VIZMUN 21

The Legal Committee

Study Guide

Most Distinguished Attendances and Respectable Advisors,

My name is Ediz Can Kaya. I am a tenth-grade student at Vizyon College and I have the topmost honor of serving as the Secretary-General of the second annual session of Vizyon College Model United Nations which will be held between 11-13 June 2021. As a Secretariat and staff, we value diplomacy and do our best to create a productive and positive experience for all delegates and advisors.

We are gathering in 6 different committees: Legal, Futuristic United Nations Security Council (Futuristic UNSC), World Health Organization (WHO), Turkish Joint Crisis Committee, Joint Crisis Committee,United Nations High Commissioner for Refugees

As a young generation, today we have the chance to change the wraceful world bringing accomplishment and security to each individual. Every day, we get a chance to do something different, to change the world! For a few months, both academic and organization teams of VIZMUN 2021 have been working on this assembly by giving an effort to provide all attendants with an unforgettable and delighted experience of Model United Nations. According to our belief, we and delegates will be contributed to relations, World awareness, and policy along with the conference.

Do not hesitate in contacting us should you encounter any doubts along the way at

secretary-general@vizmun.com

Best of luck on the path ahead!

Warm Regards,

Ediz Can Kaya

Secretary-General of VIZMUN 2021

LETTER OF UNDER-SECRETARY-GENERAL

Dear delegates of LEGAL Committee,

I am CansuTosun and I'm a junior year student in Kadir Has University and my department is Political Science and Public Administration. It is a pleasure for me to serve as the Under-Secretary-General of LEGAL Committee in Vizyon College Model United Nations conference, which is one of the prestigious and one of the most long-established conferences in Turkey.

Unfortunately, the use of social media all over the world has taken our whole lives hostage. Now people do everything on social media. Even their special memories between the family are now living through social media. They open their pain, sadness, happiness and all their feelings and thoughts to the whole world through social media. While there was so much sharing, many problems arose when social media fell into the hands of bad people. These crimes are increasing, from stealing people's private accounts and money, to revealing people's hidden files, to accessing all their personal data, and also to stealing their social media accounts. States have tried to prevent these problems with social media surveillance. So what are the benefits and harms of this? What kind of measures has your country taken in this regard? We will discuss all these together at the VIZMUN'21 conference between 11th-13th June and try to find a solution to every issue.

I would like to thank a few people which made it possible for me to take part in this conference, namely, Ediz Can Kaya, BurakYağızGüllü and SerenAnaçoğlu; our lovely Secretariat.

If you would have any inquiries or questions, please feel free to contact me via cansutosun1@gmail.com .

Best regards.

CansuTosun

Under Secretary-General of LEGAL Committee

Table of Contents

INTRODUCTION TO LEGAL COMMITTEE

The United Nations General Assembly Sixth Committee is one of six main committees of the General Assembly of the United Nations. It deals primarily with legal matters and is the primary forum for the consideration of international law and other legal matters concerning the United Nations. The United Nations General Assembly has an express mandate to promote the progressive development of public international law as laid out in the Charter of the United Nations. Specifically, Article 13 of the Charter states that the General Assembly has the authority to "initiate studies and make recommendations for the purpose of (a) promoting international co-operation in the political field and encouraging the progressive development of international law and its codification." The subsequent practice has interpreted this provision as a broad authorization to elaborate new treaties on the widest range of issues, to adopt them, and to recommend them to states for their subsequent signature, ratification, or accession. While international law-making negotiations take place in a variety of specialized bodies of the United Nations, depending on their actual subject matter, those negotiations related to general international law are usually held at the Sixth Committee.

INTRODUCTION TO AGENDA ITEM

Agenda Item: Social Media Surveillance

What Is the Social Media?

Social media is a computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is Internet-based and gives users quick electronic communication of content. Content includes personal information, documents, videos, and photos. Users engage with social media via a computer, tablet, or smartphone via web-based software or applications. Social media originated as a way to interact with friends and family but was later adopted by businesses that wanted to take advantage of a popular new communication method to reach out to customers. The power of social media is the ability to connect and share information with anyone on Earth, or with many people simultaneously. Globally, there are more than 3.8 billion social media users. Social media is an ever-changing and ever-evolving field, with new apps such as TikTok and Clubhouse coming out seemingly every year, joining the ranks of established social networks like Facebook, YouTube, Twitter, and Instagram. By 2023, the number of social media users in the United States is forecast to increase to approximately 257 million.

Effects of Social Media:

The positive aspects of social media

While virtual interaction on social media doesn't have the same psychological benefits as face-to-face contact, there are still many positive ways in which it can help you stay connected and support your wellbeing.

Social media enables you to:

- Communicate and stay up to date with family and friends around the world.
- Find new friends and communities; network with other people who share similar interests or ambitions.
- Join or promote worthwhile causes; raise awareness on important issues.
- Seek or offer emotional support during tough times.
- Find vital social connection if you live in a remote area, for example, or have limited independence, social anxiety, or are part of a marginalized group.
- Find an outlet for your creativity and self-expression.

- Discover (with care) sources of valuable information and learning.

The negative aspects of social media

Since it's a relatively new technology, there's little research to establish the long-term consequences, good or bad, of social media use. However, multiple studies have found a strong link between heavy social media and an increased risk for depression, anxiety, loneliness, self-harm, and even suicidal thoughts.

Social media may promote negative experiences such as:

Inadequacy about your life or appearance. Even if you know that images you're viewing on social media are manipulated, they can still make you feel insecure about how you look or what's going on in your own life. Similarly, we're all aware that other people tend to share just the highlights of their lives, rarely the low points that everyone experiences. But that doesn't lessen those feelings of envy and dissatisfaction when you're scrolling through a friend's airbrushed photos of their tropical beach holiday or reading about their exciting new promotion at work.

Fear of missing out (FOMO). While FOMO has been around far longer than social media, sites such as Facebook and Instagram seem to exacerbate feelings that others are having more fun or living better lives than you are. The idea that you're missing out on certain things can impact your self-esteem, trigger anxiety, and fuel even greater social media use. FOMO can compel you to pick up your phone every few minutes to check for updates, or compulsively respond to each and every alert—even if that means taking risks while you're driving, missing out on sleep at night, or prioritizing social media interaction over real world relationships.

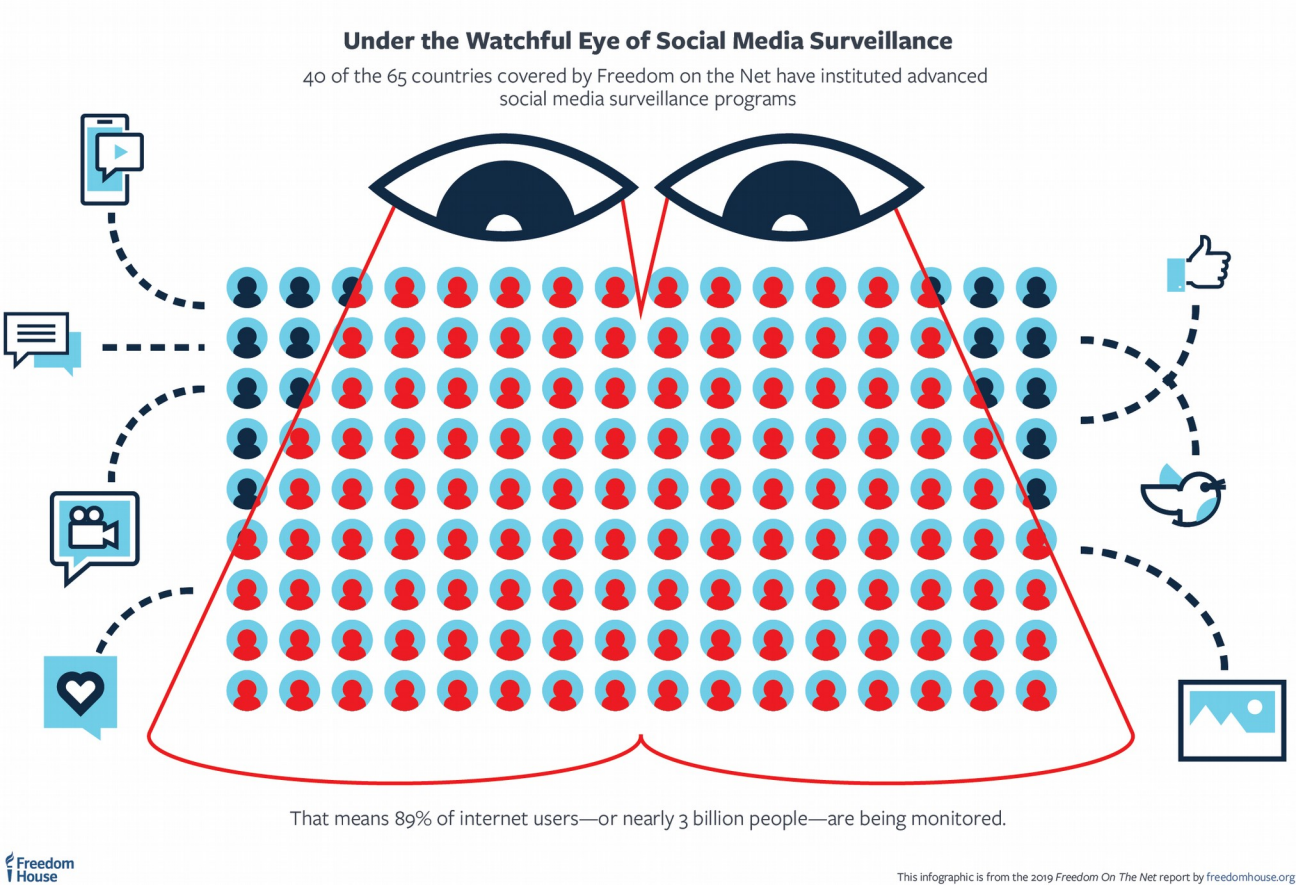
Isolation. A study at the University of Pennsylvania found that high usage of Facebook, Snapchat, and Instagram *increases* rather decreases feelings of loneliness. Conversely, the study found that reducing social media usage can actually make you feel *less* lonely and isolated and improve your overall wellbeing.

Depression and anxiety. Human beings need face-to-face contact to be mentally healthy. Nothing reduces stress and boosts your mood faster or more effectively than eye-to-eye contact with someone who cares about you. The more you prioritize social media interaction over in-person relationships, the more you're at risk for developing or exacerbating mood disorders such as anxiety and depression.

Cyberbullying. About 10 percent of teens report being bullied on social media and many other users are subjected to offensive comments. Social media platforms such as Twitter can be hotspots for spreading hurtful rumors, lies, and abuse that can leave lasting emotional scars.

Self-absorption. Sharing endless selfies and all your innermost thoughts on social media can create an unhealthy self-centeredness and distance you from real-life connections.

What Is the Social Media Surveillance?



Surveillance is a broad term. Human beings are routinely aware of their environment, consciously and less consciously taking note of the appearance and behavior of others nearby. It occurs in every social system – between friends, by colleagues and managers, and by bureaucrats (Marx, **2012**). This includes human activity on social media websites such as Twitter, Google+, YouTube, and Facebook, which reached 1.19 billion active monthly users in October 2013. While individuals typically use social media to communicate and share photos, web links, and other types of information with their associates, the main aim of social media providers is to use all of this data to create profiles that can be used to show users targeted adverts.

More deliberate monitoring of individuals often takes place in an adversarial and inquisitorial context, increasingly using technical means to gather and analyze data, and is used for social, environmental, economic, or political governance.

Etymologically, *surveillance* comes from the French word meaning "oversee" or "watch over," carried out by watchers, overseers, and officers – implying social hierarchy (Fuchs, **2011**, p. 124). The process is typically distributed across interlinked systems, bureaucracies, and social connections – converging into "surveillant assemblages" – and embedded within everyday life (Lyon, Haggerty, & Ball, **2012**). Social media sites increasingly resemble such assemblages, as they draw in data on user activity elsewhere on the internet via "cookies" and other tracking mechanisms, and from other sources of information on users, such as retailer loyalty cards, customer surveys, and smartphone location traces.

Surveillance is an ancient social process, but in the late twentieth century became a central organizing societal practice, affecting power dynamics, institutional practice, and interpersonal relations. Alongside changing technology, this transformation was driven by factors including increasing managerialism, greater public perception of risk, and political expediency (Lyon et al., **2012**). The extent and intensity of surveillance practices in some modern polities – both democracies and authoritarian regimes – have led them to be labeled surveillance societies.

A number of factors need to be taken into account when considering a particular instance of social media surveillance. Who is carrying it out – a government agency, with a broad or narrow focus? A business dealing with customers, or profiling and marketing to potential customers? A community of individuals? What are the power relations between the surveiller(s) and the surveilled? What kinds of data are being collected, using which means? These might include narrative reports (by journalists or police officers), audiovisual recordings (by webcams), or activity traces, relating to public, personal, private, sensitive, or intimate situations – all of which now take place via social media. Which norms or rules cover data security, access, and use, and how are these enforced? Which cultural factors shape the experience of watching and being watched? Is surveillance culturally linked to modernization or a benevolent welfare state, or used as a weapon against internal or external enemies during a crisis?

Social media users spend a great deal of time curating online "exhibitions" of different aspects of their identities. Identity play and control are especially important to young people as they grow up and develop their own independent identities and peer relationships. The use of social networks is now a key part of this process in advanced economies, critical for friendships, social capital, and popularity (Joinson& Paine, **2007**) and experimentation with different roles and types of identities. Children can use private online spaces for "silly, rude or naughty behaviour" and to seek confidential information and advice (Livingstone, **2006**, p. 132). This can be vital for children who may feel isolated in their local environment, such as lesbian or gay teenagers, and who can make friends online with geographically remote individuals (Marwick, Murgia-Diaz, & Palfrey, **2010**). This "identity work" in social networks, however, has a consequence usually unintended by the user: the development of commercial profiles that can have a significant impact on life chances.

Individuals' close social circle members can respond quite negatively to expressed identities that are contrary to an expected social role. The internet has given individuals greater opportunities to express and develop marginalized identities (e.g., sexuality and fringe ideologies), and to overcome social anxiety. Active participation in online groups related to stigmatized identities and ideologies allows individuals to gain support from group members, leading to increased self-acceptance and reduced feelings of isolation, difference, and shame, as well as significant increased willingness ultimately to share these identities with family and friends.

Social media surveillance reduces individuals' control over the information they disclose about their attributes in different social contexts, often to powerful actors such as the state or multinational corporations. Social networking tools make it much easier for individuals to share information about their friends and acquaintances, with or without their consent. Any of these actors in turn may treat individuals differently based on that information, and share it without their explicit consent – including using identification technologies to link surveillance data back to individuals.

Social media surveillance refers to the collection and processing of personal data pulled from digital communication platforms, often through automated technology that allows for real-time aggregation, organization, and analysis of large amounts of metadata and content. Broader in scope than spyware, which intercepts communications by targeting specific individuals' devices, social media surveillance cannot be dismissed as less invasive. Billions of people around the world use these digital platforms to communicate with loved ones, connect with friends and associates, and express their political, social, and religious beliefs. Even when it concerns individuals who seldom interact with such services, the information that is collected, generated, and inferred about them holds tremendous value not only for advertisers, but increasingly for law enforcement and intelligence agencies as well.

Governments have long employed people to monitor speech on social media, including by creating fraudulent accounts to connect with real-life users and gain access to networks. Authorities in Iran have boasted of a 42,000-strong army of volunteers who monitor online speech. Any citizen can report for duty on the Cyber Police (FATA) website. Similarly, the ruling Communist Party in China has recruited thousands of individuals to sift through the internet and report problematic content and accounts to authorities.

Advances in artificial intelligence (AI) have opened up new possibilities for automated mass surveillance. Sophisticated monitoring systems can quickly map users' relationships through link analysis; assign a meaning or attitude to their social media posts using natural-language processing and sentiment analysis; and infer their past, present, or future locations. Machine learning enables these systems to find patterns that may be invisible to humans, while deep neural networks can identify and suggest whole new categories of patterns for further investigation. Whether accurate or inaccurate, the conclusions made about an individual can have serious

repercussions, particularly in countries where one's political views, social interactions, sexual orientation, or religious faith can lead to closer scrutiny and outright punishment.

Such a reduction in disclosure control limits people's ability to regulate their social interactions (Joinson& Paine, **2007**) and to position themselves in relation to available social identities. This violates the "contextual integrity" that individuals rely on to play various roles (worker, best friend, social club member, parent, child) in different social situations. It also facilitates economic and governance aims, classifying and controlling individuals in more or less subtle ways, such as by using "risk profiles" to allocate credit or make decisions on individual passage through a border (Lianos, **2003**).

Individuals may feel that such classifications are blunt or miss important data relevant to the making of a fair decision. They may also have a "chilling effect" on the possibilities for whistle-blowing and democratic activism.

The global market for surveillance

The market for social media surveillance has grown, giving intelligence and law enforcement agencies new tools for combing through massive amounts of information. At least 40 of the 65 countries covered by this report have instituted advanced social media monitoring programs. Moreover, their use by governments is accelerating: in 15 of these countries, it was only in the past year that such programs were either expanded or newly established. Justifying their efforts in the name of enhancing security, limiting disinformation, and ensuring public order, governments have effectively co-opted social media platforms. While these platforms typically present themselves as social connectors and community builders, state agencies in repressive countries see them as vast storehouses of speech and personal information that can be observed, collected, and analyzed to detect and suppress dissent. China is a leader in developing, employing, and exporting social media surveillance tools. The Chinese firm Semptian has touted its Aegis surveillance system as providing "a full view to the virtual world" with the capacity to "store and analyze unlimited data." The company claims to be monitoring over 200 million individuals in China—a quarter of the country's internet users. The company even markets a "national firewall" product, mimicking the so-called Great Firewall that controls internet traffic in China.

Chinese agencies work closely with leading companies to monitor individuals online. A security researcher discovered an unsecured database consisting of the social media profiles, messages, and shared files of some 364 million Chinese users, updated daily, for manual tracking by law enforcement. A complex web of regulations gives the Chinese state access to user content and metadata, allowing authorities to more easily identify and reprimand users who share sensitive content. In March 2019, for example, it was reported that a member of Xinjiang's persecuted Uighur Muslim minority population was detained and interrogated for three days because someone on his WeChat contact list had "checked in" from Mecca, Saudi Arabia.

Further, several provincial governments in China are reportedly developing a "Police Cloud" system to aggregate data from users' social media accounts, telecoms records, and e-commerce activity, as well as biometric data and video surveillance footage. The big data policing system can target individuals for interacting with "persons of concern" or for belonging to "certain ethnicities," a euphemism applying to the Uighur Muslim minority. There, authorities have developed a host of invasive tools, both low- and high-tech, for repressing any behavior that strays from what is acceptable under Xi Jinping Thought—the doctrine of China's authoritarian leader.

Of the 15 countries in Asia assessed by this report, 13 have social media surveillance programs under development or in use. In Vietnam, the Communist Party government in October 2018 announced a new national surveillance unit equipped with technology to analyze, evaluate, and categorize millions of social media posts. The government has long punished nonviolent activists for what they write on social media; weeks before the October announcement, human rights defender and environmentalist LêĐìnhLượng was convicted and sentenced to 20 years in prison after a one-day trial for trying to overthrow the state, in part for Facebook posts criticizing the government. The new technology will likely enable the government to intensify its crackdown. Meanwhile, Pakistan in February 2019 announced a new social media monitoring program meant to combat extremism, hate speech, and antinational content. Only a month later, the Interior Ministry launched an investigation into journalists and activists who had expressed support for murdered Saudi journalist Jamal Khashoggi on their social media accounts.

Some countries in Asia are developing their social media surveillance capabilities in close cooperation with US authorities. In September 2018, Philippine officials traveled to North Carolina for training by US Army personnel on developing a new social media monitoring unit. While authorities claim the unit is intended to combat disinformation by violent extremist organizations, the Philippine government's broad labeling of critical journalists and users as terrorists suggests that monitoring efforts will extend far beyond any legitimate security threat. Bangladesh's Rapid Action Battalion (RAB) was approved to travel to the United States in April 2019 to receive training on "Location Based Social Network Monitoring System Software." The RAB, which is infamous for human rights violations including extrajudicial killings, enforced disappearances, and torture, was given 1.2 billion taka ($14 million) by the Bangladeshi government for "state-of-the-art equipment" to monitor in real time what it considers to be rumors and propaganda. These developments occurred in a year when authorities led a violent crackdown on dissent during national protests and general elections.

The Middle East and North Africa region, home to some of the world's most repressive regimes, is also a booming market for social media surveillance. Companies scheduled to attend a Dubai trade show in 2020 represent countries including China, India, Israel, Italy, the United States, and the United Kingdom. Knowlesys, a Chinese company whose clients reportedly include the Chinese military and government bodies, will hold live demonstrations on how to "monitor your

targets' messages, profiles, locations, behaviors, relationships, and more," and how to "monitor public opinion for election." Semptian, which has clients in the region, has a price range of $1.5 million to $2.5 million for monitoring the online activities of a population of five million people —an affordable price for most dictators.

In December 2018, it was reported that Kazakhstan had purchased a $4.3 million automated monitoring tool to track signs of political discontent on social media. The firm supplying the software is linked to Russia's Federal Security Service and has been subjected to sanctions by the US Treasury Department for its activities surrounding the 2016 US elections. Screenshots revealed that the product uses deep learning to "detect materials that discredit the state." The tools could easily be abused in Kazakhstan, where individuals have received multiyear prison sentences for social media posts that are deemed supportive of the Democratic Choice of Kazakhstan, a banned opposition party.

Russia has used sophisticated social media surveillance tools for many years. The government issued three tenders in 2012 for the development of research methods related to "social networks intelligence," "tacit control on the internet," and "a special software package for the automated dissemination of information in large social networks," foreshadowing how intelligence agencies would eventually master the manipulation of social media at home and abroad. This May, authorities released a tender for technology to collect, analyze, and conduct sentiment analysis on social media content relating to President Vladimir Putin and other topics of interest to the government. The year featured more protest-related arrests, internet shutdowns, and legal restrictions in Russia, suggesting that any new monitoring technology would simply add to the government's arsenal of tools for clamping down on unauthorized political mobilization.

Monitoring projects are under way in Africa as well. The government of Nigeria allocated 2.2 billion naira ($6.6 million) in its 2018 budget for a "Social Media Mining Suite," having already ordered the military to watch for antigovernment content online. In an ominous sign, the country experienced an increase in arrests for internet activity over the past year. Human rights and democracy activist Ibrahim GarbaWala, known as IG Wala, was sentenced in April to 12 years in prison for criminal defamation, public incitement, and unlawful assembly; the charges stemmed from Facebook posts alleging corruption in the National Hajj Commission. Israeli firms Verint and WebIntPro have reportedly sold similar surveillance software to Angola and Kenya, respectively.

In strong democracies, new tools of potential repression

The social media surveillance tools that have appeared in democracies got their start on foreign battlefields and in counterterrorism settings, designed to monitor acute security threats in places like Syria. Many US data-mining companies received seed money from the Central Intelligence Agency through its In-Q-Tel venture capital fund. While authorities in the past typically justified the use of these tools with the need to combat serious crimes such as terrorism, child sexual

abuse, and large-scale narcotics trafficking, law enforcement and other agencies at the local, state, and federal levels are increasingly repurposing them for more questionable practices, such as screening travelers for their political views, tracking students' behavior, or monitoring activists and protesters. This expansion makes oversight of surveillance policies more difficult and raises the risk that constitutionally protected activities will be impaired.

For example, in the United States, agencies within the Department of Homeland Security (DHS) —including Customs and Border Protection (CBP), Citizenship and Immigration Services, and Immigration and Customs Enforcement (ICE)—have used automated technology to collect and analyze personal information, with limited oversight and transparency. By claiming that its power to conduct warrantless searches extends within a 100-mile radius of any US border, DHS has effectively asserted extrajudicial surveillance powers over 200 million people. CBP has even purchased technology from Cellebrite, an Israeli company, to bypass encryption and passwords and enable quick extraction of data from phones and computers, including social media content. There has been a spike in device searches at the borders in recent years; the number of such searches, normally limited under the Fourth Amendment of the constitution, increased by 292 percent, from 8,503 to 33,295, between fiscal year 2015 and fiscal year 2018. Over that same period, inbound travel to the United States increased by less than 3 percent.

These searches have become part of the government's drive toward big data surveillance. The resulting information is frequently deposited in massive multiagency databases where it can be combined with public records, secret intelligence materials, and datasets (including social media data) assembled by private companies. In one case, ICE paid the data analytics company Palantir $42.3 million for a one-year contract related to FALCON, a custom-built database management tool. Its "Search and Analysis System" enables agents to analyze trends and establish links between individuals based on information gathered during border searches, purchased from private data brokers, and obtained from other intelligence collection exercises. Similar tools developed by Palantir are used by some 300 police departments in the state of California alone, as well as by police forces in Chicago, Los Angeles, New Orleans, and New York City. Many of these programs are facilitated through DHS and its Regional Intelligence Centers.

The consequences of government intrusion into the digital public square

For authoritarian and democratic governments alike, the potential for abuse presented by advanced social media surveillance is staggering. In 2019, Freedom House found that 47 of the 65 countries assessed featured arrests of users for political, social, or religious speech—a record high. The blanket monitoring of online activities for undesirable or illegal speech will undoubtedly lead to more arrests, particularly in environments that lack strong protections for free expression. Monitoring designed to detect and deter protests will also help stifle democracy movements in authoritarian settings.

Even in countries with considerable safeguards for fundamental freedoms, there are already reports of abuse. In the United Kingdom, for example, London police reportedly monitored nearly 9,000 activists from across the political spectrum—many of whom had no criminal background—using geolocation tracking and sentiment analysis on data scraped from Facebook, Twitter, and other platforms. This information was then compiled in secret dossiers on each campaigner. Similar dynamics are evident in the United States, where leaked documents revealed in March 2019 that CBP had created a list of 59 US and foreign immigration activists, journalists, lawyers, and Facebook group administrators who should be targeted for greater scrutiny at the US-Mexico border, leading to arrests in nine cases. ICE has also monitored social media in New York City to gather information on groups protesting the administration's immigration and gun-control policies. Such profiling poses a distinct threat to basic civil liberties. As the US Supreme Court ruled in 1958, "inviolability of privacy in group association may in many circumstances be

indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."

The chilling effect on free expression caused by increased surveillance is well documented. Activists and journalists who might otherwise hold governments to account for wrongdoing are more inclined to self-censor, while dissidents and members of marginalized communities will think twice about discussing their political opinions online to avoid arrests or travel restrictions. Furthermore, social media monitoring designed to quell mobilization and identify protesters hinders the public's ability to use online tools to associate and assemble peacefully. Finally, indiscriminate monitoring of the general population's online communications—even when those communications are nominally public—runs afoul of due process standards enshrined in democratic constitutions and international human rights law.

Protecting human rights in the age of AI surveillance

There is little if any public evidence that such technology is more effective than less-invasive alternatives for ensuring national security and combating serious crimes. Social media activity such as original content, likes, or shares—particularly speech that is rendered in slang or languages other than English—is susceptible to misinterpretation and misclassification. Research has estimated the accuracy rates of natural-language processing tools at 70 to 80 percent. While they are often justified as a means to reduce human error, algorithmic tools can further entrench racial or religious discrimination due to reliance on inaccurate or biased data. The resulting false positives can add innocent people to government watch lists, often without their knowledge, leaving them with little recourse for remedying the mistake.

At the very least, social media surveillance must come under greater oversight. The use of such programs must be transparent, including sustained dialogue between law enforcement and affected communities. Public civil rights assessments should be conducted, and authorities should be held accountable when tools are misused and offer remedies for any victims. Online surveillance technology should not be used to proactively monitor the planning and organization of peaceful protest activities or individuals' involvement in nonviolent political groups. And governments should swiftly amend existing privacy legislation to address the proper use of this technology.

Thanks to the development of AI-assisted tools, governments now have a greater capacity for surveillance than ever before. Given their potential impact on fundamental rights, policymakers and citizens must ask themselves whether these new tools are necessary or desirable in a democratic society. It is time to move beyond outdated arguments that individuals "should have nothing to hide" or do not have a reasonable expectation of privacy in public areas. The survival of democracy requires vibrant public spaces, both offline and online, where individuals can collaborate, organize, and go about their personal lives without fear of constant surveillance.

The Impact of New Technologies and Practices

The rapid development of computing technologies, and the social, political, and economic practices that have shaped and been shaped by this development, is one of the most significant enablers of social media surveillance.

Computer processing power continues to grow, following Moore's Law, doubling roughly every 18–24 months, although at some point the fundamental limits of engineering will limit this growth. Computer storage capacity and communications bandwidth are increasing at least as quickly. These exponential increases will significantly enhance the capability of organizations to collect, store, and process personal data.

Digital technologies generally can be configured to generate voluminous records of personal activity. In the online environment almost every communication and webpage access leaves behind a detailed footprint, linked to individuals through the IP (internet protocol) address of their computer or smartphone, and through digital "cookies" left on their browser by websites. Social media firms encourage individuals to share information about themselves with their "friends," along with the operators of those sites. Mobile phones send location information to network providers to enable calls to be forwarded, and to enable location based services such as mapping and advertising. Social media apps running on these smartphones allow users to both explicitly and implicitly share information about themselves and those around them.

Social networking sites provide detailed options for controlling who gets access to individual profiles and shared content – although these controls are often difficult to use and not prominent. Users rarely alter default settings which, therefore, have a strong impact. The providers' economic interests are generally in encouraging greater disclosure, while providing some less prominent options for the roughly one quarter of the population identified as "privacy fundamentalists" (Harris Interactive & Westin, **1999**).

Behavioral advertising companies track individuals across sites to show advertisements targeted to their profiles. Advertising agency WPP, for example, has built such profiles on 500 million individuals in North America, Europe, and Australia, while social media site users explicitly and implicitly provide profile data to enable advertising targeting. Facial recognition software is being used to match photographs and video footage of individuals against databases of criminal suspects and, more recently, by social networking sites to enable the identification of individuals in uploaded photos.

Very low-cost remotely readable radio frequency identification (RFID) tags are increasingly attached to consumer goods and access control cards, the first wave of the "internet of things" that could make some aspects of the physical world as trackable as internet activity. More sophisticated tags are included in many nations' passports, and are also being used for road toll payment systems, public transport ticketing, and in contactless payment cards such as

MasterCard's PayPass and Visa's Paywave. Gadgets such as heart rate monitors already allow individuals to share sensor information about themselves and their environment through social media.

This "ubiquitous computing" will become a pervasive phenomenon with some individuals recording detailed information about every aspect of their lives (Askoxylakis et al., **2011**). Privacy-sensitive individuals will have a limited ability to opt out of such environmental sensing by others. In the next decade, these sensors and tags are likely to become ubiquitous, dramatically smaller, and much more capable. They will fade further into the background of everyday life, with little to remind people of the data trails they are generating.

The accessibility of technology mediated activities to surveillance, not present in face-to-face interactions, can make individual control more difficult. Digital data is usually persistent (saved by default, perhaps indefinitely), searchable (much easier to find), replicable (easily shareable in convincing form), and, as a result, lacks a specific audience (boyd, **2008**, p. 126). None of these qualities is obvious to less experienced users. Real-world gossip is deniable, usually geographically limited, and fades over time. Digital information about an individual – however partial and unrepresentative – can persist as a digital scarlet letter.

Underlying developments in computing technology will enable sophisticated analysis of this flood of personal data. Profiling and data analysis algorithms are increasingly used on very large databases to spot patterns and identify individuals and behaviors "of interest." E-commerce stores can see not just their customers' purchasing behavior, but every product customers consider and for how long before deciding whether or not to buy. Service providers can store all information provided by a user, such as search terms. Companies use this transactional data to target special offers at customers and to find ways to provide slightly different products at different prices so as to maximize revenue. Using customer relationship management software, firms also focus on identifying and retaining high-value customers while reducing service levels to less profitable individuals. All of these types of data can be linked via social media profiles, now often automatically linked as they are used to log into cooperating sites elsewhere on the internet.

Social Media Surveillance and Human Rights Protections

Human rights laws provide one key protection for social media users from government abuse of surveillance powers. A range of potential transatlantic human rights standards for surveillance has been developed by civil society groups, courts, and watchdogs, such as the EU Data Protection Supervisor. Civil society groups have identified some key features for law reform that would strengthen these protections, including:

- Intelligence agencies should only have targeted, limited access to data, such as a specific person or a specific identifier (like a Facebook username) or a small category (like a group on a

terrorist organization list or member of a foreign intelligence agency). Data collection should only occur based on concrete suspicions.

- Agency access should be to specific records and communications. They should not be authorized to undertake bulk monitoring, such as the submarine cable taps that give NSA and GCHQ access to vast quantities of data which they then winnow down in secret. Any data access should trigger legal protections – this should not come only when data is picked out of a large data stream already collected by an agency.
- Data collected using special national security powers should be completely blocked from use for other government purposes, including law enforcement. It should be retained for limited periods and deleted once no longer required.
- "Metadata" revealing information accessed, and who people communicate with, where, and when, can be extremely revealing about individuals' lives, and currently receives very low levels of legal protection. This should change.
- There should be strict limits on intrusion into freedom of association by network analysis (the creation of very large datasets linking people through several communication hops – three in the NSA's case, which can intrude on the privacy of millions of people).
- Privacy protective technologies and limitations should be incorporated within surveillance systems. US groups have campaigned against the extension of interception capability requirements to social networking sites, and against requirements for service providers to build surveillance or monitoring capability into their systems, or to collect or retain particular information solely for state surveillance purposes. They also argue that governments should not require the identification of users as a precondition for service provision.
- Illegal surveillance should be criminalized with effective remedies when individuals' rights are breached. Illegally gathered material should be inadmissible as evidence, while whistle-blowers should be protected for revealing illegal behavior.

Civil society groups are also campaigning for greater transparency of surveillance activities, with publication of details of all surveillance programs, allowing the media, civil society, and individuals to understand and, if necessary, criticize agency activity. Industry groups are also attempting to persuade the US government to allow them to publish more detailed statistics on access to their customer data, with Facebook and Google taking legal action to claim First Amendment rights to share more information with the public about levels of access to user accounts.

QUESTIONS RESOLUTION SHOULD ANSWER

1. What effect does social media surveillance have on social media usage?
2. How social media surveillance has affected social media usage?
3. What is the affects of social media surveillance on the human rights, women rights, law enforcement?
4. What is the affects of social media surveillance on living conditions, social media use, education level?
5. How has the crime rate changed with social media surveillance?
6. Describe your country's problems before social media surveillance.
7. What processes have countries had regarding social media surveillance? (your own country)
8. What problems has your own country solved with social media surveillance?

FURTHER READINGS

Brown I., (04 November 2014) *Social Media Surveillance*

https://doi.org/10.1002/9781118767771.wbiedcs122

MATEESCU A. , BRUNTON D. , ROSENBLAT A., PATTON D., GOLD Z., and BOYD D. (2015)*Social Media Surveillance and Law Enforcement*

https://strongvisa.com/wp-content/uploads/2011/07/Social_Media_Surveillance_and_Law_Enforcement-2015.pdf

Shahbaz A., Funk A. (2019)*Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance*

https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance#:~:text=Social%20media%20surveillance%20refers%20to,amounts%20of%20metadata%20and%20content.