Mechanisms and controls for monitoring social networking sites

Skyline International Foundation for Human Rights

December-2022

Introduction:

The new challenge in the world is the rapid access to information. 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.

These technological developments in the field of communication include social networking websites. The operators of these websites try 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 users' personal data, such as posts and comments on social media, social and personal political tendencies, electronic communications, and any information that users enter into their profiles for various 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.

The rise and global proliferation of social networking sites has been associated with strengthening the values of freedom, communication, and freedom of expression, particularly when used to support dissident and protest movements, disseminate information, break censorship regulations, expose corruption practices, and for other purposes that have made it possible to speak of "surveillance of social media content is a cause for concern"

On the other hand, some believe that such monitoring has become urgent given the illegal use of these networks for smuggling, fraud, slander, and the spread of rumors, as well as their use by terrorist movements for propaganda and recruitment purposes. This requires refuting the idea of monitoring the content of social networks and acts of espionage, persecution and targeted attacks, as well as the necessary controls to prevent such monitoring from being used for repression under the pretext of protecting security and stability.

In its recent report, Skyline seeks to shed more light on the oversight controls on social networking sites, their types, and the restrictions imposed on users without violating their privacy and their right to protect their data and activities through these sitemar

Oversight levels

Although the term "monitoring" is associated with government and security agencies, there are actually multiple levels of monitoring of content on social media sites, from the administrators of those sites themselves to the users who are able to report content that they think is harmful or that they do not want for certain reasons. They define it, and then the surveillance practiced by external governmental or non-governmental parties for various political, security, economic, and social goals.

Social media networks' moderators have wide powers over the content published through their users' pages and accounts. They exercise this control in accordance with the terms of use, which are mandatory and must be approved in advance, and which in turn vary from website to another, but they generally agree on the right to review the content and reject or delete it. Any content or accounts that violate their current or future policies will be deleted without prior notice.

Meanwhile, there are other levels of oversight at involve third parties involved in monitoring and tracking published content that are not limited to security agencies. Local and international institutions are establishing departments, observatories, and teams dedicated to monitoring communications content, i.e., tracking, observing, and analyzing trends.

Social institutions such as schools monitor student Internet use, including social networking sites, using well-known applications such as CompuGuardian and Gaggle, which are also plagued with some violations and abuses. According to a report by the U.S. National Coalition Against Censorship (NACA), they have used these tools to suppress student surveillance abuses.

Companies and business entities also use applications and software to monitor social media content to know the trends, opinions, and discussions that affect the spread of their products and image, such as Snaptrends applications, especially since the information spread affects market trends.

State control/Oversight

Although there are many parties that "control" the content of social networks using the terms surveillance, tracking, and analysis, the surveillance practiced by governments raises controversy about its goals, legitimacy, and controls. This is due to the use of spyware to hack these sites to obtain personal information that violates the rights and privacy of individuals without oversight or judicial authorization.

Several practices can be identified that countries use to monitor social media content, some of which are legitimate, while others are considered unlawful , most notably:

1- **Establishment of observatories and follow-up units**: Both security and non-security agencies are interested in monitoring social media to identify trends in public opinion or respond to rumors and to track illegal activities (such as terrorist propaganda, fraud, etc.). An example of such units is the Observatory for Extremist Fatwas, established by the Egyptian Dar al-Iftaa to track and respond to these extremist fatwas and opinions.

2- **Use of content monitoring techniques**: These are technical solutions and services provided by technology consulting firms that monitor data-mining content on social media, collect information across different platforms, analyze this material, and extract indicators from it instantly and automatically using text analytics engines. .

Although it is lawful to collect public data that individuals post on their accounts, these applications are greatly expanded by the government and are suspected of discrimination because they focus on monitoring a particular group or sector or members of a particular movement, which may violate constitutional rights or legal norms.

A study by the Brennan Center for Justice at New York College of Law found that cities, counties, and law enforcement agencies in the United States spend $5.7 billion on social media surveillance technology to track and archive information and activities of millions of users. Such as the Department of Justice and police in Oakland, California, monitoring prominent figures in the Black Lives Matter movement on Twitter.

3- **Concluding agreements with social media companies:** One of the most well-known practices in this regard is the U.S. Combat Terrorist Use of Social Media Act of 2015, passed on December 16, 2015, which gives the U.S. government the authority to monitor this content and enter into information access agreements with the companies that own these sites.

4- **Requests for disclosure of data**: Governments submit requests to social media administrations to disclose user data or specific pages for security or law enforcement reasons. These requests are made by executive bodies or on the basis of court decisions

The transparency reports of worldwide website administrations publish the statistics on these requests. For example, Google disclosed that in 2021 alone it received 70,943 requests from governments, covering about 77,000 accounts and users around the world, and that it also received 4,931 requests from governments to remove content, 62% of which came from them. Non-judicial executive bodies, from July to December 2021, and these requests were for the deletion of 27,000 items, including 6,144 videos on YouTube and 3,808 posts.

5- **Use of Reporting Procedures:** By using the option to notify the website administration of content that violates its policies and then delete it. Although this feature is primarily intended for users, there are allegations that governments use it to delete unwanted content, through the so-called electronic committees that launch massive reporting attacks against a particular account, page or post. There is also software that can perform this task electronically.

6- **Spy and hacking software:** This is hacking software obtained by some governments and security agencies to spy on users, which violates the individual's right to privacy, and whose disclosure is tantamount to a scandal for these agencies.

One of the most sensational incidents in this area is the disturbing news in recent months about the spying on journalists, human rights activists, and dissidents by an Israeli spying program called "Pegasus," developed by the Israeli company NSO, in several countries and destinations, including four Arab countries, namely Saudi Arabia, the Emirates, Bahrain, and Morocco.

The investigation published at the time, conducted by more than 17 international media organizations, concluded that these spying operations targeted the phones of more than 50.000 people. These operations included more than 180 journalists from news agencies: the Wall Street Journal, CNN and New York Times, Al Jazeera, Reuters, El Pais, Associated Press, and other media agencies. This raises concerns that the spying operations were mainly aimed at gathering information on agencies and individuals reporting on and defending human rights in the world, especially in conflict zones.

7- **Complete and partial blocking:** this measure represents the strictest level of censorship of social networks sites , whether through a complete blocking, as in Iran and North Korea, as well as in China, which has set up alternative websites for its citizens, such as Yoko and Weibo, or through a temporary blocking related to specific events, such as the blocking of YouTube, Twitter, and Facebook in some Arab countries during the revolutions known as the Arab Spring.

Problems and controls

The dual nature of the use of social networking sites leads to calls for censorship of their content and activities , and at the same time raises concerns that such surveillancecould be used against political opposition, discrimination, and invasion of privacy, especially since much of what is disseminated through these networks is not public, but includes private correspondence, personal data, browsing activities, geographic data, and others whose monitoring requires judicial authorizations.

Although the government justifies social media surveillance as part of the security services' mission to protect public safety, there are several issues that interfere with that mission, the most important of which is privacy considerations that shift surveillance work from monitoring and analysis to spying and surveillance when done without legal oversight.

This brings us to another problem related to the definition of public interest, national security requirements, and other requirements used to justify control and surveillance measures that are important.

These problems are exacerbated by the fact that social networks have only recently begun to be used in some societies, that the associated legal frameworks are not yet mature, and that their concepts are unclear, especially given the rapid development of their techniques and tools. In addition, there is the cross-border nature of these services and the various problems that arise. Ownership by companies based in other countries of such a volume of data and information on the country's citizens is in itself a major security risk.

All of these considerations threaten social media freedoms and put the principles of global democracies to the test. This in light of the scandals and transgressions that are exposed from time to time, the involvement of social media moderators in such practises, and even the introduction of surveillance tools consistent with the policies of repressive states to reach new markets and achieve economic benefits, apart from their role in liberating peoples and supporting the values of global dialogue.

Between the fear of oppression and the concern for security threats, monitoring social media content seems an obvious matter and even an undeniable necessity. However, it must be done in the context of monitoring and analysis and not used for discriminatory practices. It should be subject to accountability, responsibility, and disclosure, and it should strike a balance between the freedom to use social networks and limiting their risks.

However, this balance cannot be achieved by relying on the integrity of executive bodies. Rather, an integrated system must be built that provides, on the one hand, for the drafting of laws to consolidate constitutional provisions in order to guarantee the individual rights, protect privacy, and streamline security performance, and, on the other hand, for the activation of the instruments of parliamentary control and accountability and judicial review.

In parallel, civil society organizations and the media must be empowered to monitor violations and guide public debate to create a balanced system based on transparency, law enforcement, and the exercise of mutual pressure. In order to protect one of the most important instruments of participatory democracy, the role of active forces in the political and social scene must be strengthened.

Conclusion:

The rapid development in information technologies has eased the ability to generate, collect, analyze and store information compared to previous times. This prompts advocacy to set up legislation to keep pace with these capabilities to control the dissemination and exchange of information. It is essential to make a real legal review that includes issuing new legislation aimed at controlling and defining the powers of social media companies in controlling individuals' online content

The international community should combine forces to fully protect social media users' information and data from being monitored and used without their consent. It is also important 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, business and academics should effectively address challenges to the right to privacy, notably in an era that is dominated by modern communication technology.

Effectively addressing privacy challenges of modern communications technology requires sustained and concerted engagement, and this process should include a comprehensive dialogue involving all relevant stakeholders, including States, civil society, human rights organisations, the scientific community, businesses, and academics.

All parties should form a common basis that ensure the protection of 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 efforts to ensure individuals' legal rights legally in case they are violated, by any party, whether countries or spying companies.