

GLOBAL PERSPECTIVES

2020-21

PROJECT ON

The proliferation of digital
social media - *where should
the line be drawn?*



Sarah Kothekar
2020

Singapore International School
Mumbai, India



Introduction

In 1995 just 1% of the world had access to the internet. Now there are more than 4 billion internet users worldwide, and this figure is skyrocketing (Watson).

Social media like Facebook, Instagram, and Twitter has allowed us to be constantly connected with many far and wide. It has allowed numerous people to find long lost friends and family members and to make many new acquaintances and friends. One can get to know more about any person, as their life is an open book on their profile page. It has made the world a connected place with no boundaries as there is no need to travel to meet someone at any corner of this world. It has become a source of knowledge, entertainment, and assistance in collaborated research. Social media is now synonymous with the social existence of an active person or a group.

However, this is where the good part ends. As the information is on a public platform, it is easily accessible to social media companies and the 'hackers,' there are serious concerns about **privacy, usage of a person's information and digital surveillance**. This report examines these three issues at the personal, national and global level and will conclude with some courses of actions that I think are urgently required.



Privacy

Like many **Individuals**, I am active on social media every day. It is a means for us friends to communicate our everyday happenings, travels, trends, experiences, and knowledge. I can search for other people, known or unknown and send messages to them. Subsequently, some people can send me hate messages on how I live and think, without the slightest consideration to what I would feel. Cases of depression due to social trolling have increased at an exponential rate, same as the rate of social media proliferation (Cakebread). While the majority are in the 18 to 24 age bracket, some are as young as 14 (Denner). Hannah Smith, aged 14, presumably hanged herself at her home in Leicestershire, after being cyberbullied. On being taunted on the controversial website Ask.fm four young men took their own lives at the thought of being publicly humiliated (Lee).

From a **National perspective**, this has allowed individuals and fringe groups to stalk people with views that differ from theirs in either religion, fashion, food habits, race and political affiliations. The abuses are visible to the victim's friends as well. Cyberbullying affects 60 million Americans, which is 24% of the adult population in America (Osborne). Even Ed Sheeran, a famous singer, had to renounce Twitter after receiving a stream of unwarranted, malicious tweets (Jackson).

From a **Global perspective**, the crimes on individuals by organized criminals across the country's border is a cause of global worry as the victim's police cannot charge or prosecute the criminal in another country. Organized criminal gangs in Russia are enticing young men across countries to performing sex acts on screen, and then blackmailing them- known as 'sextortion'. There are pedophiles in Europe scouting victims in India by acting as benevolent people (Sawer).

The solution could be to get off the social media grid and disconnect all apps. Unfortunately, for a socially active person, being on social media is a necessity. The situation is like that of the deer in the jungle. It has to go to the river to drink water, knowing well that its hunters are nearby. The survey by Tech.pinions of 1,000 Americans across age and gender demographics showed that only 9% had deleted their accounts (Osborne).

Governments have laws for online financial frauds, but not for personal crimes committed on a social platform on the web. Every country has to frame laws to punish crimes committed through social media just like the existing personal criminal laws. There has to be laws for punishing cyberbullying, trolling and blackmail, just like the existing laws that can prosecute a person for physical stalking, assault or murder. At the global level, the United Nations should take an initiative to form a body to formulate laws on all nations to prosecute cyber criminals irrespective of the country to which the victim belongs to.

Use of Our Data

Social media companies like Facebook, Instagram, Twitter and others, provide their services free to all their users. They have spent millions of dollars to build their software and provide a huge server space for storing everybody's data consisting of viewed, liked or posted pictures, videos, and chats. They have to continue spending to enhance or update their platforms, and hence need a source of income.

They earn their revenue by selling the data of their software subscribers to companies wanting to advertise their products. They have data extracting engines that collate information about a person's likes, dislikes, preferences, inquiries and attitude from the conversations, pictures and information shared. This data is used to build a psychological and social profile of the person. In a TV advertisement, only 10% of those interested in the product actually see it when it was aired. But on social media, it appears whenever the targeted person visits his or her page. This is very advantageous for the companies as they get to have an effective and targeted method of marketing at a lower cost. Total advertisement revenue earned by Facebook in 2018 was 55 billion dollars, using its 1.52 billion users (Facebook Ad Revenue).

The right to use the data of the subscriber, in any way the company wants, is enabled legally from the "terms and conditions," notification the subscribers needs to accept to be allowed to use the platform. Not accepting the terms, denies a person to use that particular social media platform. 90% of the users accept the terms without reading them (Cakebread).

Facebook can transfer or sub-license its rights over a user's content to another company or organization. Professional networking site LinkedIn has the power to use, share, publish, process, and commercialize its subscribers' data (Smith).

For an **individual** it is arm twisting, as he does not get paid for usage of his data but cannot disallow it as that will prevent him from using the website of the social media company, which is a must for any individual today (Watson).

At a **National level**, upheavals can be fostered by bombarding messages to a population of a particular profile, belief, or political affiliation. The ongoing case of Cambridge Analytica using data from Facebook to manage Trump's election campaign is a classic case.

At a **Global level**, one country can use fake propaganda to destabilize other country- like the recent fake news torrent by Pakistan to create instability in Kashmir.



The possible solution: The conventional wisdom is that the deletion of social media accounts can stop social media companies from tracking and profiling you. However, A research team from Australia showed that tweets from accounts of friends of the deleted user can help to create his profile with 95% accuracy. This research points out that there is no place to hide on social networking platforms (Lindsey). Hence the only option left is to regulate the use of the subscriber's data.

The social media companies must be forced by new laws to restrict the sale of the users' data to companies using it for advertising their products and services. They should be criminally liable for providing it to use for political gains or religious messaging. The European Union is showing the way through the General Data Protection Regulation (Lindsey). Though Silicon Valley has not shown any similar inclination, it should be prevailed upon by the United Nations through its International Court of Justice.



Digital Surveillance

Digital surveillance is an act by the government to continuously track a person or group's activities. This has proved to be useful in tracking down terrorists and lumpen elements of society who want to endanger human life or create anarchy. Digital surveillance helps nab the culprit before the criminal act is done. The Patriot Act by the USA and the NIA Act by India have been effective in preventing terrorist activities and cyber frauds. The NSA, following its unofficial motto of "collecting it all," intercepts 200 million text messages every day worldwide (Franceschi-Bicchierai).

As an **Individual**, knowing that I am being closely watched is very unnerving and stressful. This is a gross violation of my basic rights of privacy. At the same time, I feel safe as many attempts by terrorist have been thwarted by the Intelligence Bureau of India using the information gathered by the unrestricted surveillance.

At the **National level**, now there are companies doing digital surveillance for clients as a business. It includes surveillance of employees, competitors, or a particular group in the society. Though illegal, there are no laws to deter it. In some countries like the USA, UK, China and India, the government is doing the same in civil society, using the machinery built to gather information on terrorists.

At the **Global level**, countries provide info about impending criminal and terror acts to the target countries affected, which is benevolent. However, as Snowden's revelations indicate, there are many cases of strong countries blackmailing govt officials of other countries to spy for them (Franceschi-Bicchierai). They use the private conversations, pictures and videos to bludgeon govts to submit to their demands. The German newsweekly Der Spiegel revealed that the NSA of USA kept at least 122 world leaders, as well as leaders at the 2010 G8 and G20 summits in Toronto under surveillance (Franceschi-Bicchierai).

Though not visible, there is a digital war already raging between warring countries- USA and Russia, India and Pakistan, Israel, Iran amongst others (Rubenstein).

The solution: The issue widely debated by the liberals are the boundaries of digital surveillance- should every individual be constantly monitored for all aspects of his private life?

Digital surveillance by the government must be limited to certain aspects related to national security only. But then, who will bell the cat? The litigator himself is under surveillance and could be dissuaded by blackmail by the government using the data it has about him. Hence it has to be an international body like the Security Council of the United Nations, that has to formulate the limits of digital surveillance and the deterrents for violation. The deterrents could be trade sanctions against the faulting country.

References

1. Lindsey, Nicole. "New Research Study Shows That SM Privacy Might Not Be Possible." CPO Magazine, 28 May 2019, www.cpomagazine.com/data-privacy/new-research-study-shows-that-social-media-privacy-might-not-be-possible/.
2. Watson, Rowanna. "Internet Statistics & Trends in 2019." Vpngeeks, 2019. www.vpngeeks.com/internet-privacy-statistics/
3. <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>
4. Franceschi-Bicchierai, Lorenzo. "Edward Snowden: The 10 Most Important Revelations From His Leaks." Mashable, 5 June 2014, mashable.com/2014/06/05/edward-snowden-revelations/.
5. Rubenstein, Dana. "Nation State Cyber Espionage and Its Impacts." Nation-State Cyber Espionage and Its Impacts, www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/index.html.
6. "Facebook Ad Revenue 2009-2018." Statista, www.statista.com/statistics/271258/facebook-advertising-revenue-worldwide/.
7. "India- Number of Social Network Users 2023." Statista, www.statista.com/statistics/278407/number-of-social-network-users-in-india/.
8. Carter, Joanna, et al. "Global SM Research Summary 2019." Smart Insights, 18 Sept. 2019, www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.
9. Lomas, Natasha. "Facebook Agrees to Clearer T&Cs in Europe." TechCrunch, TechCrunch, 9 Apr. 2019, techcrunch.com/2019/04/09/its-free-youre-the-product/.
10. Smith, Oliver. "Facebook Terms and Conditions: Why You Don't Own Your Online Life." The Telegraph, Telegraph Media Group, 4 Jan. 2013, www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html.
11. Cakebread, Caroline. "You're Not Alone, No One Reads Terms of Service Agreements." Business Insider, 15 Nov. 2017, www.businessinsider.in/Youre-not-alone-no-one-reads-terms-of-service-agreements/articleshow/61659553.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
12. Denner, Wayne. "Online Trolling and the Effects on Young People." Wayne Denner, 16 June 2013, www.waynedenner.com/blog/online-trolling-and-the-effects-on-young-people/.
13. Osborne, Joe. "Nearly One in 10 Americans Have Deleted Their Facebook Accounts, Survey Says." TechRadar, TechRadar, 13 Apr. 2018, www.techradar.com/news/nearly-one-in-10-us-facebook-users-have-deleted-their-accounts-survey-says.
14. Sawyer, Patrick. "Huge Rise in 'Sextortion' by Crime Gangs Using SM to Entrap Victims." The Telegraph, Telegraph Media Group, 30 Nov. 2016, www.telegraph.co.uk/news/2016/11/30/huge-rise-sextortion-crime-gangs-using-social-media-entrap-victims/.
15. Lee, Dave. "Teenager's Death Sparks Cyber-Blackmailing Probe." BBC News, BBC, 16 Aug. 2013, www.bbc.com/news/uk-scotland-edinburgh-east-fife-23712000.
16. Jackson, Marc. "Ed Sheeran Has Quit Twitter over Cruel Comments." Daily Mail Online, Associated Newspapers, 4 July 2017, www.dailymail.co.uk/tvshowbiz/article-4662752/Ed-Sheeran-QUIT-Twitter-cruel-comments.html.

Sarah Kothekar
2020

Singapore International School
Mumbai. India