoring technology has ruthlessly revealed private data from a range of Internet users without permission and consent. In addition, as the credibility of digital technology becomes more credible, disregarding their effectiveness and efficiency, the capability to track, determine, and record data from various aspects of an individual has been precedently violating norms from an ethical perspective. Currently, achievements in digital age are implicitly contributing to an ongoing mass surveillance and has become a threat to privacy.

The Acting High Commissioner for Human Rights Nada AI – Nashif proclamated in 2022 that "pervasive surveillance comes at high cost, undermining rights" (OHCHR.org). This was a specific reference toward the mismanagement information on social media platforms on the Internet, as well as the revelation of private data

from organizations. Staff reports collaborated by intergovernmental and non-governemntal organizations has been conducted in the past decades in determining the culprit of data loss during migration and measures to mitigate the impact of cyber security issues.

As of 2024, mass surveillance has negatively influenced the society in aspects such as but not limited to: ideology and perception, finance, and individual identification data; all aforementioned aspects are merely imited to intrusions with authentication from encoded users. Firms responsible for invasion preventing has adopted various protection features such as encryption and Wi – Fi Protected Access (WPA) (IB.CompSciHub.net). Despite that, the society is still currently in the stage of exploration toward methods in guaranteeing future network security to promote a hospitable, harmonious, and more united virtual environment through millions of communication links that bonds countless user interfaces on a single lane.

Definition of Key Terms

Digital Age

Humanity has entered an era where tasks are completed by electronic devices manuvered by computer, and surges of information are becoming available with more advanced data transmitting systems with extensive computer networks (Dictionary.Cambridge.org). Hence, Digital Age is simultaneously defined as Information Age. The Digital Age initiated in the post – industrial era, in the mid-20th century, after computer elites redefined previous iterations of computer models. Computers commenced advancing in the early 1970s for communication, political, and business activities (DigitalSociology.org.uk).

Mass Surveillance

Mass surveillance can subject population or significant component to indiscriminate monitoring, which involves systematic measures regarding individual privacy as well as rights to freedom of speech and protest (PrivacyInternational.org). In other words, mass surveillance refers to the great pressure or depression under the exposure of private information due to the extensive wireless and cabled network worldwide, as defined by the Office of the UN High Commissioner for Human Rights (OHCHR, OHCHR.org). In addition, in the report submitted by the aforementioned commission as requested in resolution 68/167 in July 2014, surveillance that occurs digitally can be threatening both domestically and exotically.

Networks

The Dartford Grammar School Computer Science Department defines computer network as a group of computer systems or hardware devices linked together through communication medium in facilitating communication and resource – sharing activities among a range of users. Most networks are commonly categorized based on their characteristics, and data could thus be transmitted through cabled or wireless network. Network protocols, a set of rules managing the format and sequence of data transfer, facilitates the sharing process and is a factor of publicizing private data (GCore.com).

Remote Control

Remote control is initially known as the radio-frequency devices that directed German naval vessels to crash boat from adversary side. Contemporarily, software such as TeamViewer are used to fix an error or manuever certain aspects of the client computer, and it is considered one of the key factors in mass surveillance (Electronics.HowStuffWorks.com).

Encrption

Encryption describes the process of transforming readable plaintext to ciphertext that is unreadable to external intruders when transmitting data to another server or client device, which will prevent unauthorized access from suspicious users (IBM.com). The OHCHR addresses encryption as a "key enabler of privacy and human rights in the digital space," but is currently neglected by the majority of humanity; the organization is currently calling for a halt in actions such as systematic screening of individual client devices (OHCHR.org).

Background

Reports in recent years has signaled the aftermaths of mass surveillance as our society takes continues its excursion to an unprecedented epoch with advanced electronic technology performing millions of iterations of algorithmic instructions at each second. Nevertheless, digital device is simply the fuse of mass surveillance; in fact, humanity's neglection toward the consequences of over-monitoring is further exacerbating the issue where more violations from moral and spiritual perspectives are occurring. The impact of remote observing of individuals are not inconsequential as the aftermath of digital peeping is prevalent, and distinctive, in a diverse range of fields, and that considers the action as a latent emergency situation that is applicable to all Internet users. In the section, the report will discuss the byproduct of virtual surveillance from different areas that potentially involves the question of cybersecurity universally.

Social Media Surveillance

Social Media is intentionally served as a platform for resource sharing among a range of users that involves both authorities and publics. Nevertheless, misbehaving and mismanagement of citizen behavior on the platform has been detected infrequently despite the scrupulous monitoring of governments. Specifically, distorting voices is not simply the mere element leading to the ambiguous interpretation on the advantages and disadvantages of social media; in fact, the contemporary backstage of social media operation is gradually, and subtly, shifting to a machine – driven monitoring of innocent citizens along with interfering digitally with their devices. As Freedom House, an NGO, claimed in 2024, individuals attempt to communicate and express opinions may potentially concern billions of individuals who engage themselves with social media. Furthermore, additional concerns has been raised regarding the intricate algorithm in searching for user profile details that high – level artificial intelligence (AI) is capable of (FreedomHouse.org).

Governmental Speech Monitoring

Governments of Member States have cooperated in employing elites in speech monitoring, specifically toward social media through ways such as but not limited to accounts for simulation purposes in connecting with other users and gain access to other involved networks. In countries such as Iran, approximately 42,000 volunteers are currently in – position for monitoring. Moreover, the Cyber Police website was constructed for citizens to report places with suspicious contents (FreedomHouse.org).

Global Market

According to the report published by Free House, approximately 40 out of 65 countries covered revealed with well – organized systems for social media monitoring. The governmental usage of such program are increasing in 15 reported Member States, absurdly after the anniversary of the expansion of the program. Allowing governments to justify efforts in security ensurance and limiting disinformation on social platforms. Whereas most Member States are indeed in favor of the system considering its extent and limitation, agencies in adversary countries view the social media monitoring system as crossing over the boundary between socialization and personal privacy (FreedomHouse.org).

Financial Data Loss

While mass surveillance on social media could lead to personal privacy exposure, cyber attacks toward companies with important financial database is capable of collapsing the corporation. The subsequent outcome could be failure in retrieving data, thus leading to lack of financial buttress in supporting the corporation. The consequence is that some firms are capable of attracting a wide range of audiences who are keen to purchase the newly manufactured product. However, once the service is failed, the source of income will be cut. Different measures has been taken through such as but not limited to allowing the access of database. On that, financial organizations have proposed a wide range of contentions on the doubtfulness. For instance, Australian government passed a law in 2018 where enforcements and security agencies may require for designated stakeholders (Internetsociety.org) while the Juridicary Committee of the House of Representatives conducted a report that identified and examined web portals that are latently linked directly to the database of some crucial financial firms (Judiciary.House.gov). Hence, further examinations in investing in measures to mitigate the negative impact of data loss in financial data storage systems are necessary to resolve both short – term and long – term issues.

In addition, financial reporting obligations relevant to online terrorism has been proposed. For a banks in parts of the world, customer transactions are legally monitored as a requirement and the bank must store relevant data for years. Suspicious activities has been reported to Financial Intelligence Unit, and is forwarded to security intelligence agencies (SIAs) in appropriate cases. Completed under telecommunications, personal data of customers has been monitored, as stated by the Max Planck Institute, without an urgent demand for security monitor (CSL.MPG.de). In other words, most customer's authentication codes may have been exposed and displayed in a major database, of which might have included their privacy. More significantly, access to customer data even without demand of security monitor indicate the fact that the authoritative attempts in accessing without client consents were performed, potentially anticipating for more severe surveillance incidences on user privacy.

Major Parties Involved

United States of America

The U.S. is currently engaging with various forms of online – monitoring tools such as face scanning technology, which is potentially biased based on the algorithm. The device could output the completely flawed profile if the case suddenly appears. In addition, reports revealed that limited regulation exists in the nation in resolving latent sudden emergencies. That is, the face scanning device could eventually allow hackers and phishers to invade the system; hackers may expose individual profiles and leading to subsequent mismanagement and leaking of personal identification codes (ThePioneerOnline.com).

Furthermore, the U.S. Judiciary Committee from the House of Representatives conducted a report on the effect of federal law enforcement on the financial institution's spy on the Americans. According to the report, alarming evidence of enforcements in engaging with spying online and attempts to decipher the authentication code of the private transactions of domestic consumers. The Tresury Department's Financial Crimes Enforcement Network (FinCEN), collaborating with other official organizations, discussed with financial firms for private data; the financial firms included but not limited to U.S. Bank, Barclays, and Bank of America, which are among the largest corporations in the field of finance **(**Judiciary.House.gov**)**.

In fact, the aforementioned portal is a public – private partnership led by the FBI's Office of Private Sector and the Department of Homeland Security's Office of Intelligence and Analysis and is used for identification of criminals (Judiciary.House.gov).

The Commonwealth of Australia

In 2018, the Australian parliament passed the TOLA act, which caused the government to shift forward and surpass digital data protections as well as potential significant harm to the economy along with the doubt of the capability of digital devices. Specifically, enforcements and relevant agencies may contact stakeholders for entering the database, which must have been well – encrypted. Due to the severity, the Internet Society organization sent a team of researchs in accessing the economic impact of the TOLA. According to the report, the cost of TOLA is not compensatable as approximately $AUS 1 billion are in current and forecase sales, and respondents comments revealed equal concerns as the quantitative data suggested. Due to the infamousness of TOLA, imitation from other Member States have been observed, which may escalate the currently concerning situation (InternetSociety.org).

People's Republic of China

In 2022, China adopted Dahua, the second – largest surveillance company worldwide and it is selled in markets involving more than 180 Member States. Forfront progress in technological exploration by the Chinese government and elites have been engaging with computer vision and hardware manufacturing. The usage of surveillance technologies has drastically increased since the COVID – 19 pandemic in 2020, in areas such as Health Kit and temperature check at transportation stations. Due to the GDP growth drop in 2022 to 2.8%, the

Chinese government has been proposing to collect extensive demographic data extensively to discover public demand in meeting social standards in the future (TechnologyReview.com). In addition, the nation tops the most surveillanced countries in 2022 by number of population affected (Statista.com).

Russian Federation

As of 2022, the Russian Federation contains a cache with approximately 160,000 files from its robust domestic Internet regulator. Ever since the start of invasion against Ukraine in 2022, the mass surveillance in Russia digitally was already in disadvantage. A report consisting 160,000 records from the cache's archive together allowed the crtical fact of President Putin's surveillance and privacy exposure systems that has been used in tracking adversies and suppress independent information within the furthest reach of the nation's vicinity. The Internet regular utilized by the Russian government is not merely a technical online monitoring system; it in fact includes a domestic spying system that is capable of interrupting telecommunication systems as well as a culprit of data trafficking within the vicinity of Russia. In addition, sources claimed that recent incidents of online misinformation and hacking of data internationally has occurred in occasions (NYTimes.com).

The United Kingdom

The United Kingdom has become one of the countries worldwide with most severe surveillances, especially after the introduction of Investigatory Powers Act in 2016. The controversial legislation has introduced attempts in intercepting emails and important documents that determines the accountability of firms engaging in AI; the legislation simultaneously absurdly proposed the idea of aggregating a diverse range of powers to engage in relevant activities. The establishment of the law has resulted in public outcry among a range of industries disappointed by the fact. For instance, TechUK, an industry organization has expressed their concern by alleging the latent threat that the legislation could potentially bring to technological innovation firms. Furthermore, concerns regarding the prevention of encryption and patching new vulnerabilities of computer systems arose as critics proclaimed the potential of the situation transitioning to a overseas crisis (Politico.eu). Moreover, while the Home Office has granted their aim in "protecting the country from abusers and terrorists," reports in from British Broadcasting Corporation (BBC) has shown the fact that intelligence agencies may currently access private information of countless individual devices such as listening to phone calls. In fact, the data is allegedly stated as accessible to police and emergency services (BBC.com).

Previous Attempts to Resolve the Issue

Given the scope of digital surveillance worldwide, intergovernmental organizations and NGOs, collaborating with Member States governments, as well as the UN, have been endeavoring to seek for measures in mitigating the social and ethical issues caused by mass surveillance. Most discussions of the issues are bonded to the topic of enhanced encryption and authentication on individual accounts, and more discussions surrounding mass digital surveillance has occurred following the outbreak of the COVID – 19 pandemic, where most activities are migrated online.

Resolution A/75/478/Add.2, para.89

The resolution on privacy in the digital age adopted by the UN General Assembly on 16 December 2020 has underlined the interdependence and indivisibility of privacy and fundamental ethical statements (Article19.org). While recognizing the successful proposals from previous resolutions as well as providing a broad insight on the outbreak of COVID – 19 pandemic, the resolution emphasized on the importance of protecting privacy online to respect the rights of individuals, as well as Member States governmental action in ensuring interference with privacy must be consistent with legality and necessity. In addition, the resolution highlighted the emergence of new-epoch technologies such as AI; clause number 6 stated the necessity of implementing regulations or deployment on intelligent tools in preventing its cross-boundary actions of searching in private fields such as user privacy and authentication (Documents.UN.org).

In addition, human resources such as safeguards in mitigating adverse violation of human rights such as pseudomization. Thus, the resolution would have been considered effective in the given extent. Nevertheless, despite its success in adopting by the UN, the resolution is inadequately specific in particular measures to address the phenomenon of mass surveillance. For instance, for clause 9 that encouraged the secure protection of digital communication technologies did not state the fields where encryption should have been implemented. Specifically, the resolution should have subdivided the clause by emphasizing the importance of encryption on the Internet, including social media, financial data, and user privacy.

Standards of United Nations in Ensuring Privacy (Model Protocol)

On 7 March 2024, the UN Office on Drugs and Crime (UNODC), collaborating with OHCHR, developed the “Practical Toolkit for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests.” The law attempted to enhance law enforcement agencies in digital mass surveillance and protect human rights to the maximum extent. The document included concerns regarding CCTV, aerial surveillance vehicles, facial recognition, and mobile identity intercepters; it simultaneously encouraged the full extent of prohibiting the illegal use of electronic devices immorally to spot individual privacys and attempts to violate human rights (Lordslibrary.Parliament.UK). An example included in the kit was Resolution A/HRC/55/60 released on 31 January 2024; it pointed out the fact that those under age eighteen must enjoy the right to freedom of peaceful assembly equally as adults (Documents.UN.org).

The Model Protocol is generally considered as a feasible solution that may be implemented by various Member States. Admittedly, the document has provided efforts that are arguably logical and reasonable in addressing most severe issues in regard to the topic of mass surveillance; a diverse range of clauses were mentioned specifically targeting vulnerable social groups that are potentially victims. Nevertheless, as most previous resolutions and reports suggested, lack of suggestions in enhancing the extents and refraining the limitations of the currently implemented has caused the statements to become repetitive and redundant. In fact, most resolutions published prior to A/HRC/55/60 has mostly proposed the ideas that are overlapping with the resolution. Hence, the attempts from UN organizations are in fact progressing at a pessimistically dragging speed, and must require

further development in the short – term given that phenomena such as computer virus and cyberattacks has been occurring in a range of forms, and must require more critical investigation.

Possible Solutions

As social media usage is becoming more pervasive nowadays, there must be a watch on potential misinformation or exposure of clinet privacy on social media. To address this, there are various measures that may be implemented. Initially, Member State governments could collaborate with NGOs, expertise firms, and the corporation itself in programming and data management to compile the setting of the background programs on the social media. Specifically, an intricate algorithm could be constructed to detect whether the content of the post is appropriate to share on the website. In addition, as some countries have implemented tactics such as banning the account when misinformation occurs or when the user is from a source unclear to the proofreading individuals, legislations such as financial sanction or legal consequences could have been emplaced. Alternatively, to not overuse the governmental resources, each geographical area should implement their respective reporting system. Once a distorting message is sent, the social media platform may directly transmit the detected content to the central server where authorities may receive simultaneously.

In regards to financial databases, legislations that allows the company in financial burden to receive subsidize provided by the Member State govenrments on a monthly basis. This is due to the fact that in case a corporation failure occurs, many will not be capable of retriving data and the financial lost is not compensatable. Moreover, better encryption methods could have been implemented. For instance, authentication methods such as asymmetric key may potentially serve as an encryption method to adopt as data is encrypted with a public key in a readable form while the authentication will be decrypted as private message. Another method of preventing data loss for financial databases is to implement a wireless local area network (WLAN) that initially allows for the Wi – Fi. The next step is to create a Intranet, where merely employees in charge of the organization may access the data, and in cases where the members of the organization could not return to the venue, a virtual private network (VPN) that connects to the LAN of the organization with well – encrypted data to ensure that the workers continue their efforts in updating the system.

Speaking of legislations, measures of consequences must be determined base on the severity and extent of the crisis. In addition, in contrast to governmental monitoring of crisis, an internal system on the account of each user on different social platforms may be implemented to determine the context of the text sent. The system adopted may send warnings to individuals if there is a mismanaged language or form for their initial commitment. On the other hand, cases with high – severity and the detection of continuous violation of norms on the platform may lead to the internal system to lock the account temporarily or permanently depending on the extent and effects. Apart from social media, while similar strategies must be adopted regarding financial data hacking or phishing, more NGOs engaging in security and management can be opened, locating in a wide geographical range in search for the base of such illegal corporations. For financial firms, persistent storage area can be used in cases with severe havoc on primary database, and data transmission between storages should bee completed through fast and stable transmission medium such as fiber optics that are susceptible to external interference.

Bibliography

"Cybersecurity Demonstration Model." *IB CompSciHub*, Dartford Grammar School Computer Science Department, https://ib.compscihub.net/paper-1/topic-3.

"Fiber Optics." *TechTarget*, https://www.techtarget.com/searchnetworking/definition/fiber-optics-optical-fiber.

"Office of the United Nations High Commissioner for Human Rights." *OHCHR*, https://www.ohchr.org.

"Freedom House." *FreedomHouse.org*, https://freedomhouse.org.

Judiciary Committee of the House of Representatives." *Judiciary.House.gov*, https://judiciary.house.gov.

"International Monetary Fund." *IMF*, https://www.imf.org.

"Max Planck Institute for Comparative Public Law and International Law." *CSL.MPG.de*, https://csl.mpg.de.

"New York Times." *NYTimes.com*, https://www.nytimes.com.

"BBC News." *BBC.com*, https://www.bbc.com.

“Politico Europe." *Politico.eu*, https://www.politico.eu.

"Statista." *Statista.com*, https://www.statista.com.

"Technology Review." *TechnologyReview.com*, https://www.technologyreview.com.

"Internet Society." *InternetSociety.org*, https://www.internetsociety.org.

"Lord's Library." *Lordslibrary.Parliament.UK*, https://lordslibrary.parliament.uk.

"Article 19." *Article19.org*, https://article19.org.

"Digital Sociology." *DigitalSociology.org.uk*, https://digitalsociology.org.uk.

"Privacy International." *PrivacyInternational.org*, https://privacyinternational.org.

"IBM." *IBM.com*, https://www.ibm.com.

"HowStuffWorks." *Electronics.HowStuffWorks.com*, https://electronics.howstuffworks.com.

"Cambridge Dictionary." *Dictionary.Cambridge.org*, https://dictionary.cambridge.org.

Appendix or Appendices

I. https://ib.compscihub.net/paper-1/topic-3 (IB CompSciHub)

This is a source provided by Dartford Grammar School Computer Science Department as part of a pre – college curriculum. Nevertheless, this source include a range of definition of terms that are relevant to the key principles behind the function of networks and may propose measures to mitigate the negative effects on data privacy due to the mass surveillance during the digital age.

II. https://www.techtarget.com/searchnetworking/definition/fiber-optics-optical-fiber (TechTarget)

The source provides a definition of fibre optic and its practical usage. Given its high transmission speed and security, the cabled network is considered crucial in implementing measures to prevent privacy exposure.