Advances in Social Science, Education and Humanities Research, volume 592
Proceedings of the 2nd International Conference on Law and Human Rights 2021 (ICLHR 2021)

Privacy on Personal Data Collection: Surveillance During the New Normal in Indonesia

Reggy Dio Geo Fanny[1,*] Aisyah Rizky Aulia Danti[1]

[1] *Gadjah Mada University, Yogyakarta, Indonesia*
[*]*Corresponding author. Email: reggy.dio.geo.fanny@mail.ugm.ac.id*

ABSTRACT
COVID-19's New Normal situation has been leading to a huge increase in the collection of personal data. Widely and intensively used digital technologies have been an important feature of international responses to the COVID-19 pandemic. One interesting class of such technologies is the COVID-19 Contact Tracing App (CCTA). CCTA has been used to augment traditional public health interventions, including mapping population movement, tracing contacts of infected persons, and authorizing movement. Although this surveillance program enables public health interventions to mitigate the pandemic, it also raises concerns regarding users' privacy violations. The purpose of this research is to analyze existing laws in personal data protection, especially related to CCTA in Indonesia. This research also examines both national as well as international legal frameworks about personal data protection. The type of this research is legal-normative research which has a descriptive-comparative nature. The result highlights two main points: (1) There is no legal umbrella regarding personal data protection in Indonesia; (2) The use of CCTA in Indonesia is still not effective. In a New Normal situation, cooperation between the government and the public is crucial. Thus, we conclude that revising the existing legal framework in this kind of situation is urgent in order to provide assurance and legal certainty and to earn public trust.

Keywords: *law, human rights, privacy, personal data collection, Indonesia, New Normal, COVID-19.*

1. INTRODUCTION

COVID-19 in Indonesia gets worse over time. From January until March 2021 alone, there is an addition of more than 765.000 new infection cases [1]. The increasing number of COVID-19 cases that are getting worse every day can be caused by various factors. According to Dr. Masdalina Pane as the Head of the Professional Development Division of the Indonesian Epidemiology Expert Association, one of the underlying reasons behind this phenomenon is ineffective monitoring of contact tracing [2]. Contact tracing is a process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission [3]. Meanwhile, in a modern context, what is meant by ineffective monitoring of contact tracing is manual contact tracing. Manual contact tracing involves identifying and interviewing a person who is carrying a virus to identify those with whom that person had recently been in contact, informing those contacts, and repeating the process [4]. To put it another way, the locating & monitoring functions were performed in person traditionally. These conventional procedures lead to ineffective and unoptimized contact tracing monitoring.

If we look at the other countries that have succeeded in reducing cases of the spread of COVID-19, such as Singapore, China, and South Korea, all of them have one thing in common. They rely on the effectiveness of contact tracing by replacing the traditional and conventional contact tracing mechanism with the modern concept of contact tracing through the COVID-19 Contact Tracing Application (CCTA).

At the moment, Indonesia has the PeduliLindungi app as an official CCTA. However, one thing to note is that although CCTA enables public health interventions to mitigate the pandemic faster, it also raises concerns regarding users' privacy violations. In order to anticipate this issue, there are several laws and regulations in place which contain provisions regarding personal data protection. For example, in Law No. 19 of 2016, jo. Law No. 11 of 2008 on Electronic Information and Transactions in statutory level, Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation in

implementing regulation level, etc. Unfortunately, there is an absence of a comprehensive and integrated legal framework that addresses privacy on personal data protection issues adequately. Thus, the purpose of this paper is to analyze how the government of Indonesia provides personal data protection to its citizens, particularly in the implementation of CCTA, and its relation with the CCTA's usage effectiveness as well.

2. RESEARCH METHOD

This research is normative legal research that uses secondary data related to personal data protection. The secondary data were collected through literature review and were divided into (a) primary legal materials, that consist of any laws and regulations on a national and international scale; (b) secondary legal materials, that consist of literature, articles, journals, seminars, research findings, and other related scientific sources that provide answers to the problems discussed in this research.

All of the collected data will be analyzed qualitatively. Moreover, in conducting the analysis, three research approaches were used, namely: (1) statutory approach, where the authors examined the compatibility between laws and regulations related to personal data protection; (2) conceptual approach, where the authors obtained scientific justification concerning personal data protection according to the developing concepts, and; (3) comparative approach, where the authors compared the existing regulations of personal data protection and the implementation of CCTA between Indonesia and other countries.

3. FINDINGS AND DISCUSSION

During COVID-19's New Normal situation, digital technologies are being used as a part of surveillance instruments. Moreover, privacy on personal data collection has become a concern of many. Privacy in the context of personal data involves regulating and managing the processes of personal data that enable the collecting, storing, sharing, and analyzing personal data as one form of privacy on personal data protection [5].

This research will highlight two problems that arise in the current situation. The first problem faced by people whose personal data are being collected is regarding the legal framework related to user privacy on personal data collection. The second problem is related to user privacy on personal data collected in the implementation of digital technology, in particular, CCTA. Therefore, the discussion will be grouped into two parts that cover the legal aspect of personal data protection and the implementation aspect of CCTA's impact on users' privacy on personal data collection in Indonesia.

3.1. The Legal Framework of Personal Data Protection in Indonesia

3.1.1. The Absence of Specific Law Regulating Privacy on Personal Data Protection in Indonesia

As a result of cross-border information transfers, privacy has become an important concern throughout the world. The implementation of privacy rights requires the involved parties to comply with varying international standards [6]. Although there is no definitive explanation of privacy, Solove has proposed at least 6 (six) approaches in conceptualizing privacy, namely: (1) The right to be alone; (2) Limited access to the self; (3) Secrecy; (4) Control over the personal information; (5) Personhood; and (6) Intimacy [7].

In Indonesia, the Constitution does not mention privacy rights explicitly. Even so, it is widely accepted that the foundation of rights to privacy is derived from and implied by the "right to protection of self" and the "right to security and protection from threats of fear to exercise or not to exercise his human rights" in Article 28G (1) [8]. The concept of privacy rights can be seen in the phrase "self," which is further elaborated as all personal matters, including the options of the individual to do or not to do something as well as the right to be protected while exercising those rights [8]. Furthermore, the provisions regarding privacy in the context of personal data protection are varied and spread within several laws and regulations, as follows:

1. *The Law of Republic Indonesia No. 36 of 1999 on Telecommunication*

The law does not recognize privacy on personal data, although it already contains a prohibition of information tapping that is transmitted through telecommunication networks in any form (Article 40) and the obligation of information secrecy for the telecommunication service providers (Article 42)

2. *The Law of Republic Indonesia No. 36 of 2009 on Health*

The law does not recognize personal data explicitly, but it constitutes the right for every person to the secrecy of their personal health conditions that

have been disclosed to health service providers (Article 57 paragraph 1), the concept of consent from the person concerned in researches that use humans as an object (Article 44 paragraph 3), and the obligation of the researcher to guarantee the secrecy of the objects' identity and personal data (Explanation of Article 44 paragraph 3).

3. *The Law of Republic Indonesia No. 24 of 2013 on Residential Administration*

The law recognizes the concept of personal data (Article 1), the protection of residents' personal data (Article 84), and administrative and criminal sanctions for the violators (Article 95A).

4. *The Law of Republic Indonesia No. 19 of 2016 jo. Law No. 11 of 2008 on Electronic Information and Transactions*

The law recognizes the concept of privacy rights on personal data that covers: the right to enjoy private life and freedom from all kinds of disturbances; the right to be able to communicate with others without prying eyes; and the right to supervise access to information about a person's personal life and data (Explanation of Article 26 paragraph 1). Moreover, it also contains the concept of consent from data owners for data processing in electronic media (Article 26), as well as the administrative and criminal sanctions for the violators (Article 45 until 51).

5. *The Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation*

As the implementing regulation of Law No. 19 of 2016, it contains more specific provisions, for example, the obligation of electronic system providers to delete irrelevant data (Article 15), to guarantee users' personal data protection (Article 29), as well as personal data protection principles in personal data processing starting from data acquisition and collection; processing and analyzing; storage; fixation and updates; display, announcement, transfer, dissemination, or disclosure; and/or deletion or destruction (Article 14).

6. *The Ministry of Health Regulation No. 269 of 2008 on Medical Records*

Although the regulation does not contain an explicit definition of personal data, it includes provisions about the obligation of secrecy and protection towards patients' personal information such as identity, diagnosis, medical and medication history, and examination history for health providers (Article 4).

7. *The Ministry of Communication and Informatics Regulation No. 4 of 2016 on Information Security Management Systems*

The regulation contains a definition of personal data (Article 1) and the categorization of electronic systems based on personal data characteristics that it manages. (Appendix).

8. *The Ministry of Communication and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems*

The regulation contains more provisions regarding personal data protection in electronic systems, such as the concept of privacy on personal data (Article 1); personal data protection principles in data processing (Article 2); the concept of consent from data owners (Article 9); personal data owners rights (Article 26) and obligation of data users and organizers (Article 27 and 28); dispute settlement mechanism (Article 29); and also administrative sanctions to the violators (Article 36).

9. *The Ministry of Communication and Informatics Regulation No. 36 of 2014 on Procedures for Registration of Electronic System Operators*

The regulation contains provisions regarding a technical overview of electronic systems, which includes personal data protection (Article 8 paragraph 5).

From the data above, it can be seen that there are already provisions that are important in personal data protection, such as the definition of personal data, privacy rights on personal data, personal data owners' rights, the obligation of personal data users and organizers, the necessity of personal data owners' consent for data processing, personal data protection principles, and sanctions for the violators. However, there is no specific regulation that comprehensively regulates personal data protection at the statutory level. The existing laws and regulations are still sectoral-based and contain different provisions for personal data protection. Therefore, issues regarding legal certainty may arise.

In comparison to European Union with their General Data Protection Regulation (GDPR) which is known as comprehensive privacy law, the existing laws and regulations in Indonesia still do not include

provisions that could further optimize personal data protection implementation, such as Special categories of personal data (Article 9 [9]); Data Protection Officer (Article 37 until 39 [9]); and Transfer of Personal Data (Article 44 until 50 [9]).

3.2. The Absence of "Sensitive Data" Concept in Indonesia Laws and Regulations

One of the most important factors in determining the individual's perception of privacy is the sensitivity of information [10]. Although it is difficult to identify the categories of sensitive data, Bing has proposed to assign the level of personal data sensitivity from the most to the least sensitive, as follows: (1) Inherently sensitive, intimate (e.g., medical or sexual) information; (2) Judgmental data that could lead to harm for the data subject; and (3) Biographical data that provides access to more sensitive data [11].

In its existing laws and regulations on personal data protection, Indonesia still does not adopt the concept of sensitive data [12]. However, The Law of Republic Indonesia No. 24 of 2013 on Residential Administration includes 'other data elements that are a person's disgrace' as one type of resident's personal data that must be protected. Moreover, in the Government Regulation No. 40 of 2019 on Resident's Personal Data Protection, 'other data elements' is defined as elements from certain important events that cannot be known by other people unless determined otherwise in accordance with the provisions of laws and regulations. These certain important events include (1) Children who are born without any knowledge about the origin of their parents; (2) Change of sex; (3) Children who are born from relationships outside the bond of marriage; or (4) Other important events determined by the Minister (of Home Affairs).

From the explanation above, it can be concluded that the existing laws and regulations do not emphasize or adopt the concept of 'sensitive data' and do not regulate the basis of specific protection that the data requires based on its sensitive nature. In addition, there is no further explanation on how the protection will be conducted and how it is different from the protection that will be given to other types of residents' personal data.

Meanwhile, in the European Union, GDPR has already adopted the concept of sensitive data. In the regulation, 'sensitive data' is designated under the term of 'special categories of personal data,' and also classified as personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and therefore require specific protection considering that their processing could create significant risks to the fundamental rights and freedoms itself [13]. Moreover, Article 9 of the regulation contains an exhaustive list of 'sensitive data' that includes but is not limited to: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation. These categories of data are subject to additional protections and restrictions on processing [14].

Furthermore, Article a quo also states that exception shall be made under several conditions: (1) If the data subject has given explicit consent; (2) Processing is necessary for the purposes for carrying out the obligations and exercising specific rights of the controller of the data subject; (3) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (4) Processing is carried out in the course of its legitimate activities with appropriate safeguards; (5) Processing relates to personal data which are manifestly made public by the data subject; (6) Processing is necessary for the establishment, exercise or defence of legal claims or based on courts order; (7) Processing is necessary for reasons of substantial public interest; (8) Processing is necessary for the medical purposes; (9) Processing is necessary for reasons of public interest in the area of public health; and (10) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [14].

Aside from European Union, there are also several countries in Asia that have already adopted the concept of 'sensitive data' in their legal framework and include the basis of specific protection based on its sensitive nature, such as Japan with the Act on the Protection of Personal Information [15] and the Republic of Korea with the Personal Information Protection Act [16].

3.3. The Impact of CCTA Towards User Privacy on Personal Data Collection during the New Normal Era in Indonesia

As one of the countries that have developed CCTA as a surveillance instrument in the New Normal situation, there are some deficiencies in the implementation of CCTA in Indonesia. Furthermore, this part will explain several considerations of Indonesia's CCTA and its comparisons with CCTA implementation in other countries. The following are crucial issues in Indonesia's CCTA implementation, which have become the central issue of the user privacy on personal data collection:

3.4. Method

Each CCTA has its own methods in conducting data collection and user monitoring. In general, CCTA focuses on one method of data collection because this will affect the size of the app and how much battery power will be used if it is continuously opened. In this case, users often put a big consideration in the battery usage in choosing a CCTA [17]. Therefore, it can be concluded that the more focused the method is, the easier it is for the app to be accepted and downloaded by people [18].

In Indonesia, PeduliLindungi, as an official CCTA, implements various methods for data collecting, such as Bluetooth, GPS, and QR Code [19]. It is different from CCTA implementation in other countries, which generally uses Bluetooth as a data collection method [20][21], for example, Google and Apple's Exposure Notification System [22]. Moreover, they also guarantee that the Bluetooth connection used is Bluetooth Low Energy which is more battery-saving than an ordinary Bluetooth connection, even if the users are constantly transmitting Bluetooth connection [23]. The other example is CoronApp in Colombia which initially only used GPS connection, but in the process, finally took part in adopting technology made by Google and Apple [24]. Thus, GPS usage in PeduliLindungi App also needs to be reviewed since its implementation tends to be prone to inaccuracy [25] and consumes more battery power than Bluetooth [26].

The various methods used in PeduliLindungi surely give more options to the users, but on the other hand, they require more users' data to be collected and stored by the app. This obviously will raise doubts regarding privacy for new users who want to download CCTA and confusion for users who do not have sufficient technology readiness [27]. The evidence is shown in the case of Colombia with its initial version of CoronApp, which resulted in low public acceptance of the CCTA [28]. The situation did not give the government of Colombia any other option but to replace and simplify their CCTA method [24]. Therefore, it can be seen that simplification of methods also has to be taken into consideration by PeduliLindungi, which collects users' data through various methods.

3.5. Permissions

Another issue that needs to be evaluated is regarding permissions. In Android's permission system, apps must declare the permissions that they use in a manifest file ("AndroidManifest.xml") included in the app package. From here, the users can be aware of what kind of permissions are needed to be able to use an app [30]. In other words, permission serves as an entry point for an application to be able to retrieve users' personal data. Therefore, a CCTA that uses various methods will also require more permissions.

In the context of PeduliLindungi, permissions requirements raise doubts as well [31]. Some people even questioned why the number of permissions needed by the app is higher than other CCTAs in general [32]. Moreover, compared with Germany's Corona-Warn with its QR Code method, which only requests permission to access user cameras [32], PeduliLindungi (in the latest version) requests permission to access user location, gallery access, access to cellphone files, and access to the camera [33]. This can potentially cause other problems, considering that Indonesia has not established a comprehensive legal framework for personal data protection.

3.6. Storage

The methods and permissions implemented in the data collection are also related to the storage that will be used by CCTA. Generally, the data storage and processing models of digital contact tracing are divided into centralized and decentralized models [34]. In the centralized model, anonymized data are uploaded from the user's phone to centralized servers, and then health authorities can check, notify, and manage previous contacts [34]. Meanwhile, the decentralized model stores data locally on the user's phone. This way, the user or health authorities will notify the system if the user has tested positive, then the mobile app will upload the last 14 days of locally stored data to the server [34].

The choice of storage model is crucial in preventing data leakages [35]. In comparison to

countries with comprehensive laws regarding personal data privacy, such as Singapore with their TraceTogether app, they usually keep the personal data on the user's phone and will remove the data after a certain period of time [36]. On the contrary, PeduliLindungi sends the personal data regularly to the government server and removes the personal data on the user's phone instead [33]. Technically, this storage model tends to be more prone to attacks [35]. If personal data is saved in cloud storage, it means the data belongs to the internet. Thus, the potential data leakages will be greater than the decentralized model, which stores data in the cache of the phone.

Therefore, the PeduliLindungi app should consider replacing the current centralized storage model with the decentralized one so that most data processing happens locally on users' mobile phones rather than on a centralized server. Only the notification of users who have been in contact with an infected person would need to be coordinated centrally. Even in the decentralized storage model, the necessary data could be processed in a way that would effectively preclude the central server from identifying users. The system would also not require collecting any location data [37].

The importance of analyzing how the CCTA implementation affects user privacy is to increase the CCTA's effectiveness. The government should not mandate users to use an app in any circumstances, so users must have free will to decide whether they want to install the application [35]. Digital contact tracing systems need users' cooperation (by installing the app and carrying their phones with them) for any chance of success. Consequently, the effectiveness of any contact tracing system depends on public support [37].

Based on the statement of Minister of Communication and Informatics Johnny G Plate, the registrants of national CCTA is only 3% of total internet users in Indonesia [38]. It can be seen that the usage of CCTA is not yet optimized, or in other words, its usage will not be effective in detecting personal contact. Compared to other countries such as Spain with 30% [39] and Singapore with 70% [40] registrants ratio of total internet users, Indonesia is still far behind.

The reason behind the low acceptability ratio of CCTA in the general population is because the public has concerns about the application's potential privacy implications [41]. It has to be understood that user acceptability covers user privacy and data protection aspects [37]. That is the main reason why in some countries, data privacy laws affect the public acceptance of the CCTA [42]. Therefore, to increase the acceptance ratio effectiveness of CCTA in Indonesia, it's important for the government to improve the legal framework regarding personal data protection.

4. CONCLUSION

Based on the discussion above, it can be concluded that there is no legal umbrella regarding personal data protection in Indonesia. There is an absence of a comprehensive personal data protection regulation at the statutory level. Indonesia also still does not adopt the concept of sensitive data as a form of data owners' privacy protection.

Furthermore, the implementation of the PeduliLindungi app as Indonesia's official CCTA is not effective. The main reason is the public's concern about the incomprehensive legal framework in Indonesia. Moreover, there are also issues related to the various data collection methods, multiple permissions requirements, centralized storage model, which contributes to the low users' acceptability ratio of the app.

Therefore, this research strongly encourages cooperation between the government and the public through the enactment of the Personal Data Protection Bill in order to provide assurance, legal certainty and to earn public trust. It also recommends that the government should simplify the data collection method and permissions requirements and replace the current centralized storage model with the decentralized one.

REFERENCES

[1] Satuan Tugas Penanganan COVID-19, "Indonesia's COVID-19 Cases Distribution Map", https://covid19.go.id/peta-sebaran (accessed May 17, 2021).

[2] Jiang T, Zhang Y, Zhang M, Yu T, Chen Y, Lu C, Zhang J, Li Z, Gao J, Zhou S. "A survey on contact tracing: the latest advancements and challenges" in *arXiv preprint arXiv:2011.02094*. Nov 2020 [Online] Available: https://arxiv.org/abs/2011.02094.

[3] N. Sagita. "Ahli Ungkap 3 Penyebab Kasus Corona di RI Terus Meningkat Sepekan Terakhir." https://health.detik.com/berita-detikhealth/d-5286778/ahli-ungkap-3-penyebab-kasus-corona-di-ri-terus-meningkat-sepekan-terakhir (accessed May 17, 2021).

[4] Social Science Research Council. "Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice". covid19research.ssrc.org https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/ (accessed May 18, 2021).

[5] Rosadi, S. D., "Protecting Privacy On Personal Data in Digital Economic Era: Legal Framework In Indonesia," *Brawijaya Law Journal*, March 2018. [Online]. Available: https://www.researchgate.net/profile/Sinta_Rosadi/publication/324655891_Protecting_Privacy_On_Personal_Data_In_Digital_Economic_Era_Legal_Framework_In_Indonesia/links/5c6b1202299bf1e3a5b2571a/Protecting-Privacy-On-Personal-Data-In-Digital-Economic-Era-Legal-Framework-In-Indonesia.pdf.

[6] Solove, DJ & Schwartz, P., *Information Privacy Law*, USA: Wolters Kluwer Law & Business, 2014.

[7] Solove, D. J., "Conceptualizing privacy", in *California Law Review*, George Washington Law Faculty Publications, 2020., pp. 1099-1124. [Online] https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications.

[8] Pramudito, A. P., "Kedudukan dan Perlindungan Hak Atas Privasi di Indonesia" in *Jurist-Diction*, July, 2020. [Online] Available: https://e-journal.unair.ac.id/JD/article/download/20212/11112.

[9] *The General Data Protection Regulation*, European Union, 2018.

[10] Lederer, S., Mankoff, J., Dey, A. K., & Beckmann, C., "Managing personal information disclosure in ubiquitous computing environments," Intel Research, IRB-TR-03-015, 2003. [Online]. Available: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2003/CSD-03-1257.pdf

[11] Bing, J., "Classification of Personal Information, with Respect to the Sensitivity Aspect," *Proc. 1st International Oslo Symposium on Data Banks and Societies*, Oslo, 1972, pp. 98-150.

[12] D. Rahmansyah and R. Muskitta. "Indonesia: Data Protection Laws and Regulations 2020." ICLG.com. https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia (accessed May 26, 2021).

[13] European Union GDPR. "Recital 51 Protecting Sensitive Personal Data." Gdpr-info.eu. https://gdpr-info.eu/recitals/no-51/#:~:text=Those%20personal%20data%20should%20include,existence%20of%20separate%20human%20races (accessed May 26 2021)

[14] *The General Data Protection Regulation*, European Union, 2018.

[15] T. Ishiara. "In a nutshell: data protection, privacy and cybersecurity in Japan." Lexology.com https://www.lexology.com/library/detail.aspx?g=d4ddd726-57e3-4f46-8ca3-2c7e86e03e58 (accessed May 27, 2021)

[16] *The Personal Information Protection Act*, Republic of Korea, 2014.

[17] Garousi, V., Cutting, D., and Felderer, M. "Mining user reviews of COVID contact-tracing apps: An exploratory analysis of nine European apps" in *arXiv preprint arXiv:2012.13589*, Dec 2020. [Online] Available: https://arxiv.org/abs/2012.13589

[18] L. Milsom, J. Abeler, S. Altmann, S. Toussaert, H. Zillessen, and R. Blasone. "Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy" osf.io https://osf.io/7vgq9/ (accessed on May 19, 2021)

[19] F. Setu. "Pemerintah Kembangkan Fitur Aplikasi PeduliLindungi untuk Hadapi Kenormalan Baru." Kominfo.go.id https://kominfo.go.id/content/detail/27094/siaran-pers-no-76hmkominfo062020-tentang-pemerintah-kembangkan-fitur-aplikasi-pedulilindungi-untuk-hadapi-kenormalan-baru/0/siaran_pers (accessed May 22, 2021).

[20] Simmhan,Y., Rambha, T., Khochare, A., Ramesh, S., Baranawal, A., George, J.V., Bhope, R.A., Namtirtha, A., Sundarajan, A., Bhargav, S.S., and Thakkar, N., "GoCoronaGo: Privacy Respecting Contact Tracing for COVID-19 Management" in Journal of the Indian Institute of Science, Nov 2020. [Online] Available: https://link.springer.com/article/10.1007/s41745-020-00201-5.

[21] Abrahams, N., Flockhart, F., Cramer, S., Cwalina, C., Evans, M., Gamvros, A., Himo, J., Hobson, T., Kessler, D., and Kitzer, C. "Contact tracing apps: A new world for data privacy."

Nortonrosefulbright.com. https://www.nortonrosefulbright.com/en-id/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy (accessed on May 20, 2021).

[22] Google Inc., "Apple and Google partner on COVID-19 contact tracing technology." Blog.google https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/ (accessed on May 20, 2021)

[23] C. Gartenberg. "Here's how Apple and Google will track the Coronavirus with Bluetooth." Theverge.com https://www.theverge.com/2020/4/14/21220644/apple-googles-bluetooth-low-energy-le-coronavirus-tracking-contact-tracing (accessed on May 21, 2021)

[24] Li, T., Cobb, C., Baviskar, S., Agarwal, Y., Li, B., Bauer, L., and Hong, J. I. "What Makes People Install a COVID-19 Contact-Tracing App? Understanding the Influence of App Design and Individual Difference on Contact-Tracing App Adoption Intention" in arXiv preprint arXiv:2012.12415, Dec. 2020. [Online] Available: https://arxiv.org/abs/2012.12415

[25] Li, T., Cobb, C., Baviskar, S., Agarwal, Y., Li, B., Bauer, L., and Hong, J. I. "What Makes People Install a COVID-19 Contact-Tracing App? Understanding the Influence of App Design and Individual Difference on Contact-Tracing App Adoption Intention" in arXiv preprint arXiv:2012.12415, Dec. 2020. [Online] Available: https://arxiv.org/abs/2012.12415

[26] T. Nimmagada. "GPS vs Bluetooth Technology for Contact Tracing." returnsafe.com https://returnsafe.com/gps-vs-bluetooth-technology-for-contact-tracing/ (accessed May 19, 2021)

[27] Li, T., Cobb, C., Baviskar, S., Agarwal, Y., Li, B., Bauer, L., and Hong, J. I. "What Makes People Install a COVID-19 Contact-Tracing App? Understanding the Influence of App Design and Individual Difference on Contact-Tracing App Adoption Intention" in arXiv preprint arXiv:2012.12415, Dec. 2020. [Online] Available: https://arxiv.org/abs/2012.12415

[28] J. Edwards. "Tracking coronavirus: Should you install the CoronApp?" TheBogotaPost.com https://thebogotapost.com/tracking-coronavirus-coronapp/46864/ (accessed May 22, 2021)

[29] P. Dave and S. Nellis. "Colombia's coronavirus app troubles show rocky path without tech from Apple, Google." Reuters.com shttps://www.reuters.com/article/us-health-coronavirus-colombia-apps-idUKKBN22J03W (accessed on May 21, 2021)

[30] Kouliaridis, V., Kambourakis, G., Chatgozlou, E., Geneiatakis, D., and Wang, H., "Dissecting contact tracing apps in the Android platform" in Journal Plos One, May 2021. [Online] Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0251867

[31] ELSAM. "Surat Terbuka untuk KEMKOMINFO Meminta Perlindungan Privasi Pengguna yang Kuat di Aplikasi PeduliLindungi." Elsam.or.id "https://elsam.or.id/surat-terbuka-untuk-kemkominfo-meminta-perlindungan-privasi-pengguna-yang-kuat-di-aplikasi-pedulilindungi/ (accessed on May 20, 2021)

[32] P. Lin, J. Knockel, I. Poetranto, S. Tran, J. Lau, and A. Senft. "Unmasked II: An Analysis of Indonesia and the Philippines Government Launched COVID-19 Apps." Citizenlab.ca https://citizenlab.ca/2020/12/unmasked-ii-an-analysis-of-indonesia-and-the-philippines-government-launched-covid-19-apps/ (accessed May 21, 2021)

[33] PeduliLindungi Privacy Policy. PeduliLindungi.id. https://pedulilindungi.id/kebijakan-privasi-data (accessed on May 22, 2021)

[34] Hernández-Orallo E, Calafate CT, Cano J, and Manzoni P. "Evaluating the Effectiveness of COVID-19 Bluetooth-Based Smartphone Contact Tracing Applications" in Applied Sciences, Oct. 2020. [Online] Available: https://www.mdpi.com/2076-3417/10/20/7113

[35] Sowmiya, B., Abhijith, V., Sudersan, S., Sundar, R.S.J., Thangavel, M., and Varalakshmi, P. "A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19" in SN Computer Science, March 2021. [Online] Available: https://link.springer.com/article/10.1007/s42979-021-00520-z

[36] Government of Singapore. TraceTogether Privacy Safeguards. TraceTogether.gov.sg.

https://www.tracetogether.gov.sg/common/privacystatement (accessed on May 22, 2021)

[37] Abeler, J., Backer, M., Buermeyer, U., and Zillessen, H. "COVID-19 Contact Tracing and Data Protection Can Go Together" in JMIR mHealth and uHealth, Apr. 2020. [Online] Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7173240/

[38] L. Jatmiko. "Aplikasi PeduliLindungi Sepi Pengunduh, Ini Manfaatnya" kabar24.bisnis.com https://kabar24.bisnis.com/read/20210202/15/1351163/aplikasi-pedulilindungi-sepi-pengunduh-ini-deretan-manfaatnya (accessed on May 23, 2021)

[39] E&T editorial staff. "Covid-19 contact-tracing apps need high adoption to be successful" eandt.theiet.org. "https://eandt.theiet.org/content/articles/2021/01/covid-19-contact-tracing-apps-need-high-adoption-to-be-successful-study/ (accessed May 22, 2021)

[40] Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., and Abeler, J. "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study" in JMIR mHealth and uHealth. May 2020. [Online] Available: https://mhealth.jmir.org/2020/8/e19857

[41] Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., and Abeler, J. "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study" in JMIR mHealth and uHealth. May 2020. [Online] Available: https://mhealth.jmir.org/2020/8/e19857

[42] T. Ehret. "Data privacy laws collide with contact tracing efforts; privacy is prevailing." Reuters.com https://www.reuters.com/article/bc-finreg-data-privacy-contact-tracing-idUSKCN24M1NL (accessed May 23, 2021).