DATA PRIVACY ISSUES AND RISKS WITH SHARING ON SOCIAL MEDIA: AN INQUIRY

NEHALUDDIN AHMAD[1,]
Professor of Law, University Islam Sultan Sharif Ali (UNISSA), Brunei Darussalam[1]
ahmadnehal@yahoo.com[1]

Abstract. *The widespread use of spyware by governments and corporations has raised ethical questions about the cumulation and tracking of personal data. Social media networks have become increasingly embedded in our daily lives, and our concerns over online privacy and surveillance are increasing daily. This paper discusses the literal background of privacy rights which includes its position in international law as well as its challenges in developing technologies. It further examines the impact of social media networks and spyware on human rights, which include the right to privacy, free speech, and personal autonomy. Additionally, this paper will outline potential outcomes or strategies to protect privacy rights, primarily online, and advocate for continued awareness and engagement on the issue. In conclusion, this paper calls on individuals, organizations, and policymakers to work together to uphold the right to privacy and protect against the misuse of personal data.*
Keywords: *social media, right to privacy, spyware, human rights*

INTRODUCTION

In this modern era, it plays a vital role, especially in the realms of online communication, which made any communication possible through the use of computers and the Internet.[1] Accordingly, it is no doubt that people from all around the globe engage in various forms of social media as their daily routine activity. This is because of the great opportunity that it can offer, such as communicating with one another, expressing themselves, and sharing content of all kinds.[2] Instances of social media networks are Facebook, Twitter, Instagram, and LinkedIn.

Meanwhile, spyware is referred to as software that is intended to gather information from a computer system or mobile device without the permission of the user. This data can include keystrokes, passwords, browsing history, and other sensitive information. It is typically installed on a device through malicious links, software downloads, or email attachments and can be used for various purposes, including government surveillance, corporate espionage, and identity theft.

On the other hand, privacy rights are an essential component of human rights, and their protection is critical for individuals to live free and autonomous lives. It enables individuals to make absolute decisions about their lives without any interference from third parties as well as having complete control of their personal information, preventing it from being shared or sold without their consent. It is also essential for ensuring safety and security by protecting sensitive information, such as financial data or medical records, from being accessed by unauthorized parties. In addition, it protects against discrimination based on personal characteristics, for instance, racial origin, religion, or sexual orientation.

This paper calls on individuals, organizations, and policymakers to work together to uphold privacy rights and protect against the misuse of personal data. In order to better understand its concept, it is wise to know its background first. Hence, the next section of this paper discusses the literal background of privacy rights as well as its position in international law and its development in new

[1] Shelly Shekhawat and Bindu Bhat, "Analysing the Impact of Social Media on Women: A Study in Vadodara City" (2021) 9(1) International Journal of Interdisciplinary Research and Innovations 53-59.
[2] Mrunal, "Impact of Social Media on Children" (Parenting, 13 January 2023) <https://parenting.firstcry.com/articles/impact-of-social-media-on-children/#Negative_Effect_of_Social_Media_on_Kids> accessed on 20th May 2023.

technologies. Section III of this paper discusses the impact of social media on the right to privacy. Section IV discusses the impact of spyware on the right to privacy. Subsequently, it discusses the potential solutions to protect privacy rights. This article concluded that although many advantages can be offered by social media, such as a prominent means of communication nowadays, it also has taken an evitable toll on its users in which a privacy breach occurs once they have sent messages or uploaded any materials online. However, this risk can be lowered with the potential solutions suggested in this paper.

The literal background of privacy rights

The concept of an individual's right to privacy derives from the Latin term *"ius,"* which eventually came to be understood as an individual's entitlement to control or claim anything. This concept was first presented in the *Decretum Gratiani,* which was written in Bologna, Italy, in the 12th century.[3] The first explicit recognition of the right to privacy in the United States was in 1890. It is defined as the right to be left alone and aimed to protect individuals from emerging technologies such as photography and sensationalist journalism.[4] The right to privacy and technology have been intertwined since then, with subsequent legal cases and principles developing to protect individuals' privacy rights.

According to Alan Westin, the scales of privacy and disclosure have tipped in a new direction as a result of technological advancements, and privacy rights have the potential to restrict government surveillance to safeguard democratic procedures. According to him, privacy is the capacity of people, associations, or organizations to control the timing, manner, and degree of information sharing about them. He established four levels of privacy which are solitude, intimacy, anonymity, and reserve, which must be balanced against participation and social norms.[5] In political frameworks that adhere to liberal democratic principles, the protection of personal privacy makes room for personal autonomy as well as democratic freedoms of association and expression. David Flaherty is of the opinion that computer databases present a risk to individuals' right to privacy. He is an advocate for data protection as a component of privacy, emphasizing the fact that individuals want control over the manner in which their personal information is utilized.[6] Marc Rotenberg describes the modern right to privacy as Fair Information Practices, with rights allocated to data subjects and responsibilities assigned to data collectors.[7] Posner and Lessig emphasize the economic issues of controlling access to private details, with Posner opposing privacy for its tendency to conceal information and decrease market efficiency[8], while Lessig believes that breaches of privacy can be regulated through law and code and that individuals should have property rights over their personal information.[9] These economic approaches make communal conceptions of privacy challenging to maintain.

Some attempts have been made to redefine privacy as an essential human right that become a significant role in the effective operation of democratic societies.[10] Regan suggests that individualized definitions of privacy have been inadequate in policy and philosophy, and instead, she proposes a social value of privacy that consists of shared opinions, public values, and collective components.[11] Leslie Regan Shade argues that privacy is necessary for genuine democratic participation and upholds human dignity and autonomy. According to Leslie Regan Shade, the protection of one's privacy is not only essential for the exercise of genuine democratic participation but also maintains human dignity and autonomy. Shade believes that while thinking about privacy, one should not simply look at it

[3] James Griffin, "The Human Right to Privacy" (2007) San Diego Law Review 3.
[4] Warren SD and Brandeis LD, "The Right to Privacy" (1890) 4 Harvard Law Review 193
[5] A. Westin, "Privacy and Freedom" (1968) 25 Washington and Lee Law Review 166
[6] D. Flaherty, *Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (The University of North Carolina Press, 1989)
[7] A. Allen, and M. Rotenberg, *Privacy Law and Society,* (West Academic Publishing, 2016)
[8] R.A Posner, "The economics of privacy" (1981) 71 The American Economic Review 2, 405–409.
[9] L. Lessig, Code: Version 2.0., (Basic Books, 2006)
[10] Deborah Johnson, Bowie Beauchamp; Arnold (eds.). Ethical theory and business (Pearson/Prentice Hall, 2009) 428–442.
[11] P.M Regan, Legislating Privacy: Technology, social values, and public policy (The University of North Carolina Press, 1995)

through the lens of the market, but rather from the perspective of the people it affects.[12] Both scholars advocate for a stronger recognition of privacy rights in policymaking.

In the eyes of international law, privacy rights are considered as privacy as one of the most significant human rights is the UDHR. Article 12 of the UDHR states that "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation," recognizing privacy as one of the human rights. Everyone has a right to legal protection from these types of intrusions or assaults.

Privacy was also acknowledged in Article 17 of the ICCPR, which was adopted 18 years after the UDHR, by utilizing language that is comparable to Article 12 of the UDHR. The only distinction between those two articles, Article 17 of the ICCPR inserts the phrase "unlawful" before the term "interference" and "attacks". It stated that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

After two decades, another significant UN document, the 1989 Convention on the Rights of the Child (CRC), uphold privacy rights which specifically aims to protect children's private interests among other things. The UN General Assembly (UNGA) enacted Resolution 44/25, or the CRC, on November 20, 1989, pledging to uphold all children's rights, including their right to privacy. Article 16 of UNCRC affirms that "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks.

In addition to that, the UN Special Rapporteur on the Right to Privacy's Reports has made the UN's commitments and efforts to protect privacy clear and unambiguous.[13] Professor Joseph A. Cannataci was chosen by the UN Human Rights Council in July 2015 to serve as its first-ever Special Rapporteur on the topic of "The Right to Privacy in the Digital Age." He had been given orders to carry out a variety of tasks, including gathering pertinent data, spotting potential roadblocks, taking part in international campaigns, promoting awareness, and delivering annual reports to the UN General Assembly and Human Rights Council. During his time in office, Professor Joseph A. Cannataci has made many efforts and passionately started his roles on the topic.[14] In July 2021, the Human Rights Council appointed Dr. Ana Brian Nougrères of Uruguay as the Special Rapporteur on the right to privacy, and she took up the mandate on 1 August 2021.[15] A Professor of Law, Privacy, and ICT at the School of Engineering, University of Montevideo, and a Professor of Law, Data Protection, and ICT at the School of Law, University of the Republic, Montevideo. She is also a practicing Attorney-at-law and Consultant on data protection.

Despite this, privacy rights have been challenged, especially with the rapid development of digital technology, which can store and record all online activities, creating a permanent digital footprint as well as social media mining. Social media mining is a method of examining information gathered from social media activities to detect patterns. Google and Facebook use data mining techniques to analyze user information for targeted advertising. For instance, Google analyzes information in Gmail to show relevant ads, while Facebook partners with data mining companies to personalize ads for

[12] L. R. Shade, "Reconsidering the right to privacy in Canada" (2008) 28 Bulletin of Science, Technology & Society 1, 80–91.

[13] OHCHR, "Special Rapporteur on the rights of privacy" (OHCHR, n.d.) <https://www.ohchr.org/en/special-procedures/srprivacy#:~:text=In%202015%2C%20the%20Human%20Rights,and%20cases%20relating%20to%20privacy> accessed 25th May 2023.

[14] Toriqul Islam, "A Brief Introduction to the Right of Privacy – An International Legal Perspective" (NYU Law, 2022) <https://www.nyulawglobal.org/globalex/Right_To_Privacy_International_Perspective.html> accessed 25th May 2023

[15] OHCHR, "Special Rapporteur on the rights of privacy" (OHCHR, n.d.) <https://www.ohchr.org/en/special-procedures/srprivacy#:~:text=In%202015%2C%20the%20Human%20Rights,and%20cases%20relating%20to%20privacy> accessed 25th May 2023.

users.[16] Researchers are also able to leverage the huge volumes of data that are available from social media to design product features and extract insights.[17]

The ethical concerns regarding the usage of user information by companies are referred to as big data.[18] When users sign up for social media platforms, they frequently skip over the Terms of Use agreements, which leads to them having no idea how their information is being used or if they even have a choice in the matter. When user data is collected, this creates concerns about privacy and monitoring, both of which are problematic. Some social media platforms have included features such as capture time and geotagging in order to provide users with more information regarding the context of the content they are seeing. This helps to make the data more accurate and is one of the ways that social media platforms have evolved.

Mark Zuckerberg, the Chief Executive Officer of Facebook, testified in front of senators on April 10, 2018, during a hearing to answer concerns regarding various problems, including privacy, the financial model of the company, and the improper use of data. The news that Cambridge Analytica, tied to the Trump campaign, had collected information from around eighty-seven million users of Facebook to generate psychological profiles of voters during the 2016 election led to this development. The question was posed to Zuckerberg on how data about users could be obtained by third parties without the users' knowledge. In addition, MPs questioned him over the dissemination of false news on Facebook, interference by Russia in the presidential election of 2016, and the censoring of conservative media.[19]

Users generate content for social media through the interactions they have with one another on various social media platforms. Since this content is created by users but housed by the platform, the question of who owns it has been the subject of a large amount of discussion. In addition, there is a possibility that data security will be breached, since third parties that have financial interests in the platform or individuals who are looking to construct their own databases may acquire access to the material in question. Because of this, it is susceptible to exploitation by individuals who are not authorized.[20]

In order to upload content to their websites, social media platforms like Facebook, Instagram, Twitter, and YouTube are required to obtain licenses from the appropriate copyright owners. They are able to carry out a specific activity because they have been granted the legal right, which is represented by a license. When you agree to the terms and conditions of a platform, you are effectively giving the platform permission to use your content, even if you are the owner of the content. Even while these licenses are different for each social media platform, they all provide social media sites the right to use your intellectual material in any way they see fit, which may include making it available for commercial use or sublicensing it to a third party. On the other hand, because these licenses are "royalty-free," you won't earn any portion of the cash that they generate.

When Facebook purchased Instagram in 2012, the company made a stir when it declared its intention to use user posts in advertisements without first asking permission or compensating people for their contributions. This sparked a debate. Let's look at the Terms of Service to see if this is still true.[21] According to Instagram's terms, users retain ownership of any content they post on the platform. On the other hand, Instagram is granted a license to use the content that is placed on the platform of

---

[16] Tama Leaver, "The Social Media Contradiction: Data Mining and Digital Death" (2013) 16 Journal of Media and Culture 2.

[17] Sumbaly R, Kreps J and Shah S, "The Big Data Ecosystem at LinkedIn" (2013) Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data

[18] Shvalb N, Our Western Spring: The Battle Between Technology and Democracy, Moment of Truth Kindle Edition (Amazon Books, 2022)

[19] The New York Times, "Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy" (The New York Times, April 10, 2018) < https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html> accessed 20th February 2023

[20] Harvey Jones and Soltren, José Hiram, "Facebook: Threats to Privacy" (2005) MIT Computer Science & Artificial Intelligence Lab.

[21] "Help Center" (Help Center, n.d) <https://help.instagram.com/478745558852511> accessed 2nd February 2023

which is fully compensated, royalty-free, transferable, and sub-licensable. This license is not exclusive, it includes the right to display advertisements and promotions alongside user-generated content. Instagram expressly disclaims ownership of user content, but it appears that this practice of exploiting content created by users for marketing and advertising purposes has not been discontinued. Instagram has a similar provision in their terms as Facebook and Twitter, where they are allowed to use and display your content without your permission or prior notification for marketing and advertising purposes.[22]

Privacy experts advise users of social media platforms to be wary of the collection of personal data about them. Electronic tracking and apps provided by third parties have the potential to collect information about users without their knowledge or consent. Data collection for law enforcement and other government objectives is accomplished through the use of data mining techniques by social media intelligence.[23] Third parties may also gather data and information. When information is published on social media, it is no longer considered private, and young people, in particular, are at risk of sharing too much information, which could make them more vulnerable to being targeted by predators. It is crucial to monitor what is shared and whom it is shared with. Studies suggest that teens, in particular, share more personal information on the internet than ever before, including email addresses, phone numbers, and school names.[24] Many teens are unaware of how much their information can be gained by external parties.

Some people believe that privacy is no longer possible due to the pervasiveness of the use of social media. Others argue that individuals still value privacy, but social media companies may profit by sharing their personal information. People's actions on social media may contradict their stated desire for privacy. When users create an account on a social media platform, they are asked to enter personal information such as their name, birthday, location, and interests. This information is then gathered by the platform's operators and utilized by them to serve more relevant advertisements to users. Additionally, information regarding the behavior of users is recorded and used for the same function.[25]

There is a lack of knowledge about how public social media posts can be. Some users may not be aware that their posts are visible to a larger audience beyond their circle of friends. This has led to some users being criticized for their inappropriate comments, which they thought would only be seen by their close friends. Some social media sites default to sharing content with a wide audience unless the user specifically chooses higher privacy settings.

A 2016 article explored the impact of social media on expectations of privacy, revealing that on any given day, 1.18 billion people log into Facebook, 500 million tweets are sent, and 95 million photos and videos are posted on Instagram. The problem with privacy often arises from the individuals themselves, as they choose to share voluntarily and see it as a societal norm.[26] social media has become a snapshot of our lives, built on behaviors like sharing, posting, liking, and communicating. Sharing has been revolutionized by social networks, but privacy has become a redundant idea. Once something is posted, it remains accessible even if we limit who can see it. People value privacy, but their social media activities are hard to maintain.[27] Mills suggests solutions such as implementing copyright and laws of confidence, or even changing the concept of privacy altogether.

---

[22] *ibid*

[23] Auer MR, "The Policy Sciences of Social Media" (2011) 39 Policy Studies Journal 709.

[24] Madden M and others, "Teens, Social Media, and Privacy" (Pew Research Center: Internet, Science & Tech, May 21, 2013) <https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/> accessed 12 February 2023

[25] "Social Media Privacy Issues for 2020: Threats & Risks" (Tulane University | School of Professional Advancement, n.d) <https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020> accessed 23rd February 2023

[26] Kate Murphy, "We Want Privacy, but Can't Stop Sharing" (NY Times, 4 October 2014) < ytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html> accessed 3rd March 2023.

[27] Mills M, "Sharing Privately: The Effect Publication on Social Media Has on Expectations of Privacy" (2017) 9 Journal of Media Law 45.

In 2014, the Pew Research Center conducted a survey that found 91% of American adults either agreed or strongly agreed that they have lost control over how various businesses are collecting and using their personal information. Eighty percent of social media users surveyed expressed concern about businesses and marketers having access to their data shared on social media platforms, while sixty-four percent believed that the government should take additional steps to control these ads.[28]

On February 17, 2019, the Wall Street Journal published an article stating that, in accordance with UK law, Facebook does not preserve certain terms of user data in a sufficient manner.[29] The US government declared that TikTok and WeChat would be banned in the country due to national security concerns. The ban was set to begin on September 20, 2020. TikTok's access was prolonged until November 12, 2020[30], and on October 30, 2020, a federal court decision prevented the enforcement of additional measures that would have resulted in TikTok's shutdown.[31] In 2019, the Pentagon provided instructions to various US government agencies, including the Army, Navy, Air Force, Marine Corps, Coast Guard, Transportation Security Administration, and Department of Homeland Security, which highlighted the risks associated with using TikTok and advised employees to take necessary precautions to protect their personal information.[32] Consequently, these agencies banned using TikTok on government devices and even blacklisted it on their internal network services.[33]

The impact of social media networks on privacy rights

Social media networks gather vast amounts of information on their users through various methods. Some of the most common ways that social media networks track and collect data include:

(1) User-provided information: Social media networks collect information that users provide when they create an account, such as their name, birthday, and email address;

(2) User activity: Social media networks track users' activity on their platform, including which pages they visit, what content they interact with, and how long they spend on the platform;

(3) Device information: When users access a social media platform, the social media network will gather information about the device, including the type of device, the operating system, and the IP address of the user's computer;

(4) Location data: Social media networks track users' location data through GPS, Wi-Fi, and cellular network signals;

(5) Third-party data: Social media networks collect data from third-party sources, such as advertisers or data brokers, to supplement the information they collect directly from users. This data is used by social media networks for a variety of purposes, including targeted advertising, content personalization, and improving user engagement.

This has raised concerns about users' privacy on social media networks. Numerous internet companies have been accused of violating users' privacy rights. To sue for invasion of privacy, a person must have a reasonable expectation of privacy in a particular situation. However, it is often difficult to

[28] Lee Rainie, "Americans' Complicated Feelings about Social Media in an Era of Privacy Concerns" (Pew Research Center, 27 March 2018) <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/> accessed 4th March 2023

[29] Fidler S and Wells G, "U.K. Lawmakers Rebuke Facebook in Call for Social-Media Regulation" (The Wall Street Journal, 17 February 2019) <https://www.wsj.com/articles/u-k-committee-rebukes-facebook-in-call-for-social-media-regulation-11550448060> accessed 5 May 2023

[30] Clayton J, "TikTok and WeChat: US to Ban App Downloads in 48 Hours" (BBC News, 18 September 2020) <https://www.bbc.com/news/technology-54205231> accessed 22 February 2023

[31] O'Brien M, "Judge Postpones Trump's TikTok Ban in Suit Brought by Users" (AP NEWS, 21 April 2021) <https://apnews.com/article/donald-trump-entertainment-pennsylvania-courts-3573972d3aa6bee78304e3195ffe4ade> accessed 24th March 2023

[32] Reuters, "US Navy Bans TikTok from Mobile Devices Saying It's a Cybersecurity Threat" (The Guardian, 21 December 2019) <http://www.theguardian.com/technology/2019/dec/21/us-navy-bans-tiktok-from-mobile-devices-saying-its-a-cybersecurity-threat> accessed 5th March 2023

[33] Mary Meisenzahl, "US Government Agencies Are Banning TikTok, the Social Media App Teens Are Obsessed with, over Cybersecurity Fears — Here's the Full List" (Business Insider, 26 February 2020) <https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2> accessed 4th April 2023

determine how much privacy can reasonably be expected on the internet, for instance, in the case of Campbell v. Facebook, Inc.[34]

Facebook, Inc., has over two billion active users. One of the functions that the platform offers is it allows users to send a private message, and only the sender and recipient can view the contents. Matthew Campbell, Anna St. John, and other users filed a suit in a federal district court against Facebook, alleging that the company routinely captured, read, and used links in the messages with the consent of the users and in violation of federal privacy law. After four mediation sessions, the parties reached to a settlement where Facebook promised to add a disclosure to the Help Centre page on its platform for a year, revealing that "we use tools to identify and store links shared in messages." The court concluded that the plaintiffs would not likely prevail if the case proceeded and approved the settlement. St. John appealed, arguing that the settlement was unfair because the plaintiffs received only worthless relief. Nonetheless, the US Court of Appeals for the Ninth Circuit affirmed the decision of the lower court.[35]

Through this case, we learned that it is undoubtedly that social media platforms have gathered the users' information and data, but as an individual, we cannot determine how much privacy can be expected once we send the messages or the materials online, which is a drawback of social media platforms.

However, social media can play a significant part in amplifying government surveillance by providing a wealth of data on users' activities and communications. Governments can use social media platforms to gather information on individuals and monitor their online behavior. This can include tracking social media posts, messages, and search history to identify potential threats or criminal activity.[36]

Moreover, governments can use social media platforms to conduct mass surveillance, where they monitor the online activities of many people.[37] This can involve using automated tools to analyze social media data and identify patterns or trends that could be of interest to law enforcement or intelligence agencies. In some cases, social media companies may also cooperate with government surveillance efforts.[38] For example, governments can request data from social media companies through subpoenas or other legal mechanisms.[39] In some cases, social media companies may be required by law to provide user data to government agencies.[40] Overall, the benefit of social media platforms by governments to conduct surveillance raises serious concerns regarding individuals' rights to privacy and other civil liberties. This underscores the need for enhanced transparency and accountability surrounding the data collecting and usage practices of social media corporations as well as governments worldwide.

The impact of Spyware on privacy rights

The right to assembly is a vital human right that enables individuals to gather peacefully and express their beliefs and opinions The use of social media networks and spyware can have significant human rights implications. Today, while online platforms have become a crucial instrument for organizing

[34] Campbell v. Facebook, Inc., No. 17-16873 (9th Cir. 2020)

[35] *Ibid.*

[36] Touma R, "TikTok Has Been Accused of 'Aggressive' Data Harvesting. Is Your Information at Risk?" (The Guardian, 19 July 2022) <https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk> accessed 10 th May 2023

[37] "Mass Surveillance" (Privacy International) <https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing.> accessed 10th March 2023

[38] H. Panduranga and EM. Pablo, "Federal Government Social Media Surveillance, Explained" (Brennan Center for Justice, January 7, 2022) <https://www.brennancenter.org/our-work/research-reports/federal-government-social-media-surveillance-explained> accessed 12th February 2023

[39] *ibid*

[40] Elliott V, "New Laws Requiring Social Media Platforms to Hire Local Staff Could Endanger Employees" (Rest of World, May 14, 2021) <https://restofworld.org/2021/social-media-laws-twitter-facebook/> accessed 10 March 2023

and mobilizing social and political movements, enabling people to connect and share information in real time, the right to privacy is being increasingly challenged by social media at the same time.

Social media networks gather huge amounts of private details from users, which can be forwarded to external parties and organizations without their consent. The term spyware refers to the type of software that is created to gather data and information from a computer or other electronic device without the permission or knowledge of the user.[41] In other words, spyware is designed to monitor a user's activity on their device, steal personal information, and violate their privacy. It is possible to install it on a device by a variety of different methods, such as by downloading a malicious attachment or software bundle, clicking on a link or pop-up ad, or through physical access to the device.[42] Once installed, spyware can operate in a variety of ways, including:

1. Keylogging: Spyware can record every keystroke made on the device, including passwords and other sensitive information.[43]
2. Screen capture: Spyware can take screenshots of the device's screen, allowing an attacker to monitor the user's activity.
3. Remote access: Spyware can allow attackers to remotely access and control the device, giving them access to sensitive files and data.
4. Data theft: Spyware can steal sensitive data from the device, such as login credentials, banking information, and personal files.[44]

Spyware, in general, conducts its activities in secret and might be difficult to identify without the aid of specialized tools. It has the potential to be utilized for a wide range of criminal activities, such as identity theft, fraud in financial transactions, and espionage. As such, it poses a significant threat to user privacy and security.

Here are some examples of governments using spyware to target journalists, activists, and political dissidents:

1. Pegasus spyware: Pegasus is a spyware developed by the Israeli cybersecurity firm NSO Group. It has been utilized by multiple government agencies to go after people working for human rights and political dissidents, as well as journalists. In 2021, it was revealed that the Indian government had used Pegasus to spy on opposition leaders, journalists, and human rights activists.[45]
2. FinFisher spyware: FinFisher is spyware developed by the UK-based Gamma Group. It has been used by multiple governments to target activists and dissidents. It was discovered in 2013 that the government of Bahrain had been spying on opposition activists using a program called FinFisher.[46]
3. Hacking Team spyware: Hacking Team was an Italian company specializing in providing governments with surveillance software. Its spyware has been utilized by a number of governments, to target journalists and activists. In 2015, it became public knowledge that the government of Ethiopia had employed the spyware developed by Hacking Team in order to spy on journalists and opposition activists.[47]

---

[41] "What Is Spyware?" (Kaspersky, n.d) <https://www.kaspersky.com/resource-center/threats/spyware> accessed 10 March 2023

[42] *ibid*

[43] "What Is Keystroke Logging and Keyloggers?" (Kaspersky, n.d) <https://www.kaspersky.com/resource-center/definitions/keylogger> accessed 12th March 2023

[44] "What Is Data Theft and How to Prevent It" (Kaspersky, 25 November 2021) <https://www.kaspersky.com/resource-center/threats/data-theft> accessed 12 March 2023

[45] Murali Krishnan, "Pegasus Snooping Controversy Rocks Indian Parliament as Opposition Cries Foul" (RFI, 5th February 2022) <https://www.rfi.fr/en/international/20220205-pegasus-snooping-controversy-rocks-indian-parliament-as-opposition-cries-foul> accessed 12th March 2023

[46] Jadaliyya Reports "UK Spyware in Bahrain: Company's Denials Called Into Question" (Jadaliyya, 6 February 2013) <https://www.jadaliyya.com/Details/27997> accessed 10th Feb 2023

[47] Bill Marczak, John Scott-Raiton and Sarah McKune, "Hacking Team Reloaded" (The Citizen Lab, 9 March 2015) <https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/> accessed on 12th March 2023

4. NSO Group's Pegasus: It was claimed in 2019 that the Mexican government has utilized Pegasus to target journalists, attorneys, and advocates for human rights.[48]

These examples highlight how governments can use spyware to target individuals who are critical to the government or who are engaged in activism or journalism. The use of spyware in this manner constitutes a significant violation of human rights and poses a threat to individuals' freedom of expression and privacy.[49] It can give a chilling effect on individuals, causing them to fear the consequences of speaking out or sharing information online. This can limit the diversity of voices and perspectives that are represented online, and further undermine the press as well as the freedom of expression.[50] Any attempt to restrict or censor online speech can have a significant impact on an individual's right to assembly, as social media is often the primary means of communication during protests and demonstrations.

Additionally, the use of spyware is often accompanied by other forms of harassment and intimidation, creating a fear and self-censorship atmosphere.[51] This indicates the need for greater regulation and oversight of the use of spyware by governments. The ethical implications of spyware and its impact on individual privacy include invasion of privacy, lack of consent, target surveillance, the misuse of power, unfair advantage, and threat to security.

Spyware can track keystrokes, capture screenshots, record browsing history, and even activate microphones and cameras to listen to conversations and watch activities.[52] To protect personal information and devices from unauthorized access, it is important to install security software, be cautious when downloading files or clicking on links, and keep devices updated with the latest security patches.[53]

The lack of consent in the installation and use of spyware on devices is a significant concern in terms of privacy and legality. When spyware is installed on a device, the user may not be aware of its presence or functionality. The stealthy installation of spyware may happen through a variety of methods, including deceptive emails or file-sharing networks.[54] This lack of informed consent not only undermines the principle of privacy but also raises questions about the legality of such practices. The installation of spyware without the user's consent violates privacy laws, as users have the absolute right to be aware of what data is being gathered and how it is being used.[55] Additionally, using spyware without consent can lead to collecting sensitive personal data, such as financial information, login credentials, and personal communications. This can be a serious problem. Identity theft, fraud in financial transactions, and other sorts of criminal activity are all potential outcomes of this.[56] Therefore, it is crucial to raise awareness of the dangers of spyware, establish and enforce laws and regulations that protect users from unauthorized installation and use of spyware, and to ensure that informed consent is always obtained before any data is collected.

---

[48] Stephanie Kirchgaessner, "Mexico: Reporters and Activists Hacked with NSO Spyware despite Assurances" (The Guardian, October 4, 2022) <https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus> accessed 12 March 2023

[49] "Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns" <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report&gt> accessed 10 March 2023

[50] Nyst C, "Two Sides of the Same Coin – the Right to Privacy and Freedom of Expression" (Privacy International, 7 October 2013) <http://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression> accessed 20th February 2023

[51] Boris Munoz, "Journalism in Latin America Is Under Attack by Spyware" (Wilson Center, 27 January 2023) <https://www.wilsoncenter.org/blog-post/journalism-latin-america-under-attack-spyware> accessed 20 February 2023

[52] Paahinath A., "What Is Spyware? Definition, Prevention and Removal Tips" (Cyberguardd, n.d) <https://www.cyberguardd.com/spyware> accessed 6th March 2023

[53] *ibid*

[54] "How To Recognize, Remove, and Avoid Malware" (Federal Trade Commission, 27 May 2021) <https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware> accessed 10 March 2023

[55] "Spyware and the Law" (SpamLaws, n.d) <https://www.spamlaws.com/spyware-laws.html> accessed 9 March 2023

[56] *ibid*

The use of spyware for targeted surveillance of specific individuals or groups has become increasingly prevalent in recent years. This type of surveillance allows for collecting sensitive information on individuals, which can be used to gain an advantage in legal, political, or financial matters. However, using spyware for targeted surveillance raises significant concerns about privacy and free speech.[57] Having the knowledge of being monitored may cause individuals to self-censor and avoid expressing their opinions or associating with like-minded people, which can restrict individuals' rights of privacy as well as their rights to freedom of expression.[58]

In addition, individuals may be targeted and monitored without any legal basis or procedural safeguards, which violates their right to due process. The lack of transparency and public oversight surrounding these practices can make it difficult for individuals to challenge unlawful or unfair surveillance practices and access legal remedies. The fear of being under surveillance can create a chilling effect on individuals' free speech, political dissent, and other forms of expression.[59] The targeted individual may feel intimidated and pressured to conform to the norms or opinions of the surveillance agency, which undermines the principles of democracy and human rights.[60] Additionally, using spyware for targeted surveillance without due process or legal justification violates the right to privacy, and the collected data may be used to discriminate against or harm the targeted individual.[61] Therefore, it is essential to establish legal and ethical guidelines for using spyware in targeted surveillance to ensure that it is only used for legitimate purposes and is in line with the principles of human rights and privacy.[62]

The misuse of power occurs when governments or other entities that use spyware intentionally abuse their authority by targeting individuals for surveillance and monitoring. This type of behavior is often carried out without just cause or lawful authority. It can be used to intimidate, manipulate or control individuals who are not suspected of any wrongdoing. Misuse of power can also have a serious effect on free speech and other fundamental human rights, as it creates an atmosphere of fear and uncertainty that can discourage people from speaking out against injustices or abuses of power.[63] Additionally, government surveillance and monitoring of social media can further restrict the right to assembly, leading to the identification and targeting of protesters.[64] To protect the right to assembly in this modern age of information technology, it is essential to defend freedom of expression, advocate for stronger legal protections, and support the development of secure communication technologies. Therefore, it is essential to monitor the use of spyware and ensure that it is only used for legitimate purposes and within the confines of the law.

The use of spyware can provide an unfair advantage to one party, particularly in cases where businesses use it to gather competitive intelligence. This can lead to unethical practices and unfair competition, as the company using the spyware may not be competing on a level playing field.[65] Additionally, the use of spyware can harm consumers and the overall economy by allowing companies to manipulate prices and decrease competition.[66] To prevent these negative consequences, it is

---

[57] "Stop Governments Spying on Activists" (Amnesty International, 6 October 2020) <https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/> accessed 20th March 2023

[58] *ibid*

[59] Karen Gullo, "Surveillance Chills Speech—As New Studies Show—And Free Association Suffers" (Electronic Frontier Foundation, 19 May 2016) <https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association> accessed 30th March 2023

[60] *ibid*

[61] Lee and Caitlin Chin NT, "Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color" (Brookings, 7 April 2022) <https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/> accessed 30th March 2023

[62] *Ibid.*

[63] *ibid*

[64] Benedek W and Kettemann MC, Freedom of Expression and the Internet (Council of Europe Publishing, 2013) 6

[65] *ibid*

[66] U.S. Senate. Committee on Commerce, Science and Transportation. *Impact and Policy Implications of Spyware on Consumers and Businesses* (Senate Hearing, 110-1178, 11 June 2008)

essential to use technology ethically and responsibly and adhere to established laws and regulations governing the use of spyware.

The use of spyware can pose a significant security threat by surreptitiously collecting personal information and potentially granting unauthorized access to sensitive data.[67] Such information can be used for identity theft, fraud, or espionage, compromising personal, organizational, and national security. To prevent the installation of spyware, individuals, and organizations must use anti-malware software, keep systems up-to-date, and exercise caution when downloading software. Additionally, organizations must implement strict cybersecurity protocols and policies and train employees on proper cybersecurity practices to safeguard against potential attacks. [68]

Overall, the human rights implications of social media networks and spyware are complex and multifaceted. It is vital for all individuals and organizations to be aware of these implications and to take necessary precautions to preserve their privacy, freedom of expression, and other fundamental rights in the age of advanced technology. It is also vital for governments and other entities to guarantee that the use of social media networks and spyware are subject to appropriate regulation and oversight to hinder abuses and preserve human rights.

Potential solutions to protect privacy rights.

Regulatory measures and government action can play an essential part in protecting privacy rights and promoting responsible data practices. Here are some examples:

1. Data protection laws and regulations: Governments all around the globe have implemented laws and regulations to protect individuals' privacy and regulate the collection, use, and disclosure of personal information. For instance, the European Union's General Data Protection Regulation (GDPR) provides a comprehensive framework for data protection[69], while the California Consumer Privacy Act (CCPA) requires companies to disclose how they collect and use consumers' personal information.[70]
2. Enforcement actions: Governments can take enforcement actions against companies that violate data protection laws or engage in other privacy violations. For example, in 2019, the U.S. Federal Trade Commission (FTC) fined Facebook $5 billion for privacy violations related to the Cambridge Analytica scandal.[71]
3. Transparency and accountability measures: Governments can require companies to be transparent about their data collection and use practices and hold them accountable for any violations. For instance, the GDPR requires companies to provide individuals with clear and understandable information about their data collection and use practices and allows individuals to request access to and deletion of their personal information.[72]
4. International cooperation: Governments can work together to develop common standards and best practices for data protection and privacy. For example, the Organization for Economic Cooperation and Development (OECD) has developed guidelines for data protection that have been adopted by many countries around the world.
5. Public awareness campaigns: Governments can launch public awareness campaigns to educate individuals about privacy risks and best practices for protecting their personal information. For

<https://www.govinfo.gov/content/pkg/CHRG-110shrg76328/html/CHRG-110shrg76328.htm> accessed 10th March 2023

[67] "What Is Spyware | Spyware Removal and Protection | Malwarebytes" (Malwarebytes, n.d) <https://www.malwarebytes.com/spyware> accessed 19 Jan.2023

[68] *Ibid.*

[69] Wolford B, "What Is GDPR, the EU's New Data Protection Law? - GDPR.Eu" (GDPR.eu, November 7, 2018) <https://gdpr.eu/what-is-gdpr/> accessed 7th April 2023

[70] "California Consumer Privacy Act (CCPA)" (State of California - Department of Justice - Office of the Attorney General, 15 October 2018)

[71] "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (Federal Trade Commission, 24 July 2019) <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook> accessed 22 February 2023

[72] Wolford B, "A Guide to GDPR Data Privacy Requirements - GDPR.Eu" (GDPR.eu, 22 February 2019) <https://gdpr.eu/data-privacy/> accessed 20 February 2023

instance, the U.S. National Cyber Security Alliance runs the "Stop. Think. Connect." campaign, which aims to promote safe and responsible use of the internet.[73]

By implementing these regulatory measures and government actions, governments can help protect individuals' privacy rights and promote responsible data practices in the digital age.

Ethical guidelines for tech companies are designed to promote responsible and ethical use of technology and to ensure that companies prioritize the interests of users, customers, and society. In the digital age, privacy and data protection are crucial issues as users increasingly share personal information online. Tech companies have a responsibility to prioritize privacy and implement robust measures to protect users' personal information. This involves giving information that is both clear and transparent concerning the procedures of data collection and use, as well as giving users control over their private details through mechanisms such as privacy settings.[74] By prioritizing privacy and data protection, tech companies can ensure that users' privacy is respected, and their personal information is safeguarded.

Tech companies should be transparent and accountable for their actions and products, including their decision-making processes and any negative impacts on users or society.[75] This requires clear and accessible information about algorithms and data collection, as well as taking responsibility for mitigating harms and engaging with stakeholders to address concerns.[76] By prioritizing transparency and accountability, companies can build trust with users and promote ethical behavior in the tech industry.

Tech companies have a responsibility to prioritize social impact and act with responsibility by considering the potential risks and benefits of their products or services on users, customers, and society.[77] This involves anticipating any unintended negative consequences, such as harm to privacy, health, or well-being, and taking steps to mitigate them. In addition, companies should strive to create positive social impact, such as addressing social or environmental challenges.[78] By prioritizing responsibility and impact, tech companies can build trust with their users and contribute to creating a more equitable society.

Tech companies must prioritize diversity and inclusion to create equitable and inclusive tech ecosystems that cater to the needs of all users.[79] To achieve this, companies must cultivate inclusive workplaces that value diversity and implement policies that provide equal opportunities for all employees.[80] They must also ensure that their products and services are accessible and usable for all users, regardless of race, gender, or other characteristics. Companies should be aware of and address

---

[73] Stop. Think. Connect., is a national public education campaign to raise awareness about cybersecurity, ultimately increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.
"About Stop. Think. Connect." (stopthinkconnect, n.d.) < https://www.stopthinkconnect.org/about> accessed 3rd March 2023.

[74] Venky Anant, Lisa Donchak, James Kaplan and Henning Soller, "The Consumer-Data Opportunity and the Privacy Imperative" (McKinsey & Company, 27 April 2020) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative> accessed 10 February 2023

[75] Brian Fishman, "What It Means to 'Hold Big Tech Accountable'" (Lawfare, 16 September 2022) <https://www.lawfareblog.com/what-it-really-means-hold-big-tech-accountable> accessed 25 March 2023

[76] "Requirements of Trustworthy AI - FUTURIUM - European Commission" (FUTURIUM - European Commission, April 8, 2019) <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1> accessed 16 March 2023

[77] Chastity Heyward, "Council Post: The Growing Importance Of Social Responsibility In Business" (Forbes, 18 November 2020) <https://www.forbes.com/sites/forbesbusinesscouncil/2020/11/18/the-growing-importance-of-social-responsibility-in-business/> accessed 20 February 2023

[78] "What Are Social Impact Companies and Why Do They Matter? | CauseLabs" (CauseLabs, March 12, 2019) <https://www.causelabs.com/post/what-are-social-impact-companies-and-why-do-they-matter/> accessed 24th March 2023

[79] Shanis Windland, "Building a More Diverse, Equitable, and Inclusive Technology Ecosystem" (Power of Partnership, 22 October 2021) <https://blogs.vmware.com/partner/2021/10/building-a-more-diverse-equitable-and-inclusive-technology-ecosystem.html> accessed 5th March 2023

[80] *ibid*

potential biases in their products and services, and engage with a variety of stakeholders to ensure inclusivity and equity.[81] By prioritizing diversity and inclusion, tech companies can contribute to a more just and inclusive society.

Tech companies must prioritize ethical design and development practices to ensure that their products and services align with social values and priorities. This involves considering the potential unintended consequences of new technologies and taking steps to mitigate any negative impacts on users, customers, and society. Companies should engage with stakeholders and users, conduct ethical assessments, and monitor their products and services to ensure they remain aligned with social values and priorities. Moreover, they should be transparent about their development processes and decision-making systems and provide clear explanations for any decisions that impact users.[82] By adopting ethical design and development practices, tech companies can build trust with their users and contribute to creating a more just and equitable society. By following these ethical guidelines, tech companies can promote responsible and ethical use of technology and can help ensure that their products and services prioritize the interests of users, customers, and society.

CONCLUSION

In conclusion, social media networks and spyware have become ubiquitous in our lives and have significant impacts on human rights, especially the right to privacy. The rise of social media networks has brought new challenges to protecting privacy, and the use of spyware by governments and other entities raises serious concerns about surveillance and privacy violations. We must continue to critically examine the impact of social media networks and spyware on human rights and take steps to protect privacy and ensure accountability for those who violate these rights. To accomplish this, it will be necessary for governments, civic society, and the corporate sector to work together to formulate and implement legal and ethical guidelines for the application of these technologies. In the end, we need to strike a balance and a just medium between the benefits of new technologies and the requirement to defend human rights, particularly the right to privacy, to create a society that is more just and equal.

Individuals can take various steps to protect their online privacy. First, educating oneself on online privacy risks is crucial. It is essential to read up on privacy policies and understand the categories of data that companies gather and how they use it. By doing so, one can become more conscious of how their private details are being used and take appropriate steps to protect them.[83] Another step individuals can take to protect their online privacy is to use privacy-focused tools and services. VPNs can encrypt internet connections and hide IP addresses. Privacy browsers can block tracking scripts and ads. Encrypted messaging apps can secure conversations.[84]

Limiting personal information sharing is also an essential aspect of protecting online privacy. Individuals should be cautious when disclosing personal information online and restrict the amount of such information shared on social media. Posting sensitive information, such as phone numbers, addresses, and birthdates, can be used to identify individuals.[85] Using strong passwords is another key step in protecting online privacy. Individuals should protect their online accounts with passwords that are both strong and unique, and whenever it is practicable, they should use two-factor authentication.

---

[81] Donnebra McClendon, "How to Promote Diversity, Equity, and Inclusion in the Workplace" (Ceridian, 21 June 2022) <https://www.ceridian.com/blog/support-diversity-and-inclusion-in-the-workplace> accessed 5th March 2023

[82] Omer Yetimoglu, "The Impact of Diversity and Inclusion in Tech" (LinkedIn, 8 March 2023) <https://www.linkedin.com/pulse/impact-diversity-inclusion-tech-%C3%B6mer-yetimoglu> accessed 22nd March 2023

[83] "Data Privacy Policy: What It Is & Why You Need One" (Segment, n.d) < https://segment.com/product/privacy-portal/> accessed 5 March 2023

[84] Aliza Vigderman and Gabe Turner "Do VPNs Hide Search & Browsing History?" (Security, 20 January 2023) <https://www.security.org/vpn/browsing-history/> accessed 15th March 2023

[85] "What Is Online Privacy? Full Guide & Expert Tips" (Bitdefender, n.d) <https://www.bitdefender.com/cyberpedia/what-is-online-privacy/> accessed 5 March 2023

This can help prevent hackers from accessing accounts and stealing personal information.[86] Lastly, individuals must keep their software, operating system, and security software up to date.[87] This ensures that individuals have the latest security patches and protections. Hackers continually find new vulnerabilities, and software companies release updates regularly to address these issues. By staying up-to-date, individuals can protect themselves from potential security threats.[88]

Organizations can also take steps to protect user privacy. First, it is essential to establish clear and transparent privacy policies for how user data is collected, used, and shared. This information should be easily accessible to users, and any changes to the policies should be communicated effectively.[89] Conducting regular privacy assessments is another critical step for organizations.[90] These assessments can identify potential privacy risks and vulnerabilities and help organizations take proactive steps to address them.[91] Organizations should assess their data collection practices, data storage and handling practices, and data sharing practices.[92] Using encryption is another crucial aspect of protecting user data. Encryption can be used to protect user data, both in transit and at rest.[93] This can include encrypting data that is being transmitted over the internet and data that is stored on servers.[94] Training employees on privacy best practices is also important for protecting user privacy. Organizations should establish procedures for responding to privacy incidents and make sure that staff are aware of their duties and the obligations that come with them regarding the protection of user data.[95] This can include regular training on privacy policies and procedures, as well as monitoring and auditing of employee actions.[96]

Policymakers also have an essential part to play in protecting user privacy. One critical step is to enact privacy legislation that protects user privacy and establishes clear guidelines for data collection, use, and sharing.[97] This legislation should provide clear rules for companies regarding user data, including what data can be collected, how it can be used, and when it can be shared.[98] Increasing transparency is another important aspect of protecting user privacy.[99] Policymakers can increase transparency about how user data is collected, used, and shared, and provide users with greater control over their data.[100] This can include requiring companies to disclose the data they collect and provide users with clear information about how that data is used.[101] Regulating the use

[86] "Internet Safety: Creating Strong Passwords" (GCFGlobal, n.d) <https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/> accessed 17th March 2023

[87] "Keeping Devices and Software up to Date" (NCSC, n.d) <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date> accessed 15 March 2023

[88] *Ibid.*

[89] Timothy Morey, Theodore Forbath and Allison Schoop, "Customer Data: Designing for Transparency and Trust" (Harvard Business Review, May 2015) <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust> accessed 5th March 2023

[90] "5-Step Security Assessment Process | HackerOne" (HackerOne, n.d) <https://www.hackerone.com/knowledge-center/5-step-security-assessment-process> accessed 5 March 2023

[91] *ibid*

[92] "Data Collection Best Practices" (Rudderstack, n.d) <https://www.rudderstack.com/learn/data-collection/data-collection-best-practices/> accessed 5 March 2023

[93] Chen S, "What Is Data Encryption and Why Is It Important? - TitanFile" (TitanFile, 13 June 2022) <https://www.titanfile.com/blog/what-is-data-encryption-and-why-is-it-important/> accessed 10 March 2023

[94] *ibid*

[95] Sultan SA, "Privacy Training: Why Is It Required for Employees? - Securiti" (Security, 18 January 2023) <https://securiti.ai/blog/privacy-training/> accessed 5th March 2023

[96] *ibid*

[97] "What Is Data Privacy? Definition and Compliance Guide" (Talend, n.d) <https://www.talend.com/resources/data-privacy/> accessed 15th March 2023

[98] *ibid*

[99] Chiara Saullo, "Privacy Transparency Is an Opportunity, Not a Burden: Here's Why" (blog, 12 August 2021) <https://blog.didomi.io/en/privacy-transparency-opportunity-not-a-burden> accessed 5 March 2023

[100] *ibid*

[101] *ibid*

of surveillance technologies, such as spyware, is also important for protecting individual privacy.[102] Policymakers can establish clear rules for the use of surveillance technologies, including what types of technologies can be used, how they can be used, and when they can be used.[103] Collaborating with tech companies is another critical step for policymakers. By working with tech companies, policymakers can develop responsible privacy practices and ensure that technology is used ethically and responsibly.[104] This collaboration can include developing standards for data collection, use, and sharing, as well as establishing best practices for protecting user privacy.[105] By following these recommendations, individuals, organizations, and policymakers can help protect privacy rights and ensure that technology is applied in a way that is both responsible and ethical. By staying informed, advocating for privacy rights, supporting privacy-focused organizations, protecting your privacy, and spreading the word, you can help raise awareness and promote engagement on the issue of social media networks, spyware, and privacy.

[102] "Highly Intrusive Spyware Threatens the Essence of Human Rights - Commissioner for Human Rights - Public.Coe.Int" (Commissioner for Human Rights, 27 January 2023) <https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights> accessed 5 March 2023

[103] Erin Simpson and Adam Conner, "How To Regulate Tech: A Technology Policy Framework for Online Services" (Center for American Progress, November 16, 2021) <https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/> accessed 5 March 2023

[104] Lillian Ablon and Andrea Golay, "How the 'Wonks' of Public Policy and the 'Geeks' of Tech Can Get Together" (TechCrunch, 18 March 2016) <https://techcrunch.com/2016/03/17/how-the-wonks-of-public-policy-and-the-geeks-of-tech-can-get-together/> accessed 7th March 2023

[105] Tom Ovington, "Policy Makers Focus on Big Tech" (Frontier Economics, n.d) <https://www.frontier-economics.com/uk/en/news-and-articles/articles/article-i7098-policy-makers-focus-on-big-tech/> accessed 5 March 2023