Forum: United Nations Third General Assembly (GA3)

Issue: Addressing the human rights implications of surveillance technology and mass data collection.

Student Officer: Dheer Nair

Position: Co-Chair

Introduction

Over the past few years, advancements in surveillance devices and big data applications have redefined the realm of global control including law enforcement, safety, and even interactions in a given community. While traditionally a power in the use of control of their citizens and national defense purposes, surveillance has spread to various aspects of modern society. Surveillance technologies that include various forms of use of face and biometric features, internet surveillance, or social media surveillance in some areas by the authorities are generally presented as tools for preserving order in society and law enforcement services. However, with technological improvement and the increased availability of many of these technologies, concerns have been raised about the possibility of compromising some key aspects of human rights, especially those of privacy, freedom of speech, and the right of people to rightfully own their personal data. Surveillance, although efficient, is a practice with a vast controversy attached to it.

In particular, during the Second World War, the British government devised some techniques of surveillance for effective communication eavesdropping, the most famous of which was breaking the code of "Enigma" in Bletchley Park's quest for intelligence information. There are instances of political surveillance in the course of the Cold War as the United States and Soviet Russia extensively practiced this method in the management and control of suspected spies, political activists, and any other such individuals who were deemed to be of any threat.

In the United States, the National Security Agency (NSA) was particularly keen on espionage and even managed to establish a vast network where they could wiretap calls, as well as, ensure that all details of citizens were kept on file which in turn came with extra fears resulting in self-censorship among the citizenry. That is to say that such examples raised difficult ethical dilemmas regarding the power of the state and the freedom of the citizens, a dilemma that has not gone away to this day.

The emergence of digital technologies and the internet in the late 20th century ushered in a new era of mass data collection. The post-9/11 era saw a great increase in surveillance practices justified under the excuse of counter-terrorism. In the United States, the USA PATRIOT Act gave government agencies the authority to collect and analyze individuals' data. It wasn't until 2013, however, that the global community came to comprehend the relationship of practices; it was the year that former NSA employee Edward Snowden disclosed much top secret information revealing pervasive surveillance activities against US citizens and other countries' officials and populations. 'Unveiling,' in this sense, the full capabilities of contemporary surveillance also provoked still unanswerable questions on visibility, responsibility, and the validity of the balance between personal space and the freedom of one's speech in the digital age.

Today, data production and AI development are evolving rapidly and surveillance and data analysis on a large scale have also developed into a greatly intrusive system. Real-time analysis is performed by algorithms and AI on data enabling patterns to be distinguished. Nowadays surveillance is limited not only to the work of secret service agencies, it is running in modern technology, particularly in smartphones and in social media.

While such technologies can be defensively regarded as adding much-needed security and convenience to the lives of people, they can also pose a threat to civil rights and liberties, as there are negative connotations associated with the collection and utilization

of personal information, such as discrimination and manipulation. It is now the adar paramount that these implications are addressed; otherwise, the trend toward social monitoring brings about the risk of countries abandoning the very concept of freedom as well as cutting their citizens' independence.

Definition of Key Terms

Surveillance Technology:

Tools and software used to monitor individuals, often capturing data from digital activities, locations, or communications.

Mass Data Collection:

The large-scale gathering and storage of information from individuals, often without explicit consent, for analysis and use by entities.

Right to Privacy:

The human right to maintain personal security and freedom from intrusion into one's private affairs.

Big Data Analytics:

The analysis of large volumes of data to identify patterns, often used to predict or influence behavior.

Biometric Data:

Data derived from unique physical or behavioral characteristics (e.g., fingerprints, facial structure).

Edward Snowden Leaks:

In 2013, Edward Snowden exposed extensive U.S. government surveillance programs, sparking global debate on privacy and government overreach.

International Covenant on Civil and Political Rights (ICCPR):

A 1966 UN treaty protecting civil rights, including the right to privacy, against unlawful interference.

Key Issues

Privacy Violations

The usage of surveillance technology has made it possible for huge volumes of personal information to be obtained, and this is usually done without the individual's authorization. Disrespect of privacy rights can be identified as a problem since the provided International Covenant on Civil and Political Rights (ICCPR) spells out clearly the right to privacy with all available means that most of the UN member states are parties to it. When people use their personal data including their communications, the data about their place and even the history of their internet search ends up in the hands of the government, nongovernmental organizations, or individual people and this is among the major causes of concern. Inevitably, this kind of practice also heightens the chances of such information to be used against the affected parties, something which can be used for other dangerous activities be them political, or other then in some cases even on economic gains.

Freedom of Expression

Surveillance practices can have a "chilling effect" on freedom of expression, leading individuals to self-censor for fear of being monitored. This is particularly concerning for journalists, activists, and human rights defenders, who may hesitate to speak openly about sensitive issues. When suppressing diverse perspectives, surveillance undermines democratic tenets. Research on communities put under constant observation

reveals that some individuals refrain from discussing specific subjects online; this is detrimental to innovation, learned debate and the spirit of healthy argument.

Data Misuse and Security Risks

The mass storage of personal data increases the risk of unauthorized access and cyber-attacks, which can expose sensitive information to malicious actors. Governments and corporations holding large data troves become targets for hackers, leading to data breaches that compromise individuals' security. Inadequate data protection measures and security breaches have resulted in stolen information used for identity theft, financial fraud, and even political manipulation, threatening individuals' rights and security on a broader scale.

Discrimination and Bias

Storing a great amount of personal information in one place increases the possibility of unauthorized access and cybercrimes that may enable the malicious intervention into the private data of individuals. Governments and organizations that have a huge amount of data stored in them attract hackers, leading to breaches as malicious actors break in the systems exposing the security of the citizens as well. The insufficiency of data protection policies and the breakup of the existing defenses have also led to the emergence of the problem of misuse of information in key areas, including the capacities of stealing it for the purpose of identity theft, financial crime, and even political propaganda, which impacts the rights and safety of people in a more impactful way.

Lack of Transparency and Accountability

A notable dilemma surrounding surveillance and data collection systems is how secretive they can be. Frequently, there is a grand failure in the aspect that the government, multinational enterprises for one reason or the other cannot always admit to survey management scopes. Therefore, it is easier and more concrete for individuals to understand the surveillance process. However, data collectors and the process are

thoroughly obscured by the lack of open policies and law that exist in most countries. This breeds further distrust and makes it almost improbable for individuals to fight such a situation, as well as institutions to be held to account in case of any infringement.

Major Parties Involved and Their Views

United States

The United States has one of the world's most advanced surveillance infrastructures, largely expanded after the 9/11 attacks in an effort to combat terrorism. Under laws like the USA PATRIOT Act, the U.S. government gained broad authority to monitor electronic communications, collect data on citizens and foreigners, and analyze this information for potential threats. The National Security Agency (NSA), for example, gathered telephone metadata from millions of Americans until the practice was curbed in 2015 by the USA FREEDOM Act. However, programs like PRISM still allow intelligence agencies to access data stored by tech companies like Google and Facebook when national security is concerned.

In recent years, surveillance capabilities have extended to include biometric data such as facial recognition technology used in airports and public spaces. For instance, the U.S. Customs and Border Protection (CBP) has implemented facial recognition at more than 32 major airports, intending to streamline security processes. Although these measures aim to enhance security, the sheer volume of data collected raises concerns about misuse, transparency, and oversight. Despite reforms, civil rights organizations continue to question how the government manages and safeguards such extensive information, especially as tech advances make surveillance easier and more invasive.

European Union

The European Union (EU) is globally recognized for its strong stance on privacy and data protection, most notably through the General Data Protection Regulation

(GDPR), enacted in 2018. GDPR requires companies to disclose their data collection activities to the public and to give individuals the right to personal data possession as well as use by others. In addition, fines are imposed in the case of breach which may not exceed the figure of €20 million or 4% of the annual world revenue of the company, pre-tax profit, whichever is higher. Last year, for instance, Amazon attracted a fine of €746 million imposed by the Luxembourg data protection authority regarding some compliance regulation with respect to GDPR, which once again underlined the EU's authority on privacy matters.

But the GDPR is not the limit. The European Court of Justice has even nullified the relevant document, one of which was the Privacy Shield signed with the U.S. in 2016 and declared as null and void in 2020. All in the context of increasing levels of caution by the EU when it comes to sharing of European citizen data with countries without those safeguards, cementing Europe as a key privacy frontier. In more current measures similar to the Digital Service Act, the EU's objective is to enforce controls and standards in the operations of online platforms across member states so that user data and digital rights are not undermined.

China

China has a widespread and developed surveillance system in place. It is used not only for the purpose of control, it has become an integral part of a state's governance system. There are over 200 million surveillance cameras with a face recognition function within China, which is said to make the country one of the most watched in the world. This picture of the use of the social control system in daily life is multidimensional, it ranges from the use of the interface to guards for security surveillance to the use of traffic traffic violations. Apart from this, the social credit system that is still on a trial bases in a number of cities is designed to manage people's actions by evaluating behavioral attitudes and allocating a 'social credit score' which determines access to some services and opportunities.

China has also been using export of intrusive technologies as a tool to increase its political and economic presence as part of Belt and Road Initiative in developing states primarily in Africa and Asia Malaya, Sold under the brand name, companies like Huawei and Hikvision, Ltd. distribute their equipment for digital control and surveillance in many foreign countries and regions even where privacy is not strictly observed. Although China defends its surveillance as necessary for maintenance of social order, it has also led to gross violations of human rights. In this sense, the constitution provides some safeguards for guarantees of freedoms, but it is no secret that there are certain areas where the government has introduced various restrictions, particularly on individual and communal rights of the citizens; they are also most keen on maintaining power and security in the interests of the state.

Five Eyes Alliance (U.S., U.K., Canada, Australia, New Zealand)

The Five Eyes is a significant and historical intelligence alliance, which was initially established at the time of World War II. The alliance makes it possible to turn over data and information acquired during monitoring from one country to another without the need to clutter the already enormous information base further. In practice, various countries combine their capabilities to ensure that the necessary information is in one state or another, which has brought about a lot of counter-terrorism successes, for example, the pursuit of the 2005 London bombers.

Such an international alliance of intelligence services has its side effects - personal safety statistics as most of such interaction can potentially breach the right of every citizen to privacy since it provides legal means of circumventing domestic privacy laws. For instance, the United States cannot conduct overt intelligence activities against its own citizens due to laws or regulations but it can benefit from such data-gathering by its allied forces in the case of intra-governmental cyber-espionage.

Democratic People's Republic of Korea (DPRK)

North Korea (DPRK) operates one of the most extensive and restrictive surveillance systems in the world, using surveillance as a tool to maintain absolute control over its population. The government heavily monitors communications, internet access (limited and restricted to domestic intranet), and citizens' movements to prevent dissent and enforce strict ideological compliance. Citizens have no access to the global internet, and only a select few—primarily government elites—can use a tightly controlled internal network known as Kwangmyong.

North Korea's control extends beyond its borders as well, the regime monitors North Korean defectors abroad through intelligence networks and uses digital surveillance to track them and their communications. For example, North Korean authorities are known to monitor refugees who resettle in South Korea, and individuals suspected of anti-regime activities face harassment and intimidation. This totalitarian surveillance system is aimed at preventing any threats to the regime's power, with the DPRK showing no regard for privacy rights, freedom of expression, or international data protection norms.

Development of Issue/Timeline

Date	Event	Outcome
1948	The Universal Declaration of Human Rights (UDHR) adopted by the United Nations	Establishes the right to privacy (Article 12) and freedom of expression (Articles 19 and 21).
1966	The International Covenant on Civil and Political Rights (ICCPR) was adopted	Strengthens the protection of privacy, freedom of association, and freedom of expression.
1970s	Widespread adoption of telephone wiretapping and electronic surveillance in the U.S	The beginning of major concerns about the balance between national security and individual rights

1980s	Development of computer databases for tracking individuals and storing sensitive information	Early concerns arise over data collection practices by both government and private entities
1995	European Union passes the Data Protection Directive (95/46/EC)	Establishes frameworks for the protection of personal data and privacy in the EU
2001	USA PATRIOT Act enacted post-9/11 terror attacks	Expands surveillance powers in the name of anti-terrorism
2006	Introduction of RFID (Radio Frequency Identification) technology for tracking individuals	Invasiveness of tracking technology and its potential human rights violations.
2013	Edward Snowden leaks NSA surveillance documents revealing global mass data collection	International outrage and calls for reforms to prevent surveillance overreach and protect civil liberties
2014	EU Court of Justice invalidates the EU-U.S. Safe Harbor Agreement due to data privacy concerns	Reaffirms the importance of privacy and human rights in cross-border data transfers.
2016	UN Special Rapporteur on Privacy publishes report on surveillance and human rights	Highlights the disproportionate use of surveillance and its human rights impacts, urging stronger protections
2017	General Data Protection Regulation (GDPR) comes into effect in the EU	Introduces stricter data protection and privacy laws, setting a global standard for data collection practices.
2018	Facebook-Cambridge Analytica scandal exposes mass data collection for political manipulation	Increased scrutiny on tech companies' data collection practices and calls for stricter regulation.
2020	WHO's COVID-19 contact tracing apps were implemented	Calls for clear guidelines to balance public health and privacy rights during emergencies.

2021	China implements the Social Credit System, collecting vast amounts of personal data for behavioral monitoring	Call for regulation regarding state control and surveillance, especially in non-democratic contexts.
2022	UN General Assembly adopts a resolution on the right to privacy in the digital age	Reaffirms the need to protect privacy and other human rights amidst growing digital surveillance.
2022	India's Personal Data Protection Bill was introduced in parliament	Addressing privacy concerns in a rapidly digitizing nation
2023	European Court of Justice rules on the legality of facial recognition technology in public spaces	Raises questions about the use of surveillance technology in public areas
2024	Global initiative to develop a treaty on digital surveillance and privacy begins	International collaboration to address the challenges of digital surveillance and protect human rights globally.
2024	Global protests erupt against invasive surveillance systems, demanding stronger privacy protections	People worldwide push for greater oversight and restrictions on mass data collection and surveillance practices.

Previous Attempts to Solve the Issue

Data Protection Laws

Over the years, several countries have introduced data protection laws to address privacy concerns surrounding mass data collection. One of the most notable efforts is the General Data Protection Regulation (GDPR), which came into force in May 2018 within the European Union (EU). The GDPR aims to regulate how personal data is collected, processed, and stored by both public and private organizations. It provides individuals

with greater control over their data, including the right to access, rectify, and delete personal information.

In addition to GDPR, countries like Brazil (with its Lei Geral de Proteção de Dados or LGPD in 2020) and California (with the California Consumer Privacy Act (CCPA) in 2020) have implemented similar laws to protect individual privacy rights.

UN Resolutions on Privacy

The United Nations has recognized the right to privacy as fundamental in the digital age. In 2013, the UN General Assembly passed Resolution 68/167 on the right to privacy in the digital age, which called for an international response to ensure that privacy protections keep up with technological advancements. This resolution highlights the need for states to avoid surveillance practices that violate human rights, ensuring that surveillance is used only for legitimate purposes, with oversight mechanisms in place.

Additionally, the Human Rights Council (HRC) has issued reports urging governments to uphold privacy rights in the face of expanding surveillance technologies. While the UN's resolutions and reports have raised global awareness, there is a lack of enforcement mechanisms, and many countries, particularly authoritarian regimes, have ignored these calls for privacy protection.

Public Advocacy

The Edward Snowden revelations of 2013 exposed the extensive mass surveillance programs conducted by the National Security Agency (NSA), including the collection of phone metadata and internet communications under the PATRIOT Act. This triggered global outrage and led to widespread discussions on privacy rights, surveillance, and government overreach. Advocacy groups, such as the Electronic Frontier Foundation (EFF) and Privacy International, have worked tirelessly to challenge these practices and promote privacy laws.

Following the Snowden leaks, the USA Freedom Act was passed in 2015, which ended the NSA's bulk collection of phone metadata and increased transparency in government surveillance programs.

Technological Countermeasures

In response to growing concerns about surveillance, privacy-focused technologies have emerged, such as end-to-end encrypted messaging services like Signal and WhatsApp, and anonymous browsing tools like Tor. These tools aim to protect user data from government surveillance and unauthorized data collection by private companies.

Additionally, innovations in blockchain technology are being explored to provide secure, decentralized data storage and management, which could limit the ability of both governments and corporations to access and exploit personal information.

Possible Solutions

Surveillance Free - Zones

A practical solution could be the establishment of Surveillance-Free Zones in public spaces. These zones would be designated areas where individuals can opt out of surveillance measures, including CCTV cameras, facial recognition systems, and location tracking technologies. Parks, community centers, and certain neighborhoods could be transformed into safe havens where privacy is respected. Legal protections would ensure that no surveillance data is collected in these spaces, allowing citizens to enjoy moments of privacy in an increasingly monitored world.

Targeted Data Collection

A key solution would be to limit data collection to specific, targeted actions related to suspected criminal activities. Data collection should not be a blanket measure but should be based on probable cause and specific legal authorizations. Governments

and law enforcement agencies could be required to obtain warrants for any large-scale surveillance, including the monitoring of communications, location tracking, and financial transactions. Clear guidelines should ensure that only data relevant to ongoing investigations is collected, and safeguards should be in place to prevent mass surveillance of innocent civilians.

Independent Oversight Committees

An effective way to ensure the ethical use of data in criminal investigations is to establish independent oversight committees. These committees could be composed of privacy experts, civil rights advocates, and legal professionals, and would be tasked with monitoring surveillance activities, reviewing requests for data collection, and ensuring that all actions are in compliance with human rights standards. Such committees would report regularly on the effectiveness and legality of surveillance programs, offering transparency and accountability.

Clear Data Retention Policies

One of the major concerns with data collection for criminal monitoring is the potential for data to be retained indefinitely or used for unintended purposes. Governments and law enforcement agencies should implement strict data retention policies that specify how long data can be retained after its collection. Data should be stored only for the duration of an investigation or as required by law and should be destroyed or anonymized once it is no longer necessary. Clear rules on the retention, deletion, and sharing of data are essential for ensuring that surveillance does not lead to the creation of permanent records on innocent individuals.

Public Transparency and Annual Reporting

To ensure that surveillance practices remain transparent and accountable, governments should be required to produce annual transparency reports outlining the

extent of data collection, the number of surveillance requests, and the outcomes of investigations. These reports should also include the number of times surveillance led to successful criminal convictions or prevention of criminal activities. By making these reports publicly available, citizens would have greater insight into how their personal data is being used and could hold authorities accountable for any overreach.

Bibliography

The Guardian. "The NSA Files." The Guardian, https://www.theguardian.com/us-news/the-nsa-files. Accessed 4 Nov. 2024.

Electronic Frontier Foundation. "NSA Spying." EFF, https://www.eff.org/nsa-spying. Accessed 5 Nov. 2024.

Snowden, Edward. "Permanent Record." Edward Snowden, https://edwardsnowden.com/permanent-record/. Accessed 6 Nov. 2024.

American Civil Liberties Union. "NSA Surveillance." ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance. Accessed 7 Nov. 2024.

Lawfare. "Snowden Revelations." Lawfare, https://www.lawfareblog.com/snowden-revelations. Accessed 10 Nov. 2024.

MIT Technology Review. "Artificial Intelligence." MIT Technology Review, https://www.technologyreview.com/topic/artificial-intelligence/. Accessed 4 Nov. 2024.

Electronic Privacy Information Center. "Artificial Intelligence and Human Rights." EPIC, https://epic.org/issues/ai/. Accessed 5 Nov. 2024.

Stanford University. "Artificial Intelligence and Privacy." Stanford HAI, https://hai.stanford.edu/policy/policy-resources/artificial-intelligence-and-privacy. Accessed 6 Nov. 2024.

World Privacy Forum. "Artificial Intelligence." World Privacy Forum, https://www.worldprivacyforum.org/category/artificial-intelligence/. Accessed 7 Nov. 2024.

Future of Privacy Forum. "Artificial Intelligence." FPF, https://fpf.org/issue/artificial-intelligence/. Accessed 10 Nov. 2024.

Electronic Frontier Foundation. "Social Media Surveillance." EFF, https://www.eff.org/issues/social-media-surveillance. Accessed 4 Nov. 2024.

Brennan Center for Justice. "Social Media Monitoring." Brennan Center, https://www.brennancenter.org/issues/protect-liberty-security/social-media-monitoring. Accessed 5 Nov. 2024.

Center for Democracy & Technology. "Digital Privacy." CDT, https://cdt.org/area-of-focus/privacy-data/digital-privacy/. Accessed 10 Nov. 2024.

International Association of Privacy Professionals. "Glossary of Privacy Terms." IAPP, https://iapp.org/resources/glossary/. Accessed 4 Nov. 2024.

Electronic Privacy Information Center. "Privacy." EPIC, https://epic.org/privacy/. Accessed 5 Nov. 2024.

Privacy International. "What Is Privacy?" Privacy International, https://privacyinternational.org/explainer/56/what-privacy. Accessed 6 Nov. 2024.

Stanford Encyclopedia of Philosophy. "Privacy." Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/privacy/. Accessed 7 Nov. 2024.

OECD. "OECD Privacy Guidelines." OECD, https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm. Accessed 10 Nov. 2024.

Brennan Center for Justice. "Liberty and National Security." Brennan Center, https://www.brennancenter.org/issues/protect-liberty-security. Accessed 6 Nov. 2024.

Center for Democracy & Technology. "Civil Rights and Technology." CDT, https://cdt.org/area-of-focus/equity-in-civic-technology/. Accessed 7 Nov. 2024.

Privacy International. "Data and Civil Rights." Privacy International, https://privacyinternational.org/learn/data-and-civil-rights. Accessed 10 Nov. 2024.

PEN America. "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor." PEN America, https://pen.org/chilling-effects/. Accessed 4 Nov. 2024.

Electronic Frontier Foundation. "Free Speech." EFF, https://www.eff.org/issues/free-speech. Accessed 5 Nov. 2024.

ACLU. "Freedom of Expression." ACLU, https://www.aclu.org/issues/free-speech. Accessed 6 Nov. 2024.

World Privacy Forum. "Data Breaches." World Privacy Forum, https://www.worldprivacyforum.org/category/data-breaches/. Accessed 5 Nov. 2024.

Center for Strategic and International Studies. "Technology Policy Program." CSIS, https://www.csis.org/programs/strategic-technologies-program. Accessed 6 Nov. 2024.

Privacy International. "Data Exploitation." Privacy International, https://privacyinternational.org/learn/data-exploitation. Accessed 10 Nov. 2024.

AI Now Institute. "Algorithmic Accountability." AI Now, https://ainowinstitute.org/research/algorithmic-accountability. Accessed 4 Nov. 2024.

Brennan Center for Justice. "Racial Justice." Brennan Center, https://www.brennancenter.org/issues/advance-constitutional-change/racial-justice. Accessed 5 Nov. 2024.

ACLU. "Racial Justice." ACLU, https://www.aclu.org/issues/racial-justice. Accessed 6 Nov. 2024.

Center for Democracy & Technology. "Equity in Civic Technology." CDT, https://cdt.org/area-of-focus/equity-in-civic-technology/. Accessed 7 Nov. 2024.

Electronic Privacy Information Center. "Domestic Surveillance." EPIC, https://epic.org/privacy/surveillance/. Accessed 5 Nov. 2024.

Brennan Center for Justice. "Government Surveillance." Brennan Center, https://www.brennancenter.org/issues/protect-liberty-security/government-surveillance. Accessed 6 Nov. 2024.

Privacy International. "Challenging Surveillance." Privacy International, https://privacyinternational.org/impact/challenging-surveillance. Accessed 7 Nov. 2024.

American Civil Liberties Union. "Transparency." ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/transparency. Accessed 10 Nov. 2024.

Lawfare. "Surveillance." Lawfare, https://www.lawfareblog.com/topic/surveillance. Accessed 10 Nov. 2024.

European Commission. "Data Protection." EC, https://ec.europa.eu/info/law/law-topic/data-protection_en. Accessed 4 Nov. 2024.

International Association of Privacy Professionals. "Resource Center." IAPP, https://iapp.org/resources/. Accessed 5 Nov. 2024.

United Nations. "The Right to Privacy in the Digital Age." OHCHR, https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx. Accessed 6 Nov. 2024.

OECD. "Data Governance and Privacy." OECD, https://www.oecd.org/digital/data-governance-and-privacy/. Accessed 7 Nov. 2024.

Privacy International. "Data Protection." Privacy International, https://privacyinternational.org/learn/data-protection. Accessed 10 Nov. 2024.

Electronic Frontier Foundation. "Surveillance Technologies." Electronic Frontier Foundation, https://www.eff.org/issues/surveillance-technologies. Accessed 4 Nov. 2024.

American Civil Liberties Union. "Privacy and Surveillance." ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies. Accessed 5 Nov. 2024.

Privacy International. "Surveillance." Privacy International, https://privacyinternational.org/learn/surveillance. Accessed 6 Nov. 2024.
Atomic Heritage Foundation. "Espionage and the Manhattan Project." Atomic Heritage Foundation, https://www.atomicheritage.org/history/espionage-and-manhattan-project. Accessed 10 Nov. 2024.

National Security Agency. "Understanding the Threat." NSA, https://www.nsa.gov/what-we-do/understanding-the-threat/. Accessed 10 Nov. 2024.

Electronic Privacy Information Center. "NSA Surveillance." EPIC, https://epic.org/privacy/surveillance/nsa/. Accessed 10 Nov. 2024.

Federation of American Scientists. "National Security Agency." FAS, https://fas.org/irp/agency/nsa/. Accessed 10 Nov. 2024.

National Archives. "National Security Agency (NSA)." National Archives, https://www.archives.gov/research/guide-fed-records/groups/457.html. Accessed 10 Nov. 2024.

Electronic Privacy Information Center. "Big Data and the Future of Privacy." EPIC, https://epic.org/privacy/big-data/. Accessed 6 Nov. 2024.

Pew Research Center. "Internet & Technology." Pew Research Center, https://www.pewresearch.org/internet/. Accessed 7 Nov. 2024.

MIT Technology Review. "Big Data." MIT Technology Review, https://www.technologyreview.com/topic/big-data/. Accessed 10 Nov. 2024.

Future of Privacy Forum. "Big Data." Future of Privacy Forum, https://fpf.org/issue/big-data/. Accessed 10 Nov. 2024.

Department of Justice. "The USA PATRIOT Act: Preserving Life and Liberty." Justice.gov, https://www.justice.gov/archive/ll/highlights.htm. Accessed 10 Nov. 2024.

ACLU. "Surveillance Under the USA/PATRIOT Act." American Civil Liberties Union, https://www.aclu.org/other/surveillance-under-usapatriot-act. Accessed 6 Nov. 2024.