Privacy on social media
Violations and Means of Protection

Skyline International Foundation for Human Rights

August 2021

www.skylineforhuman.org
info@skylineforhuman.org

Introduction :

Currently, the world is witnessing a rapid evolution process in communication technology in terms of quantity, quality, and access to information. The revolution of modern communications technology has had its impacts in all sectors and institutions. As a result, many vital sectors witnessed a radical transformation; despite using traditional channels, they have become more flexible, accessible, more intelligent, and widespread.
The world is competing to access information and find rapid means to convey and analyze it to make decisions based on accuracy and analysis.

In this regard, a new concept emerged called “the communications technology revolution,” which contributes significantly to the emergence of globalization, including the world’s economies, during the past two decades. Social networking sites are one of the most prominent developments of modern technology.

Those who run these sites seek to play a dual role. The first role is to operate these platforms and provide various services to users. The second role is to collect and store data of a personal nature for the user, such as posts and comments on social media, social and personal political tendencies, electronic communications, and all the information that users put on their profiles for a variety of economic and political considerations.

It has become effortless to access personal data through phones, computers connected to the Internet through specific applications. Accordingly, individuals can be easily tracked through their digital data. Thus, we can say that online privacy has become fictional and impossible to maintain.

In this report, “Skyline International for Human Rights” will shed light on the issues spiked by individuals ’interaction on social networking sites and the risks that threaten the privacy of their data in light of the escalating violations and daily intrusion of personal data. Therefore, it requires reviewing existed legal terms and laws to find out the challenges created by modern means of communication and what should be done to protect personal data and private information from abuse by governments, spying companies, and social networking sites.

Skyline International for human rights

User privacy in the digital world: concept and context:

The development of any new technology always creates different results and concerns that may be legal, which significantly affect the trust between users and owners. Among those issues that have steadily increased is privacy in social media. Discussions about violating users 'privacy by social media companies recently spiked.

Thus, it becomes clear that these sites have changed from social platforms presenting opinions, ideas, and trends to platforms enabling any user to violate another user's privacy by spending a few moments accessing his profile on those platforms.

It's essential to understand the violations introduced in this report, to define the concept of privacy. "**Privacy** is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others." privacy is a right exercised by the individual to limit the knowledge of others about aspects of his life, which could be ideas or personal data.

Privacy can also be defined as "the protection of an individual's personal data, which is published and conveyed through digital media," such as "e-mail, bank accounts, personal photos, information about work and residence and all the data that we use in our interaction on the Internet while using a computer, mobile phone, smartphone, or electronic tablet...etc.

What does privacy mean in social media networks?

Privacy in social networking sites means "the right of the user to decide for himself when, how and to what extent his information may reach other users or those responsible for it." Thus, it is clear that every individual has the right to be protected from interfering in his affairs. He also has the right to freely choose the means by which he expresses himself, his desires, and his actions to others.

In this context, privacy in social media networks is related to the confidentiality of their users 'private lives and data. Whether these data are facts or information stored in computers, smartphones, or social networks, the user subscribes to, such as Facebook, Twitter, Instagram, Gmail, and other platforms.

The protection of privacy in social media is limited to the right of a person to control his personal information. However, it is one of the essential concepts that all systems

and laws protecting informational privacy require. Accordingly, the protection of informational privacy is the protection of individuals 'data who use those sites.

Social media is a must.

Social media has become a preferred tool of communication for individuals in light of the communication technological developments. Individuals tend to use social media platforms due to the ease and quick communication and sharing of ideas, information, and data.

Social networking sites have effectively provided the leading platform for political and social discussions. Arab countries and even Europe have used these sites to deliberately convey their ideas and aspirations to change their countries 'political and social conditions. These sites provided the appropriate environment in the outbreak of the Arab Spring in Tunisia, Egypt, Libya, Yemen, and the rest of the countries. Moreover, social networking sites helped address many European countries 'issues, such as racism and hatred against migrants and refugees.

Social media networks did not only trigger the Arab Spring revolution but also extended and became a powerful platform and an essential source for people and those interested in political affairs in most countries of the world. Many individuals start depending on social

media platforms to know the course of events and convey news, especially the practices of many dictatorial governments. which, in turn, sought to silence them by monitoring social media, restricting the publication policy, and setting punishments if they publish content that contradicts the "policies of governments."

The user's private life and digital threats.

Here, we should distinguish between privacy and security. Breaches in security generally concern unauthorized access by non-accredited persons to secure coding or written language. For example, a social network can fall victim to hacking, computer viruses, or a worm. But if no exploitation of users 'personal information arises from the attack, there is no loss of privacy.

Loss of privacy involves unwarranted access to private information, not necessarily due to a breach in security. For example, some social networking sites — to whom users have consented to give ownership of their personal data — may have subsequently supplied them to academic researchers and marketing companies.

According to the United Nations Interregional Crime and Justice Research Institute (UNICRI), the value of stolen personal data depends mainly on the country of residence. In March 2010, a set of personal data cost around USD 7 on the global black market. Therefore, the value to a cybercriminal of the personal data held by a social network with millions of members would be immense.

According to some ICT industry experts, the possible harm to individual users from unauthorized access to data depends on how much a user engages in a social networking site and the amount of information a user has been willing to share. Many people consider that it is up to users to take responsibility for their information about themselves.

Finally, it is well known that social networks are one of the attractive ways to breach the privacy and security of individuals, especially with the spread of spying companies that sell tracking and hacking programs that become disturbingly and widely used nowadays. The companies have advanced technology that enables them to reach much information and violate the privacy of individuals on several levels, including:

1. **Individual privacy.**
   This model is specifically concerned with the privacy of the individual. It relates to the person himself and belongs to his entity as a human being, such as name, address, phone number, and other information. Therefore, it is inherent data for every identified or identifiable person. At present, this type of data has become of great

   importance due to the contemporary information philosophy, especially since the digital world cannot proceed in development and keep pace with human interests only by using information. A personal privacy model has emerged from this, which is genuinely concerned with the person's right to control his information.

2. **Privacy of personal behavior.**
This model relates to all behavioral aspects: political activities, religious beliefs, social practices of values, customs, traditions, and principles, whether in private or public places and may be referred to by "means of privacy."

3. **Privacy of personal communications.**
This model relates to personal communications, such as conversations, telephone correspondence, e-mail, and others, which are human life matters and which no one may view or record. Thus, eavesdropping on them is an attack on private life and a violation of its privacy, whether published or not.

4. **Privacy of personal information.**
This model includes the rules that govern all private data management, such as identity card information, credit card information, financial information, and others.

5. **Location privacy.**
This model relates to the rules regulating entry into homes, the work environment, or public places, including electronic inspection and control. Also, the spatial privacy of users of social networking sites is represented in information about the locations and movements of these users. The user may provide the site with this informatio6n by writing it down on the environment and tourism bulletins. Therefore, it is essential to know the user's destination and the location of his computer or smartphone.

Recent spying scandals.

Recently, there has been disturbing news about the use of Israeli spyware known as "Pegasus", which was produced by the Israeli company NSO Group. This company has sold the license to operate this software to several states and parties, including four Arab states, Saudi Arabia, UAE, Bahrain, and Morocco, that are using Pegasus to spy on dissidents, journalists, and human rights activists.

The findings of the recently published investigation, which more than 17 international media organizations carried out, reflect a real threat to a wide range of people, mainly as these spying operations planned to target the phones of more than 50,000. Moreover, the espionage operations include over 180 journalists from news agencies: the Wall Street Journal, CNN, The New York Times, Al Jazeera, Reuters, El Pais, Associated Press, etc.

This scandal raises real fears that espionage operations mainly aim to collect information from agencies and people who defend human rights globally, especially in conflict zones. For its part, Skyline International for Human Rights sent a joint letter to a group of rapporteurs

and international people to condemn and take direct action against states that used the Israeli surveillance company NSO Group's spyware, Pegasus targeted activists, journalists, and academics. It further stressed the need to open a serious investigation into the information that has been published and the danger it poses to those individuals.

In this context, Forbes magazine revealed the activity of a new spyware Israeli company called" Paragon solutions," which specializes in collecting data and hacking encrypted smartphones apps. Despite the lack of information about this company, some information was collected by journalists, although the company does not have a website. According to this research, the company was established in 2019, and it is based in "Tel Aviv." However, the company is still stealthy and has not announced its activities, locations, and employees.

Paragon company claims to give police the power to break into encrypted instant messaging communications remotely, whether WhatsApp, Signal, Facebook Messenger, or Gmail. One other spyware industry executive said it also promises to get longer-lasting access to a device, even when it's rebooted.

How should we act to counter privacy threats?

The biggest challenge facing the right to privacy in the digital age is the apparent absence of any binding legal rules in this area. In this context, we can say that international laws and regulations regarding the right to privacy have broadly protected privacy. Still, they did not address technological development problems and their impacts on privacy.
The continuing development of the information revolution has led to new dimensions and problems in private life on the Internet. Indeed, technological progress has enabled the development and promotion of new devices of hearing, eavesdropping, espionage, and imaging, which become a threat and an attack on privacy.

From this perspective, privacy has become threatened. Personal data has become a material used commercially for marketing advertisements, monitored by government agencies, or subjected to hacking for purposes harmful to its owners. Although safeguarding digital privacy from breaches is a recent issue, the relevant legal frameworks have not evolved accordingly, and it should be updated to tackle such abuses.

Also, addressing privacy invasion is very complicated for the user as social networking sites increased their interference in the online content in cooperation with some countries - known for their suppression of freedom of opinion and expression. Social networking sites provide these countries with the appropriate tools to pursue activists, opponents, and journalists.

With the aid of social media, authoritarian governments can delete their opponents' publications, restrict access to their accounts, track their activities, and even close their pages permanently, under the pretext that their publications threaten public order and stability in the country. Such practices have become a real threat to individuals' right to freedom of expression.

All these data assure the need to end the dominance of social networking sites and the absence of real international oversight by the relevant UN agencies. Thus, the concerned parties should enact effective laws against recent hacking and espionage developments and operations and regulate access to private information. Furthermore, they should design binding and restrictive laws for social networks' powers to access users' personal and private information.

Laws and conventions:

In general, human rights international conventions and agreements have expressed the commitment of states to respect the privacy of individuals. This commitment is evident when we review the internal texts of States and their amendments according to the provisions of international charters and agreements to which the state is a party. Moreover, it is common now that some provisions of charters and agreements have been promoted and become customary rules, which means that states shall abide by them even if they are not signatories to them.

The most prominent of these covenants is the Universal Declaration of Human Rights, which stipulates in its Article 12 "no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 17 of the International Covenant on Civil and Political Rights stipules "no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

The European Convention on Human Rights also emphasized in its Article 18 the importance of preserving the public and personal rights and freedoms of European citizens, prohibiting the infringement of the sanctity of private life, determining the right of individuals to privacy by respecting their private and family life, home and correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law.

Article 11 of the American Convention on Human Rights also stipulates: "Everyone has the right to have his honor respected and his dignity recognized. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. And if there is interference

or aggression, the law protects it. Everyone has the right to the protection of the law against such interference or attacks."

As the European conventions, the American convention protected the American citizen's right directly, differentiated between private life and the right to honor and consideration, and called for ensuring the obligatory implementation of these rights through the two official bodies for this purpose.

Conclusion:

The rapid development in information technologies has eased the ability to generate, collect, analyze and store information compared to previous times. This phenomenon prompts advocacy to set up legislation to keep pace with these capabilities to control the dissemination and exchange of information. Therefore, it is essential to do a legal review that includes issuing new legislation to limit and define social media companies' power to control individuals' online content.

The international community should combine forces to protect social media users' information and data from being monitored and used without their consent. It is also essential to stipulate deterrent penalties for social media companies that violate their users' rights.

Moreover, all relevant stakeholders, including states, civil society, human rights organizations, the scientific community, businesses, and scholars, should effectively address challenges to the right to privacy, notably in an era that is dominated by modern communication technology.

All parties should form a common basis to protect individuals' rights and establish real mechanisms to confront spying companies' threats. They should develop a clear strategy in dealing with the privacy and confidentiality of individuals' information at several levels. Additionally, all concerned parties should exert more effort to ensure individuals' legal rights legally in case they are violated, by any party, whether countries or spying companies.