


COMMENTARY

Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic

Titi Akinsanmi^{1,2,3,4} and Aishat Salami^{2,5,*} 

¹African Academic Network on Internet Policy, Ibadan, Nigeria

²Technology Consulting and Research, Lagos, Nigeria

³Technology Consulting and Research, Johannesburg, South Africa

⁴Technology Consulting and Research, Innisfil, Ontario, Canada

⁵Tech Hive Advisory, Lagos, Nigeria

*Corresponding author. E-mail: barraishat15@gmail.com

Received: 03 May 2021; **Revised:** 20 August 2021; **Accepted:** 04 September 2021

Key words: COVID-19; digital security; health safety; pandemic; privacy; trade-off

Abbreviations: COVID-19, Coronavirus disease 2019; CVC, Coronavirus Vaccine Certificate

Abstract

COVID-19 has impacted all aspects of everyday normalcy globally. During the height of the pandemic, people shared their (PI) with one goal—to protect themselves from contracting an “unknown and rapidly mutating” virus. The technologies (from applications based on mobile devices to online platforms) collect (with or without informed consent) large amounts of PI including location, travel, and personal health information. These were deployed to monitor, track, and control the spread of the virus. However, many of these measures encouraged the trade-off on privacy for safety. In this paper, we reexamine the nature of privacy through the lens of safety focused on the health sector, digital security, and what constitutes an infraction or otherwise of the privacy rights of individuals in a pandemic as experienced in the past 18 months. This paper makes a case for maintaining a balance between the benefit, which the contact tracing apps offer in the containment of COVID-19 with the need to ensure end-user privacy and data security. Specifically, it strengthens the case for designing with transparency and accountability measures and safeguards in place as critical to protecting the privacy and digital security of users—in the use, collection, and retention of user data. We recommend oversight measures to ensure compliance with the principles of lawful processing, knowing that these, among others, would ensure the integration of privacy by design principles even in unforeseen crises like an ongoing pandemic; entrench public trust and acceptance, and protect the digital security of people.

Policy Significance Statement

This research uses the COVID-19 pandemic to illustrate the prioritization of security (digital or otherwise) and health safety, over the peoples’ right to privacy—without informed consent. It raises the question of whether contact tracing measures can be deemed successful if the vast intrusion to privacy rights of persons is considered? The research concludes that privacy, safety, and security are not mutually exclusive even in crisis as experienced globally in the last 18 months with COVID-19. Critical to the successful deployment of any interventions is ensuring laws and policies developed should be done collaboratively engendering trust, with the goal of enabling the safety, security, and right to privacy of persons. Our research also recommends that there should be the

implementation of a principles-based trust framework including the centering and implementation of transparency and accountability in the use, collection, and retention of user data.

1. Definition of Terms

1.1. Privacy

Privacy is a person's choice to be "left alone"—free from any external interference or intrusion into what they have designated as their personal information (PI; Warren and Brandeis, 1890; FindLaw, 2019).

1.2. Health safety

Health safety (also referred to as health security) refers to "...the activities required to minimize vulnerability to acute public health events that endanger the collective health of populations living across geographic regions and international boundaries" (Aldis, 2009).

1.3. Digital security

The principle of digital security requires that appropriate technical or organizational measures are implemented when processing PI to protect the information against accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction, or damage.¹

2. Privacy and Digital Security

Privacy and security are mutually dependent.² Although both concepts require connected but different approaches, they are both key to enabling an individual or an organization's ability to be locally relevant and globally competitive. Privacy is focused on safeguarding the rights of individuals—the right to be left alone—while digital security is concerned with protecting the confidentiality, integrity, and availability (CIA) of information. Thus, while privacy establishes a normative framework for deciding who should legitimately have the capability to access and alter information, digital security implements those choices.

With rapid advancements in technological innovations in the data-driven economy, there are magnified digital security threats, which require countermeasures—from a privacy and security approach (Sicari et al., 2015). Protecting the privacy of individuals is integral to protecting data and securing systems that contain this data and networks through which this data traverses. These protections and safeguards minimize vulnerabilities to digital security threats and mitigate the harm caused by unauthorized access, collection, deletion, modification, and disclosure of data (Bambauer, 2013). Therefore, there must be enforcement of digital security and privacy policies to ensure data confidentiality and authentication within a digital economy. Together with the conventional security solutions, there is also the need to provide built-in security in devices to pursue dynamic prevention, detection, diagnosis, isolation, and countermeasures against data breaches (Bambauer, 2013).

2.1. Status of digital security in privacy protection

Digital security as a data protection principle broadly provides that an unauthorized person should not have access to data. In addition, data should be kept secured and not compromised. CIA is fundamental tenets in the development of digital security (Stewart et al., 2012). In managing the digital security of an organization, one or more of these principles must be in place.

¹ General Data Protection Regulation, Recital 39 and Article 591 (f); Modernized Convention 108, Article 7.

² Security provides individuals with the freedom to live their lives with dignity and personal autonomy, and make life choices free from fear and coercion, and privacy enables individuals "to achieve self-determination and develop their personalit[ies] free from coercion" (Maras, 2009).

In most industrialized countries, the right to privacy and the status of digital security in privacy protection is generally uncontroversial. Essentially, “everyone has the fundamental right to the protection of data, information, and communication against unauthorized access by third parties” (Cornelius, 2019). When it comes to developing countries³—“a country with little industrial and economic activity and where people generally have low incomes”⁴—the case appears to be different, with developing countries lagging in technological progress;—and right to privacy and the status of privacy in digital security is affected by a country’s digital reflection—which also reflects in its digital security protection, and privacy awareness.

In Canada, the federal privacy laws⁵ require organizations to make their employees aware of the importance of maintaining the confidentiality of PI and that care be used in the disposal or destruction of such to prevent unauthorized parties from gaining access (Cameron and Samadmoten, 2019). The PIPEDA⁶ also speaks explicitly to the collection, use or disclosure of PI in the course of commercial activity.

The principle of safeguards in PIPEDA similarly ensures that security safeguards are provided to protect the PI of data subjects.⁷

In comparison, one finds that a developing country like India gives no cognizance to the right to privacy. Instead, there is the right to personal liberty, which is often used to extend to the right to privacy. Its Personal Data Protection Bill was just passed in 2019 (Kumaraguru and Cranor, 2005).

A quick look on the African continent shows that, unlike the western countries where there is a recognized individual right to privacy, “there are arguments, rarely supported by empirical evidence, that group interests outweigh individual interests due to the culture of collectivism; hence privacy claims are less common” (Makulilo, 2015). One of the main results of a survey of the status of privacy protection in digital security in a developing country revealed that “there was a higher fear of being unable to access their data than the fear of privacy breaches” (Dev et al., 2019).

3. Health Safety Considerations and the COVID-19 Pandemic: Contact Tracing Apps

In December 2019, the spread of COVID-19 gained international attention with the World Health Organization declaring it a global pandemic on March 11, 2020. Governments worldwide resorted to track and trace technology and other data-driven tools to curb the spread of the virus (Zwitter and Gstrein, 2020). The enforcement of the health safety precautions, including the questioning of people about their travels and movements, entailed privacy-invasive measures. At the same time, privacy regulations were relaxed to protect the health safety of people. As the pandemic worsened and claimed more lives, more stringent measures that further infringed on people’s right to privacy were employed.

The COVID-19 pandemic illustrates and confirms the immense pressures both public and private entities face to widely collect, use and share individuals’ personal health data to facilitate a coordinated pandemic response (Bernier and Thompson, 2020). The interventions in response to the pandemic have revealed details about the actual or suspected illness and information and records of those around them. The pandemic has exposed Governments to a tug of war between protecting the safety of people by enforcing public health safety measures through tracking the corona virus to curtail its spread or strengthening privacy measures to protect the sensitive PI and personal health information of persons.

³ The OECD list of developing countries contains 182 countries and territories with low and middle income, based on their gross national income (GNI).

⁴ “Developing country.” Available at <https://dictionary.cambridge.org/us/dictionary/english/developing-country>.

⁵ Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA).

⁶ Office of the Privacy Commissioner of Canada (January 2008) *The Personal Information Protection and Electronic Documents Act (PIPEDA) in Brief*. Available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

⁷ Office of the Privacy Commissioner of Canada, “PIPEDA fair information principles” (16 September 2011). Available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.

We then face a situation where many countries, such as Singapore, applauded for proper management of the COVID-19 outbreak, actually “utilized aggressive surveillance measures to track, trace and isolate affected individuals.”⁸ China is stated to have made use of authoritarian and at first effective measures. In contrast, some countries like Italy and Spain, faced more caseloads with a more relaxed approach to the pandemic.

Therefore, the problem appears to be the delineation of the two concepts. Privacy and safety are seen as mutually exclusive, with the belief that one must be sacrificed at the expense of the other. Choosing between privacy and health safety has been regarded as a “false choice,” “a false trade-off,” on the basis that “we can achieve the public health benefits of data without accepting abusive and illicit surveillance” (Goldenfein et al., 2020). Of course, good data—“comprehensive and accurate information about who has been infected and how, and which interventions did or did not work” (Goldenfein et al., 2020)—is needed to curb the spread of COVID-19 effectively. However, what we witness is “vast profiteering as both governments, and corporate entities use the crisis to extract and commodify personal data... under these conditions, sacrificing privacy for health means yielding further control to governments and tech companies that have already gained undue power through technological means.”

We must state that though the two concepts of privacy and safety can be approached differently, they function best when they co-exist. A level of balance can be sought to be attained between privacy and health safety, such that “intrusions on privacy in the public interest are treated as exceptions rather than norms” (Goldenfein et al., 2020). These exceptions must be justified, with restriction of use to which such information collected in a crisis is put (Goldenfein et al., 2020). Also, legal mechanisms can be put in place to ensure “democratic control over new technological infrastructures” (Goldenfein et al., 2020) such that operating system providers, telecommunications companies, and app developers can be regulated and held accountable for data held during a crisis.

Many Governments are undecided on whether to use decentralized⁹ contact tracing apps with privacy and security enhancing designs or focus more on public safety by using a contact tracing model that processes more user data and therefore tracks a more significant percentage of individuals.

During the pandemic, people provide their data to map and combat the virus (purpose limitation) with the expectation that such data would not be used beyond the period. Even though it is not in contention that the contact tracing apps aim to promote public health, there is the fear that the data disclosed by users for contact tracing might be retained beyond the pandemic period. Therefore, it is not surprising that one of the major privacy concerns is that the monitoring technologies deployed to combat the pandemic would continue to be used post-COVID and used for purposes different from the primary reason for collecting the data (Goldenfein et al., 2020). This fear is aptly illustrated by Hu Yong, a professor at Peking University’s School of Journalism and Communication, when he asked, “has history ever shown that once the government has surveillance tools, it will maintain modesty and caution when using them?”¹⁰ The massive deployment and proliferation of surveillance cameras post the 9/11 incident in the United States of America further drives home this point. Following the global panic after 9/11, there was the “installation of radical new government data surveillance tools and practices, premised on the idea that the key to counterterrorism was data collection and analysis. As the counterterrorism debate was framed in terms of ‘privacy versus security,’ governments argued that the tangible threat of terrorism outweighed more abstract concerns about privacy, justifying pervasive surveillance as necessary for public safety. Much of that global surveillance constellation persists to this day, ‘even as evidence of its effectiveness is lacking’” (Kirchner, 2015; Goldenfein et al., 2020).

As Governments and stakeholders worldwide are focused on ensuring the health or safety of persons from COVID-19, cybersecurity issues seem to be on the rise. COVID-19 has presented an opportunity for cybercriminals to capitalize on the chaos of the pandemic and pounce on unsuspecting persons. “Attackers are using COVID-19 as bait to impersonate brands, thereby misleading employees and

⁸ Hao (2020).

⁹ A decentralized database has no central server where data is stored and/or located.

¹⁰ Hao (2020).

customers. This will likely result in more infected personal computers and phones. Not only are businesses being targeted, but end-users who download COVID-19 related applications are also tricked into downloading ransomware disguised as legitimate applications.”¹¹ Apart from the digital security risk from hackers, or threats from ransomware, phishing scams, and like threats, the data breach could result if the information of users who contact the virus is revealed. Such data breach inherent in the mass collection of data would violate the privacy and digital security rights of victims who, based on such information, could be “discriminated against, or denied some rights” (Bernier and Thompson, 2020).

Increased reliance on digital platforms during the outbreak of COVID-19 shows that legislative frameworks that would protect users’ privacy while instilling confidence and trust in the use of the platforms would go a long way in strengthening PI online.

In the aftermath of COVID-19, it is essential that cybersecurity practices are prioritized and effective cyber risk management measures put in place. Proactive steps must be taken, and measures put in place for detection and response to such attacks.¹²

4. Impact of Adopted Policies in Tackling COVID-19 in Developing Countries

The COVID-19 pandemic has caused countries worldwide to adopt policies to guarantee the health safety of its citizens. The burning question which arises with the adoption of these policies, is whether the health safety of individuals should be overly prioritized against their individual rights to privacy and digital security. The answer to whether one of these should override the other, depends among others, on country-specific regulations and cultural norms, as well as the state of COVID-19 infections in each region (Deloitte, 2020c).

The pandemic is challenging different facets of everyday life. Societal notions of justice are also questioned. For instance, it is said that Black Americans are 2.4 times more likely to die of COVID-19 than are White Americans. The COVID-19 policies and measures of different Governments, have diverse impacts on its people. For example, “the burden of home confinement is greater in an urban apartment with several family members than in less dense housing, the burden of discontinuing public transportation falls more harshly on those without cars, and the burden of closing nonessential businesses is more onerous for low-wage service workers who cannot telecommute and who have modest savings” (Rothstein, 2020).

Other interventions may also have adverse effects with particular respect to some groups of people; such as people with disabilities or preexisting health conditions, individuals experiencing homelessness, senior citizens, people with cognitive impairments, and immigrants who lack English fluency (Rothstein, 2020).

In most developing countries where there exists a higher percentage of lower-income people, and people with less access to smartphones, the use of location data on phones would be of less significance to this category of people. The result being that the health information collected through this medium would not extend to this group of people. The lesson from this, is that adopted policies should be continually evaluated to ensure specificity to a people, and allow the inclusion of all.

5. Evaluating the Trade-off between Privacy and Security: Post-COVID

The proliferation of COVID-19 impacted many aspects of everyday activity. In the face of the pandemic, the urgent need to ensure safety allowed people’s right to privacy to be quickly eroded. At the height of the pandemic, many people shared their PI with hopes of protecting themselves against the virus; monitoring technologies—contact tracing apps—for the collection and processing of data (such as location data,

¹¹ Deloitte (2020a).

¹² Deloitte (2020a).

travel data and medical data) were deployed to curtail and track the spread of the virus. However, many of these measures encouraged the trade-off of privacy for security or safety during the pandemic.

The COVID-19 pandemic illustrates the tendency of governments and other entities to trade privacy for safety or security. Although contact tracing apps ensure public safety by monitoring the spread of the coronavirus, the apps that monitor the location of suspected ill to inform or notify others who might have been within the vicinity raise unprecedented concerns about people's privacy. The trade-off that arises in a pandemic is that we sacrifice our personal data to save our lives or those around us. Regardless of the pandemic, interference of one's privacy rights should be proportionate and reasonable in the given circumstance.

Although in the face of a pandemic, where health safety and privacy are involved, it might be challenging to choose between the two. The dilemma arises in trying to decide what information is private and what information in the face of the pandemic must be available to the public for the sake of public interest and safety.

5.1. Enabling meaningful balance between privacy, health safety, and digital security in a pandemic

In facing the future, an important question is whether the health safety measures through monitoring interventions or contact tracing apps can be deemed successful if one considers the vast intrusion to privacy rights of persons? In answering this, we propose maintaining a balance between the concepts of privacy, health safety and digital security. There must be a refrain from viewing the concepts as mutually exclusive, with the belief that one must be sacrificed at the expense of the other; because although the concepts can be approached differently, they function best when they co-exist. Where the circumstances then require that the right to privacy be restricted for the sake of public interest and public health safety, mechanisms must be put in place;—for instance, provisions for the restriction to be reasonable, time-specific, and exceedingly necessary in the circumstance—for if the rights of individuals cannot be guaranteed, chaos resulting from violations of rights would be unavoidable. There can also be the implementation of regulations such as the Seattle Surveillance Ordinance (CB 118930), which allows for transparency, accountability, and public trust; by ensuring that “the public has the opportunity to weigh the costs and benefits of new surveillance technology—including the impact on civil liberties—before the City obtains it” (ACLU of Washington, 2017). Implementing such regulations would mandate Government agencies to consider the impact of surveillance technology, build public trust, and prevent the abuse of such technology. There is the proposal being fielded that big tech ought to be regulated as public utility (Scott, 2021) such that “contact tracing response, for instance, could be managed—from data collection to analysis to implementation—by democratically accountable public health authorities, for the sake of public health alone, and be shielded from both market and policing pressures” (Goldenfein et al., 2020).

Relating this to the incidences of trade-off in a pandemic, the benefits which the contact tracing apps offer in the containment of COVID-19 can be balanced with the need to ensure that there is no threat to the PI and the right to privacy and digital security of users. This balance can be maintained by ensuring that the data collected during the period is used strictly to ensure containment of the virus; through lawful, fair, and transparent use of the data; and controlled access to the data.

In addition, the use of decentralized contact tracing Apps used in combating COVID-19 should be applauded for minimizing privacy risks while ensuring the digital security and health safety of people. To this extent, we must emphasize the importance of putting adequate measures and safeguards in place to protect the privacy and digital security of users by ensuring transparency and accountability in the use, collection, and retention of user data. We also recommend complying with the principles of lawful processing, knowing that these factors, among others, would ensure integration of the principles of privacy, entrench public trust and acceptance, and protect the digital security of people.

In addition, as further digitalization and contactless interactions become widespread in the wake of the pandemic, digital literacy must be improved to ensure the public is prepared for the increasing change. Also, “societies will need to adopt specific regulations and revisions of existing laws to strike the right balance between such data collection and personal freedom as new technologies are adopted” (Park,

2021). Further, “a social consensus on the acceptable level of conditional data collection for public health safety and the appropriate methods for collection must be addressed head-on in preparation for the next pandemic” (Park, 2021).

6. Conclusion

It is expected that in a pandemic, “fundamental rights will have to be balanced against each other. The question is whether the outcome of the balancing exercise between the right to health and the right to privacy needs to be a limitation of the latter and if so, whether this limitation is necessary, proportionate and restricted in time” (Deloitte, 2020b). The incidences of the COVID-19 pandemic revealed that in focusing only on the safety of persons, the interventions in response to the pandemic revealed PI of actual or suspected ill, resulting in violation of privacy rights and trade-off of privacy for safety; and justified the fear that the urgency needed to curtail the virus might give way to the violation of privacy rights. Moving forward, we must not treat privacy, health safety, and digital security as mutually exclusive. In evaluating a trade-off, the aim should be the attainment of balance between the concepts. The balance can be attained by ensuring the health safety and digital security of persons while also protecting their right to privacy.

Acknowledgments. We want to express our sincere gratitude to the publishers of this article, and the peer review team, for creating an avenue for us to share our thoughts with the world. We also wish to thank all the people whose support, assistance, review, and criticism were a milestone in completing this paper.

Funding Statement. None.

Competing Interests. T.A., at the time of this submission, is an employee of Google in South Africa but is writing in her capacity as the lead researcher and consultant for Technology Consulting and Research. A.S. declares no competing interests exist.

Author Contributions. Conceptualization: T.A., A.S.; Data curation: A.S.; Formal analysis: T.A., A.S.; Resources: A.S.; Supervision: T.A.; Visualization: T.A.; Writing—original draft: A.S.; Writing—review and editing: T.A., A.S.

Data Availability Statement. Data availability is not applicable to this article as no new data were created or analyzed in this study.

References

- ACLU of Washington** (2017) *Seattle Adopts Nation’s Strongest Regulations for Surveillance Technology*, 31 July 2017. Available at <https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology>. Accessed on July 30, 2021.
- Aldis W** (2009) Health security as a public health concept: A critical analysis. *Revista Gerencia y Políticas de Salud* 8(17), 12–27.
- Bambauer, Derek E**, *Privacy Versus Security*, SSRN Scholarly Paper, papers.ssrn.com, SSRN Scholarly Paper ID 2208824 (Rochester, NY: Social Science Research Network, 2013).
- Bernier C and Thompson K** (2020) Privacy Law in the Context of Pandemics. Available at <http://www.privacyandcybersecuritylaw.com/privacy-law-in-the-context-of-pandemics>. Accessed on 3rd August 2021.
- Cameron A and Samadmoten D** (2019) *Canada - Data Protection Overview*, 8 November 2019. *DataGuidance*. Available at <https://www.dataguidance.com/notes/canada-data-protection-overview>. Accessed on 29th July 2021.
- Cornelius K** (2019) Privacy Perception in Developing Countries. Available at https://www.researchgate.net/publication/337211237_Privacy_Perception_in_Developing_Countries. <http://dx.doi.org/10.13140/RG.2.2.19821.95209>. Accessed on 5th August 2021.
- Deloitte** (2020a) COVID-19’s Impact on Cybersecurity. Available at <https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html>. Accessed on 5th August 2021.
- Deloitte** (2020b) To Ease the Health-Wealth Trade-off, Reallocate Digital Property Rights. G20 Insights. Available at https://www.g20-insights.org/policy_briefs/ease-health-wealth-trade-off-reallocate-digital-property-rights/. Accessed on 5th August 2021.
- Deloitte** (2020c) COVID-19: Privacy and Security in the Next Normal. Available at <https://www2.deloitte.com/global/en/pages/about-deloitte/articles/covid-19/privacy-and-security-in-the-next-normal.html>. Accessed on 5th August 2021.
- Dev J, Das S, Rashidi Y and Camp LJ** (2019) Personalized WhatsApp privacy: Demographic and cultural influences on Indian and Saudi users. Accessed on August 1, 2021 Available at <http://www.ljean.com/files/WhatsAppDesign.pdf>.
- EURACTIV** (2021) China Launches Virus Passport, 9 March 2021. Available at www.euractiv.com and <https://www.euractiv.com/section/china/news/china-launches-virus-passport/>. Accessed on 29th July 2021.
- FindLaw** (2019) Is There a Difference Between Confidentiality and Privacy? 25 October 2019. Available at <https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.html>. Accessed on 28th July 2021.

- Goldenfein J, Green B and Viljoen S** (2020) Privacy versus Health is a False Tradeoff. Berkman Klein Center, 22 April 2020. Available at <https://cyber.harvard.edu/story/2020-04/privacy-versus-health-false-trade>. Accessed on 30 July 2021.
- Hao K** (2020) *Coronavirus is Forcing a Trade-off between Privacy and Public Health*. *MIT Technology Review*. Available at <https://www.technologyreview.com/2020/03/24/950361/coronavirus-is-forcing-a-trade-off-between-privacy-and-public-health/>. Accessed on 1st August 2021.
- Kirchner L** (2015) *What's the Evidence Mass Surveillance Works? Not Much*. *ProPublica*. Available at <https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much>. Accessed on 2nd August 2021.
- Kreps BZ, Weissinger L, Himmelreich J, McMurry N, Li T, Schinerman N and Kreps S** Available at <https://www.brookings.edu/techstream/building-robust-and-ethical-vaccination-verification-systems/>.
- Kumaraguru P and Cranor L** (2005) Privacy in India: Attitudes and awareness. In Danezis G and Martin D (eds), *Privacy Enhancing Technologies: The International Workshop on Privacy-Enhancing Technologies*, Vol. 3856. Berlin: Springer, pp. 243–258.
- Makulilo AB** (2015) Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review* 31(1), 78–89.
- Maras M-H** (2009) From targeted to mass surveillance: Is the EU data retention directive a necessary measure or an unjustified threat to privacy? In Goold B and Neyland D (eds), *New Directions in Surveillance and Privacy*. Devon: Willan, pp. 74–103.
- Olsen JM** (2021) Denmark to Develop Digital Passport Showing COVID-19 Vaccination, 3 February 2021. *Los Angeles Times*. Available at <https://www.latimes.com/world-nation/story/2021-02-03/denmark-develop-digital-passport-showing-covid-vaccination>. Accessed on 3rd August 2021.
- Park J** (2021) Striking a Balance between Data Privacy and Public Health Safety: A South Korean Perspective. The National Bureau of Asian Research (NBR), 29 April 2021. Available at <https://www.nbr.org/publication/striking-a-balance-between-data-privacy-and-public-health-safety-a-south-korean-perspective/>. Accessed on 3rd August 2021.
- Paul O** (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *57 UCLA Law Review* 1701.
- Rothstein MA** (2020) Public health and privacy in the pandemic. *American Journal of Public Health* 110(9), 1374–1375.
- Scott M** (2021) Coronavirus Crisis Shows Big Tech for What It Is – A 21st Century Public Utility, 25 March 2020. *POLITICO*. Available at <https://www.politico.eu/article/coronavirus-big-tech-utility-google-facebook/>. Accessed on 4th August 2021.
- Sicari S, Rizzardi A, Grieco LA and Coen-Porisini A** (2015) Security, privacy and trust in internet of things: The road ahead. *Computer Networks* 76, 146–164.
- Stewart JM, Chapple M and Gibson D** (2012) *CISSP: Certified Information Systems Security Professional Study Guide*. Indianapolis, IN: John Wiley & Sons.
- UN News** (2020) *\$2.5 Trillion COVID-19 Rescue Package Needed for World's Emerging Economies*, 30 March 2020. Available at <https://news.un.org/en/story/2020/03/1060612>. Accessed on 4th August 2021.
- Warren SD and Brandeis LD** (1890) The right to privacy. *Harvard Law Review* 4(5), 193.
- Zwitter A and Gstrein OJ** (2020) Big data, privacy and COVID-19 – Learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action* 5(1), 4.