Kathmandu School of Law Review (KSLR),
Volume 8, Issue 2, 2020, pp 50-67
https://doi.org/10.46985/kslr.v8i2.2152

COVID-19 Contact Tracing Apps and Technologies as a tool of Mass Surveillance: A Cure Deadlier than the Disease

*Arafat Ibnul Bashar**

Abstract

"Desperate times call for desperate measures" – COVID-19 contact tracing apps and technology have been operating in the desperate times created by the COVID-19 global pandemic. But the impact of these apps and technology on society is contentious, as the benefit gained from such is said to be largely outweighed by the negative impact it can have during and after the pandemic. Surveillance measures have always been a tricky business. Labeled as the 'magical solution' for most horrid problems of our time such as terrorism, crime prevention, it has always failed to live up to its name and has proved to be one of the prominent tools for the authoritarian regimes to oppress people and commit gross human rights violations. Over-reliance on COVID-19 apps and considering them a 'magical solution' to containing the spread of Coronavirus can have irreversible consequences. Instead, the pandemic and desperate situation posed by it may have provided the regimes around the world an opportunity to introduce new surveillance infrastructures or strengthen the existing ones, which would have taken years and lots of friction from courts, activists, and civil society, to achieve. The article assesses the legality of COVID-19 contact tracing apps and technology and tries to draw a picture of the society that faces the consequences of surveillance and data collected through such apps and technology and looks at how legal mechanisms can cope with such consequences.

Introduction

In recent times, governmental surveillance has emerged as a dangerous habit rather than an exceptional measure.[1] The 9/11 terror attacks have changed the practice of surveillance forever. Surveillance has become a regular fixture in tackling the threat of terrorism and subsequently made its way into the detection of other crimes. But disclosures of different governmental surveillance activities over the years have proved to us why surveillance was seen as a "shameful act" by Foucault.[2] The massive intrusion in privacy and infringements of many other human rights that have resulted

* Arafat Ibnul Bashar is currently a student of LL.M. in the Department of Law, University of Chittagong, having passed his LL.B. from the same university. He can be reached at a.ibnul.b@gmail.com; arafat.law@std.cu.ac.bd.

1 '*The Right to Privacy in the Digital Age*', 30 June 2014, U.N. Doc. A/HRC/27/37; GAOR.

2 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, Pantheon Books, New York, 1977, p. 172.

from the government surveillance activities have turned the work of George Orwell in the dystopian novel "1984" into reality. Nonetheless, many countries have still resisted developing surveillance infrastructures either due to the lack of financial or technological capabilities or due to the resistance of different institutions.

However, in the wake of the COVID-19 Pandemic, surveillance measures have been on the rise again. Governments are deploying all the available resources and using up all mechanisms at their disposal to combat this unprecedented virus, and the use of technology and surveillance measures are contributing to this fight against the pandemic. Deploying apps for COVID-19 contact tracing has become an integral part of the action plan for many countries to contain this virus. People, in general, have become so occupied in their fight against this virus and its economic consequences that no one is interested in questioning such measures, as long as it gives them even the slightest hope of containing the virus. But the introduction of many of these apps and technology is questionable. Even if the COVID-19 tracing apps and technologies are making of these extraordinary times, like any other government decisions and initiatives, it should not escape scrutiny. The efficacy of such apps and technologies must be properly evaluated, keeping in mind its human rights implications, during and after the pandemic.

State of COVID-19 Surveillance Technology

Due to the highly contagious nature of the Coronavirus, it has become a necessity to identify the people who have been in close contact with an infected person. Contact tracing is a process through which people that have come into close contact with a person who has been exposed to the virus, are monitored. The practice of contact tracing has been used for a long time against the spread of diseases such as SARS, AIDS, Typhoid, in the 1918-19 influenza pandemic, for venereal diseases during World War II, etc.[3] Even the eradication of smallpox was achieved by exhaustive contact tracing.[4] Contact tracing has been identified as an essential component for controlling the spread of COVID-19.[5] The systematic and effective implementation of contact tracing can help to *"break the chains of human-to-human transmission."*[6] In fact, the use of contact tracing, in different forms, has helped in controlling the spread of COVID-19 in places like Singapore, Taiwan, and South Korea, Kerala in India.[7]

---

3 Genevieve Bell, 'We need mass surveillance to fight COVID-19—but it doesn't have to be creepy', *MIT Technology Review*, 2020, available at https://www.technologyreview.com/2020/04/12/999186/COVID-19-contact-tracing-surveillance-data-privacy-anonymity/, accessed on 10 July 2020.

4 F. Douglas Scutchfield & C. William Keck, *Principles of Public Health Practice*, Delmar Learning, New York, 3rd edition, 2003, p. 71.

5 'Digital tools for COVID-19 contact tracing', *World Health Organization*, 2 June 2020, , p. 1. available at https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1, accesed on 18 April 2021.

6 Ibid.

7 Yasheng Huang, Meicen Sun &Yuze Sui, 'How Digital Contact Tracing Slowed COVID-19 in East Asia', *Harvard Business Review*, 2020, available at https://hbr.org/2020/04/how-digital-contact-tracing-slowed-COVID-19-in-east-asia, accessed on 31 July 2020.

Contact tracing can be carried away either through tracers in the field or digitally. For example, in Wuhan, the epicenter of the pandemic, a total of 9,000 contact tracers were mobilized, who traced 'tens of thousands of contacts per day.'[8] A lot of countries around the world have deployed digital tools to surveil people to carry out contact tracing. A group of researchers from Oxford University has emphasized that a mobile contact tracing app was urgently needed to support health services to control coronavirus transmission and keep people safe since the traditional public health contact tracing approaches do not provide complete data and are not equipped to keep up with the pandemic.[9] At present, at least 34 countries have upgraded their surveillance measures to tackle the pandemic.[10] The use of technology in South Korea in flattening the curve has been lauded by the pundits. Korean authorities repurposed the data of credit card and bank transactions used for investigation of tax fraud, which was already on the government databases to retroactively track where people went.[11] The opinion of the Korean people regarding the surveillance measures has also been overwhelmingly positive.[12]

Despite the success, there have been concerns about the detail released by health authorities, as in a case, there has been an incident which led to the identification of a couple engaged in an extramarital affair.[13] Although the occurrence can be easily counted off as a one-off incident, the practices in other countries have sparked controversies. 60% of contact-tracing apps around the globe are vague about what is being tracked, do not mention the terms and conditions in advance, or deploy intrusive methods, such as surveillance of camera footage.[14]

World Health Organization has stated that currently, it possesses limited evidence to evaluate the effectiveness[15] and impact of digital tools for COVID-19 contact tracing. They have cautioned that such tools should be considered as complementary tools

8 'Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)', *World Health Organization*, 2020, available at https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-COVID-19-final-report.pdf., accessed on 10 July 2020.

9 'Controlling coronavirus using a mobile app to trace close proximity contacts', *Oxford University*, 2 April 2020, available at https://www.ox.ac.uk/news/2020-04-02-controlling-coronavirus-using-mobile-app-trace-close-proximity-contacts, accessed on 4 August 2020.

10 Dave Gershgorn, 'We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World', *OneZero*, 9 April 2020, available at https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9, accessed on 11 July 2020.

11 Justin Fendos, 'How surveillance technology powered South Korea's COVID-19 response ', *Brookings*, 29 April 2020, available at https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-COVID-19-response/, accessed on 11 July 2020.

12 Ibid.

13 Ibid.

14 Sebastian Klovig Skelton, 'Surveillance capitalism in the age of COVID-19', *ComputerWeeklycom*, 13 May 2020, available at https://www.computerweekly.com/feature/Surveillance-capitalism-in-the-age-of-COVID-19, accessed on 10 July 2020.

15 Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing (Interim guidance), 28 May 2020, p.2, available at WHO/2019-nCoV/Ethics_Contact_tracing_apps/2020.1.;WHO contact tracing (n 5), p. 4.

rather than 'single solutions' for contact tracing[16] and not as a replacement for contact tracing teams.[17] The apps deployed by Bahrain, Kuwait, and Norway were dubbed as incompatible with the requirements of necessity and proportionality for surveillance in the context of a public health response as they were broadcasting the locations of users to a government database in real-time.[18] Norway pulled its contact tracing app due to such concerns.[19] In Israel, the Shin Bet, the internal security agency that is notorious for carrying military operations in the occupied territories in Palestine, has been able to access the location data of mobile phone users to trace those who have been close to confirmed patients.[20] Such unprecedented expansion of its powers has raised concern[21] and the Supreme Court of Israel has banned the agency from tracking the phone location of the infected until new laws are passed.[22] The COVID-19 crisis is said to have allowed India to accelerate the process of deploying surveillance technologies.[23] The Aarogya Setu app, developed by the government, aside from tracing contacts, can also access a smartphone's data and contacts and utilize built-in sensors such as the microphone.[24]

In April 2020, over 300 academics signed a statement favoring decentralized proximity tracing applications over centralized models,[25] as it was considered to have better privacy benefits.[26] But recent studies have gone on to show that even a decentralized contact-tracing app is not free from privacy concerns.[27] This indicates that even experts have not been able to identify the best practices of contact tracing surveillance technology. Although the surveillance measures to tackle COVID-19 are supposedly temporary,

16 WHO contact tracing (n 5), p. 4.

17 Ibid.

18 Nick Statt, 'Gulf states using COVID-19 contact tracing apps as mass surveillance tools, report says', *The Verge*, 16 June 2020, available at https://www.theverge.com/2020/6/16/21293363/COVID-19-contact-tracing-bahrain-kuwait-mass-surveillance-tools-privacy-invasion, accessed on 1 July 2020.

19 Natasha Lomas, Norway pulls its coronavirus contacts-tracing app after privacy watchdog's warning, *TechCrunch*, 15 June 2020, available at https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/, accessed on 23 July 2020.

20 Tom Bateman, 'Coronavirus: Israel turns surveillance tools on itself', *BBC*,12 May 2020, available at https://www.bbc.com/news/world-middle-east-52579475, accessed on 3 July 2020.

21 Ibid.

22 'Coronavirus: Israeli court bans lawless contact tracing', *BBC*, 27 April 2020, available at https://www.bbc.com/news/technology-52439145, accessed on 23 July 2020.

23 Aadil Brar, 'COVID-19 Boosts India's Growing Surveillance State', *The Diplomat*, 14 April 2020, available at https://thediplomat.com/2020/04/COVID-19-boosts-indias-growing-surveillance-state/, accessed on 10 July 2020.

24 Ibid.

25 Alex Hern, 'Digital contact tracing will fail unless privacy is respected, experts warn', *The Guardian*, 20 April 2020, available at https://www.theguardian.com/world/2020/apr/20/coronavirus-digital-contact-tracing-will-fail-unless-privacy-is-respected-experts-warn, accessed on 19 July 2020.

26 Douglas Busvine, 'Rift opens over European coronavirus contact tracing apps', *Reuters*, 20 April 2020, available at https://uk.reuters.com/article/uk-health-coronavirus-europe-tech-idUKKBN2221U6, accessed on 28 July 2020.

27 Serge Vaudenay, 'Analysis of DP3T: Between Scylla and Charybdis', *Cryptology ePrint Archive*, 8 April 2020, available at https://eprint.iacr.org/eprintbin/getfile.pl?entry=2020/399&version=20200409:125022&file=399.pdf, accessed on 28 July 2020.

the data collected and the effect of such data collection are said to be everlasting. The concern of public health has prompted governments and authorities over the world to take drastic measures but the effect of these measures may have serious implications for human rights long after the end of this pandemic. The surveillance measures implemented after the Attacks of 9/11 later went on to become a permanent fixture. Once the infrastructures for surveillance are put into place, it's hard to imagine authorities ever taking them down. Human Rights Watch and more than 100 other human rights organizations have called on States to ensure privacy and human rights and not "*usher in a new era of greatly expanded systems of invasive digital surveillance*", in the name of containing the pandemic through digital technologies.[28]

How much Surveillance is actually needed?

After the 9/11 attacks, surveillance has become a regular fixture in combatting terrorism and for tightening national security. Seeing that even terrorists have embraced technology,[29] the governments around the world have not felt shy to resort to new technological advances in the field of surveillance. It became somewhat a normal practice for the states to sacrifice all interests in privacy just to achieve just the slightest gain in security.[30] The enactment of the USA PATRIOT Act has considerably increased the US government's authority to use surveillance in the domestic and international context and removed several restrictions that safeguarded personal privacy.[31] It had been immensely controversial and has a far-reaching global impact.[32] As failing to give priority to state surveillance would put the state and its population at risk, it was considered necessary and legitimate.

Surveillance measures that compromised privacy were thus justified through the notion that "*privacy is not an absolute right but security is.*"[33] But authorities often over-emphasize

---

[28] 'Mobile Location Data and COVID-19: Q&A', *Human Rights Watch,* 14 April 2020, available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-COVID-19-qa, accessed on 1 July 2020; Danny Bradbury, 'Rights groups appeal to governments over COVID-19 surveillance', *Naked security by SOPHOS*, 2020, available at https://nakedsecurity.sophos.com/2020/04/06/rights-groups-appeal-to-governments-over-COVID-19%20surveillance/, accessed on 10 July 2020.

[29] Steven Swinford, 'Privacy has never been an absolute right: U.K. electronic spy agency urges Facebook, Twitter, to help stop terrorists', *The Telegraph*, 2014, available at http://news.nationalpost.com/news/privacy-was-never-an-absolute-right-u-k-electronic-spy-agency-urges-facebook-twitter-to-help-stop-terrorists, accessed on 10 July 2020.

[30] Kenneth Einar Himma, 'Why Security Trumps Privacy', in Adam D Moore (ed), *Privacy, Security and Accountability Ethics, Law and Policy,* Rownman & Littlefield International Ltd, Lanham, 2016, p. 148.

[31] See Walter Peissl, 'Surveillance and Security: A Dodgy Relationship', *Journal of Contingencies & Crisis Management* p. 19, volume 11:1, 2003; See Cary Stacy Smith and Li-Chung Hung, *The Patriot Act issues and controversies*, Charles C Thomas Publisher, Springfield, 2010.

[32] Krystal Lynn Conniry, *'National Security, Mass Surveillance, and Citizen Rights under Conditions of Protracted Warfare',* Master of Science, Portland State University, 2016, p. 7.

[33] Lseamnesty, 'Privacy advocate and security expert clash at debate over mass surveillance', *LSE Su Amnesty International*, 2016, available at https://lseamnestyinternational.wordpress.com/2016/02/12/privacy-advocate-and-security-expert-clash-at-debate-over-mass-surveillance/, accessed on 1 August 2020.

the role of surveillance in combatting terrorism. Although data retained through surveillance can be also used for serious crime detection and pre-crime prediction,[34] the prevention of crimes or terrorism is not fully dependent on surveillance measures. Tackling problems like terrorism is not only about catching a perpetrator in the act or preparation, but also requires imparting proper religious and moral education, eradicating social and economic inequalities, discrimination; cutting the sources of terrorism funding, and various others steps. Identifying surveillance as the only solution to stop terrorism and other crimes over-simplifies the underlying problems and in terms may help in the escalation of the problem. Again gathering large collections of personal data can make it possible for the governments to be more "citizen-focused" and offer services that are tailored to the needs of the citizens.[35] But such data could be collected through voluntary participation of the citizens, without resorting to any massive mass surveillance measures.

Regimes that are increasing surveillance apparatus to combat the COVID-19 Pandemic are over-emphasizing its role. It cannot be denied that surveillance measures can reduce the burden of the health officials and authorities in containing the virus, but even the apps and technology that only serve a specified and compelling health need cannot work miracles. 'Manual contact tracing' and facilitating 'access to accurate testing and treatment' have proven to be effective mechanisms in combatting the pandemic.[36] COVID-19 apps can prove to be helpful only as a part of a larger governmental response.[37] Over-relying on surveillance technologies will greatly undermine the proper mechanism needed to contain this pandemic.

Negative Impact of Surveillance

Even the introduction of the slightest amount of surveillance can have long-lasting effects on the way of life of citizens of a country. A study has found that "*merely hanging up posters of staring human eyes is enough"* to alter people's behavior.[38] Mass surveillance technologies can potentially affect large sections of the public and can endanger privacy and the personal autonomy flowing from it.[39] The realization of constant observation

[34] See B Carlton and Jude Mcculloch, 'Preempting justice: suppressing of financing of terrorism and the "war on terror"', *Current Issues in Criminal Justice* p. 397, volume 17:3, 2006.

[35] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, 2008-2009, United Kingdom, volume 1, p. 24, para. 92.

[36] 'COVID-19 Apps Pose Serious Human Rights Risks', *Human Rights Watch*, 2020, available at https://www.hrw.org/news/2020/05/13/COVID-19-apps-pose-serious-human-rights-risks, accessed on 1 July 2020.

[37] Paul Schwartz, 'Protecting privacy on COVID-19 surveillance apps', *Iapp*, 2020, available at https://iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps/ , accessed on 11 July 2020.

[38] Sander van der Linden, 'How the Illusion of Being Observed Can Make You a Better Person', *Scientific American*, 2011, available at http://www.scientificamerican.com/article/how-the-illusion-of-being-observed-can-make-you-better-person/ accessed on 26 July 2020; See Ryan Calo, 'People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship', *Penn State Law Review*, p.1, volume 114:3, 2010, available at http://ssrn.com/abstract=1458637, accessed on 2 August 2020.

[39] *Surveillance: Citizens and the State* (n 35), p. 26, para. 100.

or the slightest fear of it can make the 'development of the self' nearly impossible.[40] If the authorities can make such an intrusion, they will have the power to interfere with one's choices or self-representation.[41] Individuals who know that they are surveilled, become more self-conscious about their interaction, about what they say, and may even become less willing to enter specific public places.[42] Although the impact of surveillance on right to privacy has always been the subject of debate, surveillance measures have the potential to affect other rights too.

Realization of freedom of expression, freedom from discrimination, and freedom of assembly and association are somehow connected to surveillance. Surveillance has time and again encouraged discrimination due to its use in racial profiling[43] In fact the use of surveillance has been historically linked to the European colonizers.[44] The Dutch in Southeast Asia, the French in Africa, the British in India and North America, and the Belgians in Rwanda have all used fingerprinting, census taking, map-making, profiling, and other basic tools of surveillance to rule the colonies.[45] During World War II, the Japanese Americans were interred by the USA, through the use of census data.[46] Even in modern times, surveillance measures have been used to create "Zones of invisibility, exclusion, and death" – areas where "undesirable" people such as migrants, refugees, minorities, poor communities live.[47] Such areas are ripe with human rights violations and are severely underprivileged. The more the government resorts to profiling, no matter whatever the criteria are, the more they run the risk of stigmatization, discrimination, and social exclusion.

Besides surveillance measures are often used by regimes to silence opposition and dissent. Governments have used data collected through surveillance to silence journalists, activists, and minorities.[48] FBI routinely monitored Dr. Martin Luther King, Jr. and other prominent civil rights leaders, organizers, and activists, through 'illegal wiretaps, photographic surveillance, and physical observation of movements.'[49]

---

40 See Jeffrey Rosen, 'Out of context: the purposes of privacy', *Social Research* p. 209, volume 68:1, 2001.

41 See Titus Stahl, 'Indiscriminate mass surveillance and the public sphere', *Ethics and Information Technology* p. 33, volume 18:1, 2016.

42 Moira Paterson, 'Surveillance in Public Places and the Role of the Media: Achieving an Optimal Balance', *Media and Arts Law Review* p. 241, volume 14:3, 2009, p. 249.

43 Clive Norris & Gary Armstrong, 'CCTV and the Social Structuring of Surveillance', *Crime Prevention Studies* p. 157, volume 10, 1999, p. 175.

44 Dhakshayini Sooriyakumaran, 'Surveillance will not save us from COVID-19', *Al Jazeera*, 21 May 2020, available at https://www.aljazeera.com/indepth/opinion/surveillance-save-COVID-19-200520095528251.html , accessed on 3 July 2020.

45 Ibid.

46 David Murakami Wood, 'A Report on the Surveillance Societ For the Information Commissioner by the Surveillance Studies Network', 2006, p. 3, para. 2.6.

47 Dhakshayini Sooriyakumaran (n 44).

48 'Five reasons to care about mass surveillance', *Amnesty International,* 2015, United Kingdom, available at https://www.amnesty.org.uk/blogs/ether/five-reasons-care-about-mass-surveillance-edward-snowden-gchq-nsa-citizenfour, accessed on 1 July 2020.

49 Beverly Gage,'What an uncensored letter to M.L.K. reveals', *The New York Times Magazine*, 11 November 2014, available at https://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html, accessed on 1 July 2020.

Black Lives Matter, an activist movement aimed at combatting systemic racism, police brutality, and racially motivated violence against African-American people in the USA has been frequently surveilled.[50] Besides, constant, pre-emptive mass surveillance can potentially distort the nature of the relationship between an individual and the state.[51] Carrying out surveillance on the whole or a distinct section of the population all the time gives them the notion that the state considers all of them as potential criminals and law-breakers. As it gives the citizen the notion that they cannot be trusted,[52] the trust between the people and its government begins to deteriorate. Anything that undermines people's trust in the state can generate resistance and make the relationship between the individual and the state, "antagonistic."[53] Not to mention it also contradicts the legal principle that *"coercive measures should only be used against people when there are reasonable grounds to suspect them of criminal activity."*[54]

It is often argued, that there is virtually no privacy available since social media and tech companies have all our personal information. It has been argued that Google and Facebook might know an individual better than he knows himself.[55] Thus, a question arises – Why would a person in an Asian country, like Bangladesh prefer Facebook to have all his information rather than his government, if he doesn't have anything to hide? While breach of privacy by tech companies is also a matter of great concern, unlike governments, the tech companies do not have the power to penalize, discriminate and put sanctions on an individual. While a foreign entity may have more information about an individual, a person's fate rests with the government of his own country, under whose jurisdiction he resides. Democracies with traditions of strong rule of law and powerful oversight institutions have failed to properly ensure individual human rights in undertaking surveillance programs.[56] And the situation is far worse in the weaker democracies.[57]

---

50 George Joseph,'Feds regularly monitored Black Lives Matter since Ferguson', *The Intercept*, 2015, available at https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/, accessed on 1 July 2020.

51 *Surveillance: Citizens and the State* (n 35), p. 27, para. 105.

52 Ibid, para. 107.

53 Ibid, para. 108.

54 Pieter Kleve et.al, 'Surveillance technology and law: the social impact', *International Journal of Intercultural Information Management* p. 2, volume 1:1, 2007.

55 See James Carmichael, 'Google Knows You Better Than You Know Yourself', *The Atlantic*, 19 August 2014, available at https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/, accessed on 4 August 2020; Jon Evans, 'When Facebook Knows You Better Than You Know Yourself', *TechCrunch*, 24 October 2015, available at https://techcrunch.com/2015/10/24/when-facebook-knows-you-better-than-you-know-yourself/, accessed on 4 August 2020.

56 Steven Feldstein, 'The Global Expansion of AI Surveillance: Distinguishing Between Legitimate and Unlawful Surveillance', *Working Paper,* Carnegie Endowment for International Peace, 17 September 2019, p. 12.

57 Ibid, p. 13.

Requirements of a Lawful Surveillance

Whenever a government intrudes into any rights of the citizens, it is incumbent upon them to justify it.[58] Measures of surveillance must be such as to keep the 'interference' to what is 'necessary in a democratic society".[59] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression have affirmed that any interference with privacy must be provided by law, necessary to accomplish a legitimate aim, and proportionate to the aim sought.[60] Based on the practice of the Human Rights Committee,[61] as well as the wording of the European Court of Human Rights, International Covenant on Civil and Political Rights, and other relevant legal documents, the surveillance can be conducted on the fulfillment of the following three conditions:

(i) In accordance with the law

The wording of almost all legal documents refers that any interference to privacy must not be arbitrary and in accordance with the law. Since surveillance limits a person's right to privacy, measures must be conducted in accordance with a law that has been enacted to regulate such surveillance. It is not enough that such surveillance is permissible under the constitution. *General Comment 16* affirms that the collection of personal information by public authorities "must be regulated by law."[62] Surveillance measures having 'some basis in domestic law' ensures that it is accessible to the person concerned, is foreseeable as to its effects,[63] is relatively detailed,[64] sufficiently provides for adequate protection against abuse of power,[65] is precise, effective, and comprehensive.[66] Such law should not confer unfettered discretion.[67] The domestic statute should also specifically set out the

---

58 Anthony Ha, 'Edward Snowden's Privacy Tips: "Get Rid of Dropbox," Avoid Facebook And Google ', *TechCrunch,* 2014, available at techcrunch.com/2014/10/11/edward-snowden-new-yorker-festival, accessed on 13 July 2020.

59 *Big Brother Watch v. UK*, European Court of Human Rights, Judgment, 2018, Application nos. 58170/13, 62322/14 and 24960/15, para. 422.

60 The Right to Privacy in the Digital Age (n 1), paras.21- 23.

61 '*General Comment 27: Freedom of Movement (Article 12)'*, UN Doc CCPR/C/21/Rev.1/Add.9, 2 November 1999, paras. 14-15; '*General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*', HRI/GEN/1/Rev.9 (Vol. I), 8 April 1988, paras. 3,4,8; *Tooten v Australia*, United Nations Human Rights Committee, 1994, Communication No 488/1992, UN Doc CCPR/C/50/D/488/1992, para. 8.3.

62 Ibid, General Comment No. 16, para. 10.

63 *Roman Zakharov v. Russia,* European Court of Human Rights, Judgment, 2015, Application no. 47143/0, para. 228.

64 Ibid, para. 231; See *Huvig v France,* European Court of Human Rights, Judgment (Merits and Just Satisfaction), 1990, Application No 11105/84.

65 See *Liberty and Others v. The United Kingdom,* European Court of Human Rights, Judgment, 2008, Application no. 58243/00*; Szabo and Vissy v. Hungary,* European Court of Human Rights, Judgment, 2016, Application no. 37138/14.

66 Kieren McCarthy, 'European human rights court rules mass surveillance illegal', *The Register*, 2016, available at http://www.theregister.co.uk/2016/01/20/human_rights_court_rules_mass_surveillance_illegal/, accessed on 31 July 2020.

67 '*General Comment No. 34. Article 19: Freedoms of Opinion and Expression*', UN Doc CCPR/C/GC/34, 12 September 2011, para. 25.

details regarding; [68] (i) the categories of people who can be subjected to interception; (ii) the nature of the offenses which may necessitate an interception order; (iii) duration of such interception; (iv) the procedures to be followed for examination, use and storage of such obtained data; (v) the precautions to be undertaken when communicating the data to other parties, and (vi) circumstances in which the obtained data can be erased or destroyed. The law should also be compatible with other relevant human rights obligations, including non-discrimination. Therefore, all aspects of a surveillance measure and data collection from such measure, from initiation to continuation, to its minute details to cessation, must be covered by the law.

(ii) Legitimate aim

Any surveillance measures must be conducted for the fulfillment of a legitimate aim. European Convention on Human Rights provides a comprehensive list of legitimate aims, which includes the protection of health, rights, and freedoms, among others.[69] Constitutions and legislations that deal with surveillance or privacy should contain the circumstances under which surveillance may be carried out. But such an aim should be clear and specific and not subject to any vagueness. Vague notions of National Security have been often used by authorities to deploy surveillance measures without any adequate safeguards.[70] Only randomly stating a legitimate aim is not enough to conduct surveillance. There must be reasonable ground to avail surveillance for the fulfillment of such aim. In *Zakharov v Russia,* the European Court of Human Right's Grand Chamber stated that surveillance authorized on 'national, military, economic or ecological security grounds' are insufficient, requiring that any authorization must be based on a 'reasonable suspicion against a person concerned.'[71]

(iii) Necessity and proportionality.

It is often seen that surveillance measures that are deployed under the guise of a legitimate aim, are more than what is necessary and required for achieving such aim. Thus, comes in the requirement of necessity and proportionality of surveillance. Necessity and proportionality of surveillance mean that the interference caused by the surveillance cannot be greater than what is necessary to address a pressing social need[72] or as stated under the Inter-American jurisprudence, adequate to the legitimate aim pursued by such measures.[73] In *Klass v Germany*[74] and later in *Zakharov v Russia*,[75] the

68 *Roman Zakharov v. Russia* (n 63), para. 231.

69 The European Convention on Human Rights (formally the Convention for the Protection of Human Rights and Fundamental Freedoms), 3 September 1953, ETS 5, Rome, 4 November 1950, art. 8(2).

70 Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April, 2013,UN Doc A/HRC/23/40, para. 58.

71 *Zakharov v Russia* (n 63), para. 260.

72 Bernadette Rainey, Elizabeth Wicks, & Clare Ovey, *The European Convention on Human Rights*, Oxford University Press, United Kingdom, 6th edition, 2014, p. 325.

73 *Case of Fontevecchia y D`Amico v. Argentina*, Inter-American Commission on Human Rights, Merits, Reparations and Costs, 2011, Series C No. 238, para. 53.

74 *Zakharov v Russia* (n 63), para. 48.

75 *Klass and Others v. Germany,* European Court of Human Rights, Judgment, 1978, Application no. 5029/71,

European Court of Human Rights emphasized that states do not enjoy an unlimited discretion to subject persons within their jurisdictions to secret surveillance and *"may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."* Hence, having a legitimate aim to curtail one's right to privacy is not sufficient for surveillance. It is also mandatory to show that such surveillance is necessary for that legitimate aim and should be carried out only in proportion to the specific target.

Besides these three requirements, there has been a common practice in many jurisdictions that any surveillance measures are to be authorized and sanctioned by an independent and impartial judicial authority. The idea pans out from the fact that most of the surveillance measures are related to criminal matters or national security, and thus warrant or order from the court of law is necessary and that intervention of a judicial authority works as a strict safeguard against abuse of power by the government. According to Korean National Human Rights Commission, the absence of prior judicial authorization for accessing the data collected through surveillance, by police, violates international human rights.[76] The Communications Assistance for Law Enforcement Act of 1994 in the USA; Coercive Means Act as amended by the Act 1995/402 in Finland; Criminal Procedure Code (Strafprozeßordnung, StPO), 1987 of Germany; The Communications Interception Law, 1999 of Japan; The Protection of Communications Secrets Act, 1993 of South Korea; The Crimes Act 1961 and the Misuse of Drugs Amendment Act 1978 of New Zealand; the Criminal Procedure Act, 1981 of Norway; The Republic Act No. 4200 of the Philippines; The Code of Criminal Procedure, 1997 of Poland, etc. contains provisions for a warrant or prior approval of a court of law to conduct surveillance.

There have been many instances of contrary practices, where the prosecutor[77] or any member of the executive branch[78] determines the necessity of any surveillance measure. Leaving the decision to the executive branch is quite tricky as mostly their decisions are based on subjective satisfaction and are not qualitatively much different from the decision to be solely left to the law enforcing bodies or any other entity carrying out the surveillance. Even nurturing a practice where judicial affirmation is required to carry out surveillance cannot be said to be a full assurance of misuse of surveillance measures. But it is comparatively better than leaving the decision fully at the hand of the executive branch or the law enforcing agencies. Additionally, it is desired that the entity carrying out the surveillance should inform the judicial authority about the progress they have made through surveillance to properly assess the feasibility and continued legality of such measures.

---

para. 49.

76 *Korean Constitutional Court's Decision 2010 Hunma 47*, 252 (consolidated) announced 28 August 2012; *Korean High Court*, October, 2012; *Seoul High Court*, 2011Na19012.

77 National Security Law, 1991 (Law No. 51/1991), Romania, art. 13.

78 The Regulation of Investigatory Powers Act, 2000, United Kingdom, s. 5.

The Legality of Mass Surveillance

The validity of mass surveillance has been a matter of controversy for quite some time. Even many experts who are tolerant of surveillance are skeptical of the use of mass surveillance. Unlike targeted surveillance, mass surveillance requires no reasonable suspicion of wrongdoing or probable cause.[79] In matters regarding terrorism, crime detection, and national security, targeted surveillance is deemed to be more preferable to mass surveillance. There is no inherent prohibition on mass surveillance measures. But still, whether it's targeted or mass surveillance, both must satisfy the requirements of the legislation, legitimate aim, necessity, and proportionality.

Rather than an umbrella approach, courts have rather proceeded on a case-by-case basis to scrutinize mass surveillance measures. In *Zakharov v Russia*, the Grand Chamber of the European Court of Human Rights held that the Russian system for permitting surveillance across mobile networks, which required the network operators to install equipment for the interception of all telephone communications without prior judicial authorization, violated right to respect private and family life under Article 8 of the European Convention on Human Rights[80] Similarly in *Szabo v Hungary,* the Court held that there had been a violation of Article 8 of the convention as the surveillance powers of the Hungarian intelligence agency contained in the Police Act 1994, included virtually everyone in the country and was without an assessment of whether such measures were strictly necessary.[81] In *S and Marper v. The United Kingdom*, the ECHR held that keeping the DNA profiles of individuals not convicted of a criminal offense breached Article 8 of the Convention.[82] Again in *Digital Rights Ireland and Seitlinger and Others*, the Court of Justice of the European Union ruled that data retention measures apply to persons, for whom there is no evidence suggesting that their conduct might have even an indirect or remote link to serious crimes, are disproportionate.[83] The requirements of surveillance in public health crisis lean more towards mass-oriented than targeted. Public health has been widely regarded as a valid ground for derogation of rights. But still, the measures need to adhere to the proportionality of needs.

Thus any COVID-19 app or technology that may affect the rights of the masses beyond limiting the spread of the disease and facilitating public health authorities to manage the risk through monitoring the longer-term trends of transmission and the changes in the virus,[84] are unlawful. But the problem stands because the line which separates the lawful use of surveillance and technology from the unlawful is almost invisible.

---

79 Ben Beaumont, 'Easy guide to mass surveillance', *Amnesty International*, 2015, available at https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/, accessed on 12 July 2020.

80 *Zakharov v Russia* (n 63).

81 *Szabo and Vissy v Hungary* (n 65).

82 See *S and Marper v United Kingdom*, European Court of Human Rights, Judgment, Application nos. 30562/04 and 30566/04.

83 See *Digital Rights Ireland and Seitlinger and Others*, Court of Justice of European Union, 2014, Joined Cases C-293/12 and C-594/12, para. 58.

84 Surveillance strategies for COVID-19 human infection, Interim guidance, *World Health Organization,* 10 May 2020, p. 1c available at WHO/2019-nCoV/National_Surveillance/2020.1.

Data collected through lawful surveillance, which are essential for containing the virus can be simultaneously or at a later period be used for impermissible purposes. Thus, it is almost impossible to put a restriction on certain measures because, during the pandemic, the concern for public health is set to take priority over other rights.

Impact of COVID-19 Apps and Technology in the Society

Whenever liberties are sacrificed to meet a threat, they are not likely to be regained easily.[85] New governmental powers, created to coerce private citizens during emergencies, are not toned down after the crisis has been subdued.[86] According to Edward Snowden, the new powers introduced by states to combat the coronavirus outbreak will become permanent even after the crisis has been controlled.[87] WHO itself has warned that surveillance during public health emergencies *"can quickly traverse the blurred line between disease surveillance and population surveillance."*[88] While the question may arise that since surveillance measures have been in place long before the pandemic came into being, what can the new measures and the new data, which are significant health-related, possibly change.

Firstly, some of the countries will use the excuse of the pandemic to introduce surveillance measures that didn't exist before. Some countries will take the existing surveillance measures to such heights, which would not have been possible in ordinary times or which would have taken years or even decades to implement. Support for legislation excusing certain COVID-19 apps from general privacy restrictions has surfaced.[89] Yuval Noah Harari has warned that resorting to surveillance technologies, such as contact tracing apps, in response to the COVID-19 pandemic might constitute *"an important watershed in the history of surveillance."*[90] According to him, such measures may mark *"a transition from 'over the skin' to 'under the skin' surveillance."*[91] This means that if governments can record the body temperature, blood pressure, and heart rate of an individual under different circumstances, it can easily learn their liking and disliking.[92] As a result, the entity in control of such data can easily predict the feelings of an

---

85 Marie-Helen Maras, 'The social consequences of a mass surveillance measure: What happens when we become the 'others'? ', *International Journal of Law, Crime and Justice* p. 65, volume 40:2, 2012, p. 66.

86 Robert Higgs, *Crisis and Leviathan: Critical Episodes in the Growth of American Government*, Oxford University Press, New York, 1989, chp. 4.

87 Isobel Asher Hamilton, 'Edward Snowden says COVID-19 could give governments invasive new data-collection powers that could last long after the pandemic', *Business Insider*, 27 March 2020, available at https://www.businessinsider.com/edward-snowden-coronavirus-surveillance-new-powers-2020-3, accessed on 3 July 2020.

88 WHO Ethical Considerations (n 15), p. 1.

89 Kelly Servick, 'Cellphone tracking could help stem the spread of coronavirus Is privacy the price?', *Science*, 2020, available at https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price, accessed on 3 July 2020.

90 Yuval Noah Harari, 'Yuval Noah Harari: the world after coronavirus', *Financial Times*, 2020, available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75, accessed on 13 July 2020.

91 Ibid.

92 Ibid.

individual and also manipulate them.[93]

Secondly, the surveillance measures will escalate discrimination and discriminatory practices. Glimpses of such practices are already evident from the disproportionate number of death of people of color from COVID-19 in the USA and Britain, use of coronavirus stay-at-home orders and policies making masks mandatory, by the police to harass and abuse Black Americans in the USA, disproportionate realization of public health order compliance fines from the indigenous peoples and migrants in Australia.[94]

Thirdly, surveillance measures could usher discrimination towards new groups of people. On top of the prevalent discriminations in society, surveillance measures could risk sick and immunocompromised people being subject to discrimination.[95] In the South Asian countries, there have been incidents of obstruction of burial and funeral rites and incidents of obstructing people from an urban area to visit their village homes due to fear of the virus. People living in slums have been afraid to take coronavirus tests or reveal to others about showing symptoms in the fear that they will be evicted from the slums. During the time of pandemics, misinformation and superstitious belief are ripe and the slightest exposure of data that a particular class of people or people living in a particular area are more likely to be infected could perpetuate hatred, violence, and even discriminatory practices towards them. During the time of the Black Death, the Jews, who were comparatively less affected by the plague due to their sanitary practices, were blamed and prosecuted by the Christians.[96]

Although we have come a long way from those dark ages, the truth is, times of crisis can bring out both the best and worst in us. In the wake of the COVID-19, there has been a significant rise in anti-Asian racism and xenophobia,[97] due to the origin of the virus. Besides WHO has additionally cautioned that implementation of digital technologies in contact tracing can harm through incorrect medical advice based on self-reported symptoms and systematic exclusion of some members of society who do not have access to such technologies.[98]

The use of COVID-19 apps and technology can proliferate an era of increased and more sophisticated surveillance, where discrimination, inequality, and mutual hatred become an accepted norm. Such a society can in no way be regarded as more safer and acceptable than a society suffering from a global pandemic.

---

93 Ibid.

94 Ibid.

95 Dhakshayini Sooriyakumaran (n 44).

96 Berel Wein, 'The Black Death', *JewishHistoryorg*, available at https://www.jewishhistory.org/the-black-death/, accessed on 4 August 2020.

97 Press Release, 'Secretary-General Denounces 'Tsunami' of Xenophobia Unleashed amid COVID-19, Calling for All-Out Effort against Hate Speech', SG/SM/20076 United Nations, 8 May 2020, available at https://www.un.org/press/en/2020/sgsm20076.doc.htm, accessed on 13 2020.

98 WHO contact tracing (n 5), p. 4.

Additional requirements for Surveillance during Public Health Emergencies

The criteria set for assessing the legality of surveillance measures may not be sufficient to detect whether the apps and technology used for COVID-19 contract tracing violate human rights or whether data collected through such measures are being used for other purposes. Many additional criteria and basic principles have been suggested by different human rights organizations and bodies in this circumstance. ACLU, a nonprofit organization that defends and preserves the rights and liberties of the people of the USA, have suggested that technology-assisted contract tracing must adhere to some basic principles such as being voluntary, non-punitive, being built with public health professionals, non-discriminatory, minimal reliance on central authorities, no data leakage, having an exit strategy, specifically targeted towards an epidemic, auditable and fixable, etc.[99] The suggestion also states that such measures should not displace non-technical measures.[100]In the letter signed by more than 100 human rights groups to the governments regarding the use of technology to combat the COVID-19 Pandemic, eight conditions were set for the governments to satisfy to enhance surveillance, some of the conditions being surveillance measures to be kept lawful and transparent so that third parties can evaluate them, having a time for the cessation of additional surveillance measures, only using the data collected for responding to the pandemic, give individuals the right to challenge the collection of their personal data, etc.[101] World Health Organization has extensively set out principles to guide ethical principles for the appropriate use of digital proximity tracking technologies for COVID-19 contact tracing.[102] The guideline proposes that any digital tools should not be adopted without proper evaluation and must be transparent, reader-friendly, limited data retaining, etc.[103] It also states that there should be accountability, remedies available for abuse, proper oversight, and should include the participation of relevant stakeholders.[104] All these guidelines and principles could be compiled to form a best practice manual for developing apps and technologies for COVID-19 contact tracing and if properly executed, they could be used for public health emergencies in the future.

Solutions that keep pace with the problem

As previously stated, emergency and crisis have been often used as an excuse to introduce extraordinary measures that violate human rights even after the end of the crisis. It is high time that such solutions are introduced that lasts long after the end of

99 Daniel Kahn Gillmor, 'ACLU White Paper — Principles for Technology-Assisted Contact-Tracing', *ACLU*, 2020, available at https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing, accessed on 16 July 2020.

100 Ibid.

101 Bradbury (n 28).

102 WHO Ethical Considerations (n 15), pp. 2-5.

103 Ibid.

104 Ibid.

the crisis, just like these extraordinary measures. These solutions should complement the existing legal requirements of valid surveillance; any measures available to determine to evaluate such legality and the widely accepted principles to conduct surveillance for contact tracing. These steps are as follows:

(i) *Pre-Launch Evaluation of the technology by an independent body along with the participation of civil society*

Deployment of any app, technology, that can surveil or gather data, no matter whatever be the nature or quantity of the data must be evaluated and regulated by an independent body with the help of experts. Evaluation and regulation don't imply resorting to legal devices. Evaluating surveillance technology will require independent bodies that can deal with surveillance measures and data collection initiatives as soon as such technology is developed and is ready for use or talks of such deployment takes place. Such a body will assess any actual or potential effects that a surveillance or data collection initiative may have on human rights issues such as privacy, discrimination, etc., while also proposing how to tackle and mitigate such effects. Findings of such body should be brought to attention to the relevant stakeholder. This body can directly move to the court with their finding and observation of the stakeholder if they believe that any measures in talks are not compatible with human rights. Lack of regulation and transparency allows governments to abuse their power of mass surveillance.

(ii) *Right to Information*

There are no assurances that either in good or bad faith, the data collected during the time of public health emergencies may not get added to the pre-existing databases. The right to information has been recognized as a human right due to being an integral part of the right to freedom of expression.[105] At present, around 120 countries have some form of legislation regarding access to information.[106] In a democratic society, any information in the control of the state should be made public and accessible, subject to some exceptions.[107] At least, when it comes to their own information, an individual should have unlimited access. Access to information laws could be used by citizens to inquire as to how much of his information has been acquired by the government or any other entities authorized to conduct surveillance. Such laws could assure that everyone has free access to all the information regarding himself which the authorities hold. Any information about any individual which is acquired through illegal means or acquiring which are illegal can be taken down through remedial procedures. This measure also conforms to the doctrine of "informational self-determination." This doctrine proposes that every individual has the right to control the flow of his or her

[105] *Universal Declaration of Human Rights*, 10 December 1948, UNGA 217 A (III), art. 19; *International Covenant on Civil and Political Rights*, 23 March 1976, 999 UNTS 171, New York, adopted 16 December 1966, art. 19; *American Convention on Human Rights*, 18 July 1978, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123, San Jose, 22 November 1969, art. 13.

[106] 'Right to Information: A Tool for People Power', *Transparency International*, 2019, available at https://www.transparency.org/en/news/right-to-information-people-power#, accessed on 28 July 2020.

[107] *Gomes Lund et al. (Guerrilha do Araguaia) v. Brazil,* Inter-American Commission on Human Rights, Preliminary Objections, Merits, Reparations, and Costs, 2010, Series C No. 219, para. 230.

personal data, but subject to restrictions fixed by the test of proportionality.[108] Access to information laws will clearly inform an individual whether the government has acquired information about him without his consent and thus will give him a chance to remedy it.

(iii) *Periodic Review*

Even after any surveillance measure has been sanctioned by regulatory bodies and competent judicial authorities, such measures and the technology must be reviewed regularly. This is necessitated because even measures that have been initially taken for lawful means may later succumb to unlawful ones or any defect in the technology which was initially not discovered, could later surface. In the age of ever-growing scientific inventions, sometimes it becomes hard to identify the implications of new technology, especially on human rights issues. Continued regulation of surveillance measures is essential to keep surveillance measures and technology up to date with human rights issues.

The European Court for Human Rights and the Court of Justice of the European Union have played a crucial role in the protection of privacy by limiting the ever-growing desire of states in Europe, to collect massive information about their citizens.[109] Such type of regional court is absent in Asia, the region that has become the hub of mass surveillance. Neutral regional courts would have been the proper institutions for keeping the governments in check regarding the deployment of invasive surveillance measures and even for other human rights violations.

Concluding Remarks:

Any secret surveillance measure has the potential to undermine or even destroy democracy under the cloak of defending it.[110] The phrase - "You have nothing to fear if you have nothing to hide" has often been used by the supporters of mass surveillance to justify measures that compromise privacy. The fact that the phrase is attributed to Nazi Joseph Goebbels,[111] is enough to justify the absurdness of such rhetoric. Justifying mass surveillance measures by saying that one has nothing to hide, means that one doesn't care about the violation of rights caused by such surveillance. After the 9/11 terror attacks, the USA government leveraged public fears to expand its surveillance

[108] *Surveillance: Citizens and the State* (n 35), p. 89, para. 383.

[109] Vera Rusinova , 'A European Perspective on Privacy and Mass Surveillance at the Crossroads', *WP BRP 87/LAW/2019*, National Research University Higher School of Economics, 2019, p. 3, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347711#, accessed on 2 July 2020.

[110] *Szabó and Vissy* (n 65); Sarah St. Vincent, 'Did the European Court of Human Rights Just Outlaw " Massive Monitoring of Communications" in Europe?', *Center for Democracy and Technology*, 2016, available at https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/, accessed on 28 July 2020.

[111] 'If you have nothing to hide, you have nothing to fear': MP accused of quoting Nazi leader', *TheJournalie*, 2015, available at https://www.thejournal.ie/surveillance-bill-goebbels-2426368-Nov2015/, accessed on 4 August 2020.

power, but it contributed little to making the country safer.[112] This has been a recurring phenomenon – the use of the public's helplessness and fear to introduce measures that oppresses them. A COVID-19 contact tracing app that stands in breach of legal requirements of surveillance and can create stigmatization and discrimination in the society is an infringement of the human rights of its potential user, even if it has not been used for any harmful purpose yet. The impact of the COVID-19 pandemic has already been felt in almost all sectors of human life. Currently, there is rarely any financial sector that has not incurred losses due to the pandemic. On top of that, this pandemic has already been termed the "Pandemic of Misinformation," due to the rapid spread of false information.[113] This has prompted people to act out in hostile nature towards each other and discriminate against others, due to fear. COVID-19 contact tracing apps and technologies which are supposed to benefit people in these trying times should not be the source of further discrimination, inequality, and human rights violation. Advocating for a blanket ban of COVID-19 contact tracing apps and technologies might not be a beneficial solution to the problem. Careful deployment of such apps and technology, maintaining proper legal and ethical measures, with the help of public health professionals is what we should rather aim at. It is alarming enough that more countries are embracing surveillance due to the gradual decline in the costs of technology. A global public health emergency should be the time to re-think about the better implementation of human rights and strengthen the ties of brotherhood, and not to reinforce inequality, oppression, and discrimination.

[112] Mike Giglio, 'Would You Sacrifice Your Privacy to Get Out of Quarantine?', *The Atlantic*, 22 April 2020, available at https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/, accessed on 3 August 2020.

[113] See J Kluger, 'A Pandemic of Misinformation',*Time,* volume 196(5-6), 2020, pp. 17-18.