BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 4 • N° 14 • OCTOBER 2018

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

# ENFORCEMENT IN INDONESIA DATA PRIVACY LAWS: THE 2018 FACEBOOK-CAMBRIDGE ANALYTICA SCANDAL AS A CASE STUDY

by Anbar Jayadi[1]

## Abstract

The Facebook-Cambridge Analytica scandal is an issue-in-progress in Indonesia. Indonesia is the third country that had its Facebook users' data allegedly 'improperly shared' with Cambridge Analytica. This raises concerns over how Facebook (Indonesia) handles the data of its Indonesian users and its transparency to the Indonesian public. Class-action lawsuits, parliamentary hearing, and warning letters have all been started. Nevertheless, to this date, the Indonesian authorities seem at loss. The problem is twofold: coherent data protection legislation is absent (as of the writing of this paper), and law enforcement mechanisms are weak. Academic literature and reports have already discussed, in general, the existing and upcoming data protection legal framework in Indonesia. Therefore, this paper is more interested in exploring, how the Indonesian law enforcement works when it comes to data privacy cases, using the Facebook-Cambridge Analytica scandal as a case study. The identified issues are the failure of protection of the secrecy of personal data and the exercise of the data subject's right to sue for compensations. This paper concludes with an evaluation of forthcoming data protection challenges for Indonesia.

**Keywords:** Cambridge Analytica, data privacy, Facebook, personal data protection in Indonesia

# Contents




The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.

# 1. Introduction

The Facebook-Cambridge Analytica scandal is an issue-in-progress in Indonesia.[2] There is an on-going class action lawsuit by civil society.[3] Also, the Indonesian Parliament conducted a hearing attended by Facebook representatives in the Asia Pacific and Indonesia.[4] Additionally, warning letters to Facebook Indonesia have been sent from the Indonesian Ministry of Communication and Informatics (MCI).[5] Nonetheless, so far, responses coming from the Indonesian government institutions are not assuring as to how the enforcement mechanisms will work on this matter, whether such enforcement will hold Facebook and Cambridge Analytica accountable under Indonesian laws and whether it will bring justice for Indonesian Facebook users.

The issue in Indonesia is twofold: coherent data protection legislation is absent (as of the writing of this paper), and law enforcement mechanisms are deemed as weak. Academic literature and reports have already discussed the existing and upcoming data protection legal framework in Indonesia.[6] Therefore, this paper will focus on exploring, using the Facebook-Cambridge Analytica scandal, how the Indonesian law enforcement works on this matter.

Graham Greenleaf points out that Indonesian data privacy regulations are fragmented.[7] There are three principal regulations. First, there is Law No. 11 of 2008 on Electronic Information and Transaction, later amended by Law No. 19 of 2016 (EIT Law). In essence, the EIT Law regulates activities about the use of electronic information and legal conducts involving the use of computers or any other form of electronic media. Second, there is Government Regulation No. 82 of 2012 on the Implementation of the Electronic Information and Transaction Law (GR 82/2012). In general, the GR 82/2012 is a further detailed regulation of the EIT Law. A third relevant regulation is Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (MCI 20/2016).

---

1 Anbar is/was a junior member in the Department of International Law, Faculty of Law, Universitas Indonesia (2015-2018). Contact: ajayadi@fastmail.com. Anbar obtained her Master degree from Vrije Universiteit Amsterdam, the Netherlands with the LPDP scholarship, a scholarship funded by Indonesia Endowment Fund for Education. Anbar would like to thank NICHE CAPDEV-TL Project at Faculty of Law, Universitas Indonesia for providing the funding for her research visit at the Brussels Privacy Hub.

2 Indonesia is the third country after the U.S. and the Philippines that its users' data is allegedly 'improperly' shared. See Mike Schroepfer, 'An Update on Our Plans to Restrict Data Access on Facebook' (Facebook Newsroom, 4 April 2018) <https://newsroom.fb.com/news/2018/04/restricting-data-access/> accessed 30 May 2018.

3 See Tempo, 'Indonesian Institutions File Class Action against Facebook' (7 May 2018) <https://en.tempo.co/read/news/2018/05/07/056918224/Indonesian-Institutions-File-Class-Action-against-Facebook> accessed 3 June 2018.

4 See Wiki DPR, 'Kebocoran Data 1 Juta Pengguna Facebook di Indonesia – RDPU Komisi I dengan Kepala Kebijakan Publik Facebook Indonesia dan Vice President of Public Policy Facebook Asia Pacific' [**Data Breach of 1 Million Facebook users in Indonesia – Commission I RDPU meet with (sic) the Head of Public Policy Facebook Indonesia and Vice President of Public Policy Facebook Asia Pacific**'], https://wikidpr.org/rangkuman/kebocoran-data-1-juta-pengguna-facebook-di-indonesia---rdpu-komisi-i-dengan-kepala-kebijakan-publik-facebook-indonesia-dan-vice-president-of-public-policy-facebook-asia-pacific accessed 3 June 2018.

5 See 'Kominfo Minta Penjelasan dan Dokumen Atas Penyalahgunaan Data' [**The Ministry Asked For Clarification and Documents on the Data Misuse**] (the Ministry Press Release, 19 April 2018) <https://www.kominfo.go.id/content/detail/12919/siaran-pers-no92hmkominfo042018-tentang-kominfo-minta-penjelasan-dan-dokumen-atas-penyalahgunaan-data/0/siaran_pers> accessed 1 June 2018.

6 Reports among others Asian Business Law Institute (ABLI) Legal Convergence Series on "Regulation of Cross-Border Transfer of Personal Data in Asia", the Universal Periodic Review Stakeholder Report on "The Right to Privacy in Indonesia" by the ELSAM and Privacy International, and Privacy International Report on "A New Dawn Privacy in Asia". Academic literature such as Graham Greenleaf, "Asian Data Privacy Laws: Trade and Human Rights Perspectives", First Edition 2014, Oxford University Press; Sinta Dewi Nursadi, 'Protecting Privacy on Personal Data In Digital Economy Era: Legal Framework in Indonesia' **Brawijaya Law Journal Volume 5 No. 1 April 2018**. Also, an article by Indonesian lawyer, Andin Aditya Rahman, 'Indonesia enacts Personal Data Regulation', **Privacy Laws & Business Issue 145 February 2017**. Furthermore, the privacy protection is regulated in various sectoral laws such as banking law, **et cetera**. I will not discuss this extensively in this working paper. See further Heppy Endah Palupy (2011), 'Privacy and Data Protection: Indonesia Legal Framework' (Master Thesis at Tilburg University) <http://arno.uvt.nl/show.cgi?fid=114884> accessed 10 May 2018.

7 Graham Greenleaf, "Asian Data Privacy Laws: Trade and Human Rights Perspectives", First Edition 2014, Oxford University Press, Chapter 13 on Vietnam and Indonesia- ASEAN's sectoral laws.

As a result of these fragmented laws, there is uncertainty that hampers the protection of personal data and the enforcement of the regulations. Furthermore, as the Indonesian privacy scholar, Sinta Dewi Rosadi, asserts, while there is an increasing concern over the protection of the right to privacy in Indonesia, the government legal enforcement on this issue is somewhat shadowed by the reputation of corruption.[8]

Reports, such as the Asian Business Law Institute (ABLI) Legal Convergence Series on "Regulation of Cross-Border Transfer of Personal Data in Asia" in 2018, in general, summarises the existing data privacy frameworks and enforcement mechanism in Indonesia.[9] For example, while MCI is "the sole authority" for the implementation of EIT Law, GR 82/2012, and MCI 20/2016, the MCI has almost no rules on international membership or cooperation. The Report indicates that MCI is not an Accredited Member or an Observer of the International Conference of Data Protection and Privacy Commissioners. Furthermore, the Report said, **"..to date, MCI has not concluded any bilateral or multilateral arrangements with the authorities of other jurisdictions to co-operate in the implementation of privacy laws."**[10]

In another report, the Universal Periodic Review Stakeholder Report (UPR Stakeholder Report), submitted by the Institute for Policy Research and Advocacy (ELSAM) and Privacy International in September 2016,[11] the authors point out that a comprehensive legal framework for data privacy in Indonesia is non-existent; equally missing is a data protection authority.[12] However, the UPR Stakeholder Report does not address the MCI and its roles.

As for the upcoming data protection law, the Indonesian government, mainly the MCI together with the Indonesian Parliament, is working on the Draft Law on Personal Data Protection (PDP Draft Law).[13] The PDP Draft Law is expected to be a law that comprehensively and in a uniform manner regulates the protection of personal data. This expectation means that once the PDP Draft Law is enacted, provisions in the EIT Law, GR 82/2012 and MCI 20/2016 will no longer be enforced insofar as those provisions are already regulated under the PDP Draft Law.

The legislation progress of PDP Draft Law is rather slow due to the fact that the Draft is not included in the priority list of legislation for 2018.[14] Noticeable provisions in the PDP Draft Law include regulation of categories of personal data (general and specific personal data), sensitive data, cross-border data transfer, data breaches, and the establishment of an independent commission on personal data protection.[15]

Notwithstanding the academic literature and reports discussing data privacy legal frameworks and enforcement in Indonesia, there little is known about how the frameworks and enforcement mechanism

8 Sinta Dewi Nursadi, 'Balancing Privacy Rights and Legal Enforcement: Indonesian practices', **International Journal Liability and Scientific Enquiry Volume 5 No. 3 / 4 2012,** p. 232-241.

9 ABLI, "Regulation of Cross-Border Transfer of Personal Data in Asia". The report is available here http://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia last accessed 30 September 2018.

10 **Id,** p. 161.

11 The report is available here: http://elsam.or.id/2017/03/stakeholder-report-upr-27th-session-indonesia-the-right-to-privacy-in-the-indonesia-2/ last accessed 30 September 2018.

12 **Id,** p. 6.

13 The latest version of the Indonesian Draft Law on Protection of Personal Data is available here: http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html (in Bahasa Indonesia) last accessed 30 September 2018. This version will be the reference of this paper when elaborating about the Draft Law on Protection of Personal Data. The reason for this is this version of the Draft is the one available and accessible by the public.

14 See Kompas, 'RUU Perlindungan Data Pribadi Dinilai Perlu Diprioritaskan' [The Draft Law Needs to be Prioritized], https://nasional.kompas.com/read/2018/09/12/17585051/ruu-perlindungan-data-pribadi-dinilai-perlu-diprioritaskan last accessed 30 September 2018. See also Graham Greenleaf, 'ASEAN's Two Speed Data Privacy Laws: Some Race Ahead', (2017) **147 Privacy Laws & Business International Report 25-28.**

15 See Lexology, 'Indonesia –Government publishes new draft data protection law', https://www.lexology.com/library/detail.aspx?g=499916e4-0b16-42e1-95e2-4a077402ecf5 last accessed 30 September 2018.

works. The main reason for this is that before the ongoing class-action lawsuit against Facebook and Cambridge Analytica, the cases related to the protection of personal data in Indonesian courts were almost non-existent. Hence, it could rarely been observed how law enforcement authorities such as the MCI, the police, and the judges handle the issue of protecting personal data. The Facebook-Cambridge Analytica will be the first case that provides the opportunity to assess how the law enforcement authorities in Indonesia work for data privacy.

This paper will study the functions of the relevant law enforcement authorities, existing sanctions, and possible compensations concerning data protection. In doing so, this paper will use the Facebook-Cambridge Analytica issue in Indonesia as an example. Hereby, this paper will be organised in the following manner: The first part is an introduction to the issue. The second part introduces Indonesia, its legal system, and the "trend" concerning the Facebook presence and its users in Indonesia. The third part shortly reviews the Facebook-Cambridge Analytica debacle in Indonesia. The fourth part is about the Indonesian data privacy legal frameworks relevant to the Facebook-Cambridge Analytica. The fifth part will describe relevant authorities and their functions in handling data privacy cases. The sixth part is analyses efforts in regard to Facebook-Cambridge Analytica and examines forthcoming challenges with such efforts. The final seventh part concludes this working paper.

# 2. Indonesia In Context

Before going deeply into the issue, this part will first describe Indonesia's legal system and the "trend" of privacy-related issues, particularly with Indonesian Facebook users. This information is relevant because it gives context to not only the legal frameworks but also the operation of law enforcement authorities in Indonesia.

## 2.1 Legal system

Indonesia has a complex legal system. It inherited from the Dutch, a civil law tradition; and nowadays also shows common law influence.[16] It also has Adat (customary) law and Islamic law intact in specific areas such as marriage and inheritance.[17] For the particular region, Aceh, Islamic law is entirely in force including for criminal matters.[18]

Regulations in Indonesia are hierarchical.[19] This subpart will only discuss, from the highest to the lowest, the Constitution, non-constitutional laws (in other names: "Law", "Bill" or "Act"), governmental regulations, and ministerial regulation. The reason is that such forms of regulation are relevant to the later discussion on primary legal frameworks on data privacy in Indonesia.[20] It is important to note that regulations in Indonesia and its hierarchy is intricate. However, it is not the primary focus of this paper to discuss this extensively.

16 See further Hikmahanto Juwana (2014), 'Courts in Indonesia: a mix of Western and local character', in **Asian Courts in Context,** Jiunn-Rong Yeh and Wen-Chen Chang (Eds.), Cambridge University Press, p. 303-339.
17 **Id.**
18 The Jakarta Post, 'Q&A" What you need to know about sharia in Aceh', http://www.thejakartapost.com/news/2018/03/04/qa-what-you-need-to-know-about-acehs-sharia-law.html last accessed 30 September 2018.
19 See Law No. 12 of 2011 on the formulation of laws and regulations.
20 There are other forms of regulations such as city and regency regulations, provincial regulations, and regulations enacted by state institutions such as the Supreme Court.

The highest law is the 1945 Constitution of Indonesia. The Constitution contains among other provisions, rules on the division of powers among the executive, legislative, and judicial branch. Moreover, there are human rights provisions in the Constitution, including a provision providing the constitutional basis for the right to privacy.[21] This provision is Article 28G para. (1) of the Constitution, it says: **"Every person shall have the right to protection of his/herself, family, honor, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to exercise or not exercise his/her basic rights."** No provision in the Constitution explicitly mentions "a right to privacy" or "a right to the protection of personal data."

Besides the constitution, there is non-constitutional laws. Some translations of Indonesian regulations call it "Law", "Bill" or "Act." In general, such law is a further stipulation of the Constitution. The Indonesian Parliament together with the relevant ministries are the pivotal actors in the law-making process in Indonesia.

For technology use, the EIT Law is the primary law.[22] As was said before, the EIT Law regulates activities linked to the use of electronic information and legal conducts involving the use of computers or any other form of electronic media. In the EIT Law, privacy rights are specified. The law says,

> **"...privacy rights shall contain the following meaning:**
> **a. A privacy right shall be the right to enjoy personal life and be free from any invasion.**
> **b. A privacy right shall be the right to communicate with other Persons without surveillance.**
> **c. A privacy right shall be the right to inspect access to information about the personal life of and data on individuals."**[23]

At the point of the writing of this paper, it remains unclear as to what is the use of this enumeration of privacy rights in the EIT Law above other than to explain what privacy rights are. It is especially uncertain, whether this explanation can be used as a legal basis before a civil court to claim compensation. Such uncertainty is a common problem with Indonesian laws where sometimes such stipulations are just bare words. To make such a law enforceable, authorities often ask for implementing regulations such as governmental or ministerial regulation.

Next in the hierarchical Indonesian legal order is the governmental regulation. Ideally, the governmental regulation provides the details of the provisions contained in the law. In the case of the EIT Law, the GR 82/2012 is the further implementing regulation. In general, the GR 82/2012 is about the management of electronic system and transactions. For example, concerning privacy rights, Article 15 para. (1) of the GR 82/2012 states that electronic system providers must protect the confidentiality, integrity, and availability of personal data within the management of such providers. Article 15 para. (3) of the GR 82/2012 further details the protection of personal data that will be regulated under the ministerial regulation.

A ministerial regulation is a regulation enacted by the ministries. As described before, the MCI is the primary authority when it comes to data privacy in Indonesia. The MCI is the one that issues ministerial regulations regulating data privacy in Indonesia. The central ministerial regulation is MCI 20/2016 on the protection of personal data in the electronic system. This Regulation furthers especially Article 15 of the

21 See N. Rianarizkiwati and Jimly Asshiddiqie (2017) on "Protection of personal information: the state's obligation to guarantee the right to privacy in Indonesia" in Harkrisnowo, H., **et.al.**. In Law and Justice in a Globalized World. Taylor & Francis Group.
22 See for example Edmon Makarim, 'Hybrid Paradigm from European and America Concerning Privacy and Personal Data Protection in Indonesia', **Indonesia Law Review Volume 3 No. 2 (2013),** p. 101-114.
23 Elucidation of Article 26 of EIT Law. See also Graham Greenleaf, **Supra note 7,** p. 385.

GR 82/2012 that emphasizes the protection of personal data. In a glance, the MCI 20/2016 specifies the protection of personal data, rights of the personal data owners, responsibilities of electronic system providers, the alternative dispute settlement mechanism, and administrative sanctions. At first, there was a welcoming attitude toward this Ministerial Regulation. After all, it is "the first comprehensive privacy law in Indonesia."[24] Nonetheless, as an Indonesian lawyer identifies, the enforcement mechanism is still lacking force, because it is still based on complaints from data subjects rather than non-compliance mechanism.[25]

To sum up, the following is the hierarchy of Indonesian regulations relevant to data privacy:

i. Constitution:
   - 1945 Constitution.
   - (Implicit) Right to privacy: Article 28G para. (1).

ii. Laws:
   - EIT Law.
   - Privacy rights: Elucidation of Article 26.

iii. Governmental regulations:
   - GR 82/2012.
   - Personal data protection: Article 15.

iv. Ministerial regulations:
   - MCI 20/2016.
   - Personal data protection: all articles.

## 2.2 The "trend" of privacy-related issues

Indonesia is "the third largest democracy" in the world with a Muslim-majority population.[26] Nevertheless, to date, the soundness of Indonesian democracy is questionable. Factors contributing to such questionability include a "further mainstream of conservative Islamic morality" and "reactionary hyper-nationalism in Indonesian political discourse and practice."[27]

Furthermore, access to the internet and social media like Facebook play a role.[28] On the one hand, one can argue that those platforms help to enhance democracy as Indonesian citizens, can express and discuss political views more widely through Facebook,. On the other hand, those platforms are also providing a mean for "Indonesia's alt-right" to further their agenda, using threats that in some instances can result in real physical attacks (due to "doxing").[29]

Having the above context in mind, three legal issues are usually predominant: freedom of speech, defamation and blasphemy. Regarding the first, freedom of speech, Indonesian Facebook users express and exchanges their views through status or tweets. In some cases, such expression constitutes hate speech. This leads to the second issue - defamation. Indonesian Facebook users often face defamation claims for their online expressions. Online expressions can also lead to the third legal issue of blasphemy.

24 Andin Aditya Rahman, 'Indonesia enacts Personal Data Regulation', **Privacy Laws & Business Issue 145 February 2017**.
25 **Id.**
26 See Robert W. Hefner (2018), 'Indonesia at the crossroads: imbroglios of religion, state, and society in an Asian Muslim nation' in Routledge Handbook of Contemporary Indonesia, Robert W. Hefner (Ed.). Routledge.
27 Vedi R. Hadiz, 'Indonesia's year of democratic setbacks: towards a new phase of deepening illiberalism?', **Bulletin of Indonesian Economic Studies 53:3,** p. 261-278, doi: 10.1080/00074918.2017.1410311.
28 **Id.**
29 Tim Lindsey, 'Is Indonesia retreating from democracy?', https://theconversation.com/is-indonesia-retreating-from-democracy-99211 last accessed 30 September 2018.

There have been instances where a person's Facebook status led to that person being charged under the blasphemy law.

The Facebook-Cambridge Analytica scandal gives another nuance to the existing "trend," above, in the sense of it adds a concern, i.e., how Facebook handles Indonesian user data and its overall transparency to the Indonesian public. It also challenges law enforcement authorities like MCI and the police, who usually handled cases locally, with a case that more or less needs cooperation with other countries authorities (at the point of writing, the Indonesian authorities rely more on the information fed by Facebook representatives rather than actively seeking new information). Part 3 below will elaborate on the Facebook-Cambridge Analytica scandal in Indonesia.

# 3. Facebook-Cambridge Analytica Debacle In Indonesia: A Short Review

Facebook established its office in Indonesia in August 2017.[30] It is a somewhat new presence in the country. The MCI welcomed such establishment, because the MCI generally hopes for Facebook to improve available services to Indonesian users.[31] Moreover, the MCI expected Facebook to contribute to tackling harmful contents in its platform including online hate speech.[32]

In April 2018, the news broke of the Facebook-Cambridge Analytica data breach and/or misuse 2018.[33] Indonesia is one of the countries where the data is allegedly 'improperly shared.' Responding to this allegation, the MCI sent warning letters to the Facebook office in Indonesia, and the Indonesian Parliament held a hearing with Facebook representatives in Indonesia and the Asia Pacific. Additionally, a class-action lawsuit was filed by civil society against Facebook and Cambridge Analytica. This part will briefly explain these efforts.

## 3.1 Class action lawsuit

In May 2018, a class-action lawsuit against Facebook and Cambridge Analytica was filed by the Institute for the Development and Empowerment of Indonesian Information Society (In Indonesian abbreviation, LPPMI) and the Indonesia ICT Institute (IDICTI).[34] The LPPMII is a non-governmental institution focusing on the issue of the telecommunications industry. It conducts research and advocacy.[35] The IDICTI is an institute concentrating on research, consultation, and stakeholders engagement in the field of Information

30 Kompas, 'Facebook Resmi Buka Kantor di Indonesia' [**Facebook Officially Opens Office in Indonesia**], https://tekno.kompas.com/read/2017/08/14/17094217/facebook-resmi-buka-kantor-di-indonesia last accessed 30 September 2018.

31 Lazuardhi Utama, 'Sejarah Panjang Facebook Buka Kantor di Indonesia' [**Long History of Facebook Opens Its Office in Indonesia**], https://www.viva.co.id/digital/digilife/946291-sejarah-panjang-facebook-buka-kantor-di-indonesia. See also Southeast Asia Freedom of Expression Network (Safenet), 'Protecting Freedom of Expression and Digital Rights: The Case Study of Indonesia' http://safenetvoice.org/2015/03/protecting-freedom-of-expression-digital-rights-the-case-study-of-indonesia/ accessed 10 April 2018.

32 **Id.**

33 See among others The Guardian, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election last accessed 30 September 2018.

34 Anbar Jayadi, 'Indonesian class action lawsuit against Facebook sets precedent'. **The Jakarta Post,** http://www.thejakartapost.com/academia/2018/08/10/indonesian-class-action-lawsuit-against-facebook-sets-precedent.html accessed 12 August 2018.

35 See http://lppmii.or.id/.

and Communication Technology (ICT).[36] The case was filed in the South Jakarta District Court, Indonesia, with the Case No. 396/Pdt.G/2018/PN JKT.SEL.[37]

The main issue of the lawsuit is the failure to give notification by the electronic service provider, i.e., Facebook, for alleged data leak or misuse to the users of the electronic services.[38] The plaintiffs sue both the Facebook California office and the Indonesian one, as well as Cambridge Analytica in England. The plaintiffs elaborate that both Facebook offices fall into the category of Electronic System Provider under Indonesian laws. However, the plaintiffs do not elaborate how Indonesian laws is applicable to Cambridge Analytica. Instead, the plaintiffs argue that the alleged data misuse by Cambridge Analytica occurred because Facebook allows for it. As such, Cambridge Analytica can be sued as well.

The first trial hearing was in 21st August 2018, but the session was suspended due to the absence of the defendants, i.e., Facebook and Cambridge Analytica. The next hearing is scheduled for 27th November 2018.[39]

## 3.2 Parliament hearing

In April 2018, the Indonesian Parliament held a hearing with the Head of Public Policy of Facebook Indonesia and the Vice President of Public Policy Facebook Asia Pacific on this matter.[40] The plan for the hearing was to have Facebook account for the alleged data leak or misuse of Indonesian users of Facebook. Facebook Indonesia explained that, it did investigate and so far, there was no relevant finding. It also assured that, because of a change of the Facebook Indonesia platform, a situation similar to the one with Cambridge Analytica is prevented from occurring again. The members of the House still urged Facebook to be held accountable. In the end, there was no sound conclusion from this hearing, i.e., what are the follow-up actions or even recommendations from the Indonesian Parliament to the relevant law enforcement officers.

## 3.3 The Ministry's warning letters and complaint mechanism

In April 2018, the MCI sent warning letters to the Indonesian Facebook office.[41] Sending warning letters was the first response from the Indonesian authorities, namely the MCI, once the Facebook-Cambridge Analytica scandal broke to the public.

Those MCI letters contained requests for explanation and data regarding the Facebook-Cambridge Analytica scandal. The MCI warned that failure to entertain the request would lead to blocking Facebook in Indonesia.[42] Facebook responded and explained to the MCI that there were no data of Indonesian users

36 See https://www.idicti.com/.
37 The case info is available here at the South Jakarta District Court website: http://sipp.pn-jakartaselatan.go.id/detil_perkara
38 **Supra note** 34.
39 **Supra note** 37.
40 **Supra note** 4.
41 See Press Release by the MCI among others No. 86/HM/KOMINFO/04/2018 and No. 89/HM/KOMINFO/04/2018.
42 See the statement from the Minister of the Ministry of Communication and Informatics (MCI), https://kominfo.go.id/content/detail/12881/menkominfo-rudiantara-saya-tidak-ragu-blokir-facebook/0/sorotan_media (in Bahasa Indonesia).

of Facebook being shared in the scandal.[43] So far, the MCI relies on this information given by Facebook as to what happened with the alleged data misuse or leak and also, Facebook is the one updating the MCI about the ongoing legal process particularly the one in the United Kingdom.[44] In this stream of information, it seems MCI is somewhat passive in a way that the MCI only does wait and hear (from Facebook).
In August 2018, the MCI opened a complaint channel for the Indonesian public on this matter.[45] This action seems like an attempt to obtain a more active role in the scandal. By the beginning of September 2018, there were no complaint being made.[46] The purpose of this complaint channel other than to inform the MCI is unclear. There is little information as to what the MCI wants to do with the complaints (if there are ever any). Not to mention, MCI relying on complaints (rather than an active investigation into the Facebook-Cambridge Analytica issue) is weak because the absence of complaints by Indonesian citizens does not mean that there is nothing wrong with how Facebook handles Indonesian user data and its transparency to the Indonesian public.

# 4. Data Privacy Legal Frameworks In Indonesia

As previously stated, there are three principal regulations for data privacy, namely EIT Law, GR 82/2012, and MCI 20/2016. Furthermore, there is an upcoming draft law namely Draft Law on Personal Data Protection (PDP Draft Law). This part will elaborate on the mentioned regulations by focusing on the following topics: (i) scope and territorial applicability of the regulation, (ii) definition of personal data, data subject, and electronic system provider (later in the PDP Draft Law, the term will be "data controller" and "data processor"), (iii) data breach notification, (iv) sanctions, and (v) compensations. The reason for this focus is that those topics relate to Facebook-Cambridge Analytica scandal in the Indonesian context and to avoid too much redundancy since there are other existing sources discussing the general Indonesian legal framework on data privacy.

## 4.1 On the scope and territorial applicability

The EIT Law, as explained before, essentially regulates activities about the use of electronic information and legal conducts involving the use of computers or any other form of electronic media. Article 2 of EIT Law governs the scope and applicability. On the scope, this Article says:

"**This Law shall apply to any person who commits legal acts as governed by this law,...**"

The EIT Law defines "person" as **"an individual, whether Indonesian citizens, foreign citizens or legal entities."** By "legal acts" it includes any acts that involved using electronic information and of computers and any other form of electronic media.

43 See the statement from the Directorate General for Informatics Applications of the MCI on Facebook's explanation about Facebook-Cambridge Analytica issue https://kominfo.go.id/content/detail/14292/tak-ada-penyalahgunaan-data-facebook-di-indonesia/0/sorotan_media (in Bahasa Indonesia).
44 See the statement from the Minister of the MCI on Facebook's explanation on the data misuse/data breach https://kominfo.go.id/content/detail/13539/facebook-surati-menkominfo-tak-ada-penyalahgunaan-data/0/sorotan_media (in Bahasa Indonesia).
45 **Supra note** 43.
46 **Id.**

For territorial applicability, Article 2 of EIT Law further states:

> **"...both within the jurisdiction of Indonesia and outside the jurisdiction of Indonesia, having legal effects within the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and detrimental to the interest of Indonesia."**

In summary, the EIT Law is applicable both in Indonesia and extra-territorially. The provision on extra-territoriality is problematic. It is doubtful as to what extent this provision is enforceable outside Indonesian territory by the Indonesian government. At the end of the day, as Purna Cita Nugraha asserts, to overcome the problematic nature of Article 2 EIT Law, Indonesian authorities must enhance its international cooperation with other governments.[47] For example, in combatting transnational crime including cyber-crimes, Indonesia has an agreement with the Australian government.[48] In the field of data protection, however, as identified in the ABLI Report, MCI as the leading authority has no agreements of that sort.

In the PDP Draft Law, scope and territorial applicability are more or less repeated in the same way. Article 4 of the Draft stipulates:

> "**This Law shall apply to any Person, Public Entities, Business Entities, and Civil Society Organizations who commits legal acts as governed by this Law,..."**

This provision is more elaborate than Article 2 of the EIT Law as it is more specific than saying "**This Law shall apply to any Person..."** Furthermore, on extra-territorial applicability, the Article 4 of the Draft states:

> **"...both within the jurisdiction of Indonesia and outside the jurisdiction of Indonesia, having legal effects within the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and detrimental to the interest of Indonesia."**

Article 4 of the Draft is the same as Article 2 EIT Law. In the PDP Draft Law, however, Article 39 regulates "International Cooperation." This provision might be a way to compensate what is absent in the EIT Law namely channels for international cooperation. Unfortunately, the wording of the Article is confusing. Article 39 para. (1) of the PDP Draft Law states that the Indonesian government must make policies at the international level. It does not elaborate as to what kind of policies, how the Indonesian government will make it, and the role of such policies compared to the existing instruments at the international level. Paragraph 2 of Article 39 of PDP Draft Law states that the Indonesian government shall take policies if there are violations of data subject rights in the cross-border data transfer. Again, to date, there is no explicit discussion of this issue.

## 4.2 On personal data, data subject, and electronic system provider

In the EIT Law, there is no definition provided for "personal data." MCI 20/2016 provides such a definition. Article 1 No. 1 of the MCI 20/2016 states that personal data is: **"...particular individual data that are stored, maintained and kept for its authenticity."** Moreover, the "particular individual data" constitutes

47 Purna Cita Nugraha, 'Penerapan Rezim Ekstraterritorial Jurisdiction dalam Hukum Siber di Indonesia' [The Implementation of Extraterritorial Jurisdiction Regime in Cyber Law in Indonesia, **Jurnal Opinio Juris Vol. 15 January-April 2014,** p. 104-126.

48 **Id,** p. 122-123.

> **"any authentic and actual information that relates to any individual and is identifiable directly or indirectly to be managed following laws and regulations."**

In the PDP Draft Law, personal data is defined as: **"any data about a person that identifiable and/or can be identified individually or combined with other information either directly or indirectly through electronic and/or non-electronic system."** This is different from Article 1 No. 1 of the MCI 20/2016.

As for the term "data subject," the MCI 20/2016 defines it as **"any individual to whom the Particular Individual Data relate."** In the PDP Draft Law, the definition is as follows: **"Data subject is any natural or legal person who is the legitimate owner of the Personal Data."** There is a change in the definition as there is no mention of "particular individual data" as in the MCI 20/2016.
In the EIT Law and MCI 20/2016, there is no mention of "data controller" or "data processor." Instead they use the term "Electronic System Provider" (ESP). Article 6a of the amended EIT Law states that:

> **"Electronic System Provider is every Person, Public Authority, Business Entities, and community that provide, process, and/or operate the Electronic System, either by themselves or together to the users of Electronic System for personal or other parties' purposes."**

The PDP Draft Law no longer uses the term Electronic System Provider, but introduces the terms "data controller" and "data processor." The Draft Law defines data controller as **"Any natural or legal persons, public authorities, business entities, and/or civil society organizations which control the processing of Personal Data."** The data processor's definition is **"Any natural or legal persons, public authorities, and/or civil society organizations which processes personal data on behalf of the controller."**

The terms used in the PDP Draft Law are similar to the terms used in the European standards of data protection.[49] The similarity is due to the influence of European standards of data protection in the making of the PDP Draft Law.[50] In the academic paper preparing the PDP Draft Law, there are quite some references to EU or European instruments and cases such as the Handbook on European Data Protection Law and the EU Data Protection Directive.[51]

## 4.3 On data breach notification

Article 16 para. (1) EIT Law regulates that an ESP must protect the secrecy of the electronic information. The GR 82/2012 furthers this with Article 15 para. (2) of GR 82/2012, saying that in the event of a failure to protect the personal data, the ESP must notify the data subject. Moreover, Article 20 para. (3) of GR 82/2012 states that in the event of the failure of or the disturbance in the system, the ESP must secure the data and immediately notify relevant authorities.

49 This paper use the phrase "European standards" as references made in the Academic Paper of the PDP Draft Law are both European Union and the Council of Europe legal instruments.

50 On the European influence, Sinta Dewi Rosadi, an Indonesian privacy scholar who is also involved in the drafting of the Academic Paper of PDP Draft Law and the PDP Draft Law itself, in her article 'Protecting Privacy on Personal Data In Digital Economy Era: Legal Framework in Indonesia' stated that "...**it is important for Indonesia to meet the EU standards regarding privacy on personal data."** (p. 155). Sinta explains this in the context of maintaining EU-Indonesia economic relations.

51 See The Academic Paper for the draft law on personal data protection. The Paper is available here https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf (in Bahasa Indonesia). Nevertheless, European data privacy standards influencing other countries legislations is not that unusual. On this, see further Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108', **International Data Privacy Law, 2012 Vol 2 No. 2,** p.68-92.

The MCI 20/2016 then specifies more in Article 28 letter b of the MCI 20/2016, stipulating that the ESP must provide written notice to the data subject. The written notice is as the following:

a. The notice must contain reasons or causes of the failure;
b. The notice can be in electronic form insofar there is a consent given to do so by the data subject at the time of obtaining and collecting the data subject's data;
c. The ESP must ensure the data subject receive the notice if such failure potentially damage the data subject;
d. The notice must be given the latest fourteen days from the day the failure is known.

The unsettling part of the above provisions is the vagueness of "authorities," so who is going to enforce this provision. The MCI as the central authority could be an option. However, this might depend on the business sector.[52] For instance, for the financial sector, there is the Financial Service Authority.[53]

In the PDP Draft Law, the explanation of Article 13 states that the data controller must protect and ensure the security of personal data under its control. Unlike the previous regulations, where there was vagueness on the authorities, the PDP Draft Law establishes an independent commission. One of the functions of this commission is to ensure compliance of the data controller. Part 5 below will discuss more on the authorities.

## 4.4 On dispute settlements

Article 38 of the EIT Law regulates that any Person can bring lawsuits against another person or ESP for damages. The Article also allows the public to file class-action lawsuits against a person or ESP for public damages. Besides courts, the EIT Law allows for arbitration or other alternative dispute settlement mechanisms.

In the MCI 20/2016, the dispute settlements provisions are mostly about the complaints-based mechanism. This mechanism means, referring to Article 31 of the MCI 20/2016, that a data subject or the ESP file complaints with the MCI for a failure of protection of confidentiality of personal data. The MCI can, through its Directorate General, form a dispute settlement panel for a personal data issue, and such a panel will hear the complaints. For "confidentiality of personal data," regulations, GR 82/2012 give a rather tautological explanation, namely that **"confidentiality refers to the legal concept of confidentiality of electronic information and communication."**

Article 44 PDP Draft Law states that there are two mechanisms of dispute settlement. The first one does not involve courts, instead the independent commission for the protection of personal data can be involved. Alternatively, mechanisms like mediations, negotiations, conciliation, or arbitration can be used to resolve the dispute as well. The second avenue is via the courts. Parties can only go to courts if there is a written objection from one of the parties involved to the independent commission's decision. What the significance of such written objection is, how the commission will hear such an objection, and how the commission's decision on the objections is enforceable in comparison to the court's ruling, is not elaborated (yet) in the PDP Draft Law available to the public.[54]

52 SSEK Indonesian Legal Consultants, 'Data Privacy by Sector in Indonesia', https://www.lexology.com/library/detail.aspx?g=8939c768-b641-4463-99fd-c0ca3952d5f7 accessed 25 September 2018.
53 **Id.**
54 The latest version of the Indonesian Draft Law on Protection of Personal Data is available here: http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html (in Bahasa Indonesia) last accessed 30 September 2018.

## 4.5 On sanctions

For a breach of security of personal data, it is not the EIT Law that regulates the sanctions but the MCI 20/2016. This is because MCI 20/2016 is the special regulation on the protection of personal data. Article 36 para. 1 of the Regulation stipulates the following:

> "**Any person obtains, collects, processes, analyses, stores, displays, publishes, transmits, and/or disseminates Personal Data in an unauthorized manner or other than per the provisions of this Ministerial Regulation or other laws and regulations shall be imposed administrative sanctions…"**

The administrative sanctions are verbal warnings, written warnings, suspensions of activities, or public announcement on a website. These sanctions are carried out by the Ministry and on a step-by-step basis. Concretely, the MCI will first give a verbal warning. If the person concerned does not pay attention to this, then the MCI will give written warnings (usually up to three times), and if the concerned person still ignores the warnings, the sanction continue until the sanction of a public announcement on a website.

In the PDP Draft Law, there are new provisions for administrative sanctions. First, the MCI is not the authority that gives administrative sanctions but the independent commission. Second, for the sanctions, as the Article 53 para. (2) of the Draft Law describes, they include (i) instructions to stop the business activities, (ii) instructions to delete the personal data, (iii) instructions to stop the data misuse, (iv) decisions to pay for damages, and (v) fines in the maximum amount of 25 billion Rupiah (around 1.5 million Euro) and the minimum amount of 1 billion Rupiah (around 50,000 Euro).

While these sanctions are more elaborate than the ones in the MCI 20/2016, the PDP Draft Law is not better in explaining as to how such sanctions are helpful in ensuring the protection of personal data to the fullest. For example, it is unclear what kind of legal force all the instructions, i.e., to stop the data misuse, to delete personal data, and to stop business activities, have. It will be the homework of the independent commission to build such a powerful profile so that those instructions have any use (if such commission is going to be established, as this is still a Draft Law and subject to change).

## 4.6 On compensations

For the data subjects, if there is a failure of protection of the personal data, EIT Law, GR 82/2012, MCI 20/2016, and PDP Draft Law include no provisions on compensations.[55] If the data subject file a civil lawsuit, the basis for compensation is the Indonesian Civil Law Code. Following is the Article 1365 of the Civil Code:

> **"Each law-violating act that brings disadvantage to another party requires the person guilty of producing such a loss, to compensate the loss."**

55 Graham Greenleaf details that, when explaining about enforcement, **"…such sanctions do not eliminate civil or criminal liability, such as the right to sue for compensation under article 26 of the 2008 Law…**" While this is correct, there are no provisions on what exactly are the compensations for the data subjects in the event of violation of privacy rights. Not to mention, while the provision Article 26 para. (2) of the EIT Law states that every one has the right to sue for compensation, the legal basis of that lawsuit will likely be the Article 1365 of the Indonesian Civil Law Code (though Greenleaf identifies about Article 1365 of the Indonesian Civil Law Code as well). It is because of the Article 26 para. (2) of the EIT Law only gives the right to sue for compensation, but such Article is not about what should be in the claim when it comes to asking for compensations (the Article 30 of the PDP Draft Law provides the similar formulation on the right to sue for compensation) and hence the reference of Article 1365 of the Indonesian Civil Law Code. See Graham Greenleaf, **Supra note 7,** p. 386.

Prominent Indonesian civil law scholar, Rosa Agustina elaborates on this Article. Agustina explains that "law-violating act" includes an act that violates the legal obligation of a person. There must be guilt or mistake, a loss, and a causal relationship between the law-violating act and the loss.[56] For data privacy cases, these elements might be quite a high threshold if data subjects want to seek compensation using this Article. The reason is twofold. First, what constitutes as the loss, in the eye of most Indonesian judges is the material and concrete loss; that it is calculable.[57] For example, a loss of a house. However, in data privacy cases, the loss is to some degree intangible namely the loss of privacy. As such, arguing the loss of privacy in the event of data breach before Indonesian judges can be non-permissible from the eyes of such judges. Secondly, the causal relationship threshold might pose issues. Since the loss is often intangible, and such intangibility might not be permissible in front of court, arguing a causal relationship can be difficult.

To briefly conclude, this part explains the EIT Law, GR 82/2012, MCI 20/2016, and the PDP Draft Law on the following topics: (i) scope and territorial applicability of the regulation, (ii) definition of personal data, data subject, and electronic system provider (later in the PDP Draft Law, the term will be "data controller" and "data processor"), (iii) data breach notification, (iv) sanctions, and (v) compensations. There are some unclarities in the provisions of the mentioned regulations that can lead to not fully upholding them. Not to mention, there are still some obstacles despite the regulations such as the (in)tangibility of the loss that can affect the determination of the compensation by the Indonesian judges.

# 5. Indonesian Law Enforcement Authorities Relevant To Data Privacy Cases

This part will explain the relevant authorities that are likely involved in the event of a failure of protection of personal data, namely the MCI and the courts. As for the Indonesian police, to date, they are more involved in cases like cyber-fraud, pornography, illegal access, and online hate speech.[58] The Indonesian Parliament is an important actor as well, but its role is limited to ensuring due course of the law enforcement process.

## 5.1 Ministry of Communication and Informatics

On its website, the MCI states, that it has a duty for **"...monitoring government affairs in the field of communication and information technology..."**[59] In the event of a failure of protection of the secrecy of personal data, the MCI has the following competences:

a. To receive complaints from the data subjects concerning such failure. The relevant Directorate-General in the MCI will follow-up on such complaints and can form a dispute settlement panel on personal data (Article 29 and Article 30 of the MCI 20/2016).
b. To ask data and information of ESP to protect personal data (Article 35 of the MCI 20/2016).
c. To give administrative sanctions for the failure of protection of secrecy of personal data.

In the PDP Draft Law, there these competences are no longer mentioned for the MCI. The independent commission will take over. More elaboration on the commission below in the subpart 5.3.

56 Rosa Agustina (2013), 'Perbuatan Melanggar Hukum' [**Law-Violating Acts**], Pascasarjana Universitas Indonesia, p. 117.
57 I am indebted to Luthfi Sahputra for discussion about this point.
58 Based on the discussion at the Indonesia-Netherlands Rule of Law and Security Update, at the session "Preventing and Combatting Cybercrime", 18 January 2018, in Jakarta, Indonesia.
59 See MCI website https://kominfo.go.id/tugas-dan-fungsi (in Bahasa Indonesia).

## 5.2 Courts

A data subject can sue for compensation under the Indonesian Civil Code. In such a case, there will be a role for the Indonesian courts. In general, the hierarchy of the courts in Indonesia is the following: the district court, the High Court, then the Supreme Court. There are other courts such as religious courts, military courts, and administrative courts as well as other specialized courts such as tax and commercial courts.[60] These later courts are less relevant to the case discussed here in this paper. As such, this paper will not give extensive attention to them.

The district court is a court for the first instance located in a city or regency. It handles civil and criminal matters. The High Court is an appeal court located in a province. It deals with appeal requests against the ruling of a district court. The Supreme Court is the highest court located in the capital city of Indonesia.[61] It is a court of cassation. It also has the power to conduct judicial review of implementing regulations such as Ministerial Regulations against Laws.

These courts handle class-action lawsuits. In Indonesia, class-action lawsuits generally are for issues relating to the environment, health and consumer protection.[62] There has not been a class-action lawsuit on data privacy before the one prompted by Facebook-Cambridge Analytica.

## 5.3 Independent commission for the protection of personal data

In the PDP Draft Law, there are provisions on the establishment of an independent commission for the protection of personal data.[63] As stated in Article 1 no. 13 and Article 41 PDP Draft Law, the commission has the function to enforce the law on the protection of personal data and settle disputes.

Referring to Article 42 para. (2) of the PDP Draft Law, the duties of the independent commission are the following:

a. To receive complaints, to facilitate dispute settlement, and to assist data subjects if there are violations of personal data protection law;
b. To monitor all stakeholders relevant to the personal data protection;
c. To take the necessary measures to ensure compliance with the standards of personal data protection;
d. To coordinate with public authorities and business entities in creating and enforcing policies to strengthen personal data protection;
e. To publish periodically about guidelines on steps to protect personal data.

60 See Hikmahanto Juwana (2014), **Supra note 16.**

61 There are two highest courts in Indonesia. One is the Supreme Court. The other is the Constitutional Court. For the latter court, it handles matters on the constitutional review of Laws in Indonesia. On privacy rights, I discuss the cases in the Constitutional Court elsewhere. see Anbar Jayadi, 'What Constitutes as Limitation of (Human) Rights in Indonesian Legal Context', **Hasanuddin Law Review Volume 3 Issue 3 December 2017,** p. 290-306, doi: http://dx.doi.org/10.20956/halrev.v3i3.1203.

62 The Supreme Court of Indonesia (2009), 'Class Action & Citizen Lawsuit Laporan Penelitian' [**Class Action & Citizen Lawsuit Research Report**].

63 See for further discussion Muhammad Iqsan Sirie, 'The Mandatory Designation of a Data Protection Office in Indonesia's Upcoming Personal Data Protection Law', **Padjajaran Journal of Law Volume 5 No. 1 2018,** p. 24-49.

The competences of the independent commission, as Article 42 para. (3) of the PDP Draft Law stipulates, are the following:

a. To give warning letters to data controllers if there are violations;
b. To provide recommendations to law enforcement officers regarding the prosecution process in the issue of personal data protection;
c. To take the necessary measures to facilitate the enforcement of personal data protection;
d. To present advice about regulations concerning personal data protection;
e. To decide whether there is a violation of personal data protection;
f. To negotiate agreements regarding personal data protection with other countries' data protection authorities.

The independent commission can act as a mediator in a dispute settlement process. It can also act as the body which adjudicates the matter through the panel formed by the commission. Moreover, the independent commission is the one that will give administrative sanctions if there is a violation of personal data protection.

To sum up, this part explains the functions and authorities of three relevant stakeholders when it comes to the enforcement of personal data protection. The stakeholders are the MCI, the courts, and the future independent commission. On the commission, since the PDP Draft Law is still a draft, all results are still subject to change depending on whether the commission is going to be established.

## 6. Will It Work? Legal Enforcement In Facebook-Cambridge Analytica Scandal In Indonesia

Will legal enforcement in Indonesia work for resolving the Facebook-Cambridge Analytica scandal? This is indeed a difficult question to answer. This part will evaluate the existing efforts and the forthcoming challenges.

As explained in part 3, there is an ongoing class-action lawsuit against Facebook-Cambridge Analytica in the South Jakarta District Court, Greater Jakarta, Indonesia. The case number is Case No. 396/Pdt.G/2018/PN JKT.SEL.

There is optimism about this case, because it is the first case before any district courts concerning two data privacy issues. The first issue is on the failure of protection of secrecy of personal data and a failure to notify data subjects about the breach (Article 16 of EIT Law, Article 15 para. (2) of GR 82/2012, and Article 28 letter b of the MCI 20/2016). The second issue concerns the data subjects' right to sue for compensation (Article 26 para (2) of the EIT Law and Article 1365 of the Civil Code). The ruling from the court will be eagerly awaited.

The lawsuit will however face at least three challenges. First, there is an issue with the extraterritorial effect of this lawsuit. Facebook has an office in Indonesia, and therefore, it can fall under the category of ESP under Indonesian laws (as the plaintiffs argued). Cambridge Analytica does not have such an office in Indonesia. Other than sending summon letters through the Ministry of Foreign Affairs (as the Court did with Facebook California office), it is not clear how the Court or the plaintiffs will pursue Cambridge Analytica's liability. Not to mention, Cambridge Analytica may have ceased to exist.

Second problem is the nature of the class-action lawsuit in Indonesia. First, there is the difficult determination of "class." In the class-action lawsuit against Facebook-Cambridge Analytica, the plaintiffs call for Indonesian Facebook users who regard themselves as a victim to come forward with proof of purchase of internet credit. Such a call might be problematic because, in the class-action lawsuit, there must be substantial similarities of facts and/or similarities in the laws concerned.[64]

For substantial similarities of laws, the relevant provisions are in the EIT Law, GR 82/2012, and MCI 20/2016. As for the substantial similarities of facts[65], the Indonesian Facebook users do not know for a fact that they are the victims of a failure of protection of secrecy of personal data. How could they know as they do not have the means to obtain such knowledge? Moreover, as described before, Facebook Indonesia claims that there is no Indonesian Facebook user data involved in the Facebook-Cambridge Analytica scandal. Second, the credibility of the representatives of the group, i.e., LPPMII and IDICTI will be under heavy scrutiny. In practice, attacking the credibility of the representatives is one of the most followed strategies. This explanation does not mean this paper wants to undermine the credibility of LPPMII and IDICTI instead it urges for caution.

Thirdly, there is a problem related to the compensation itself. The plaintiffs in the case ask for compensation for material and immaterial loss. As explained before, the intangibility character of the loss, the loss of the right to privacy, might be not be permissible for the judges.

Additionally, the complaint-based mechanism opened by the MCI from August to September 2018 is problematic. No complaint has yet been submitted by any Indonesian Facebook user, i.e., the data subjects. As previously elaborated, this absence of complaints by Indonesian citizens does not mean that there is nothing wrong with how Facebook handles Indonesian users data and its transparency to the Indonesian public. Moreover, it is a weak way of enforcement to rely on the right for data subjects to file complaints bearing in mind that data subjects are not in a position to know whether they have indeed been the victims of a failure of protection of secrecy of personal data; only Facebook holds such information.

Would the establishment of the independent commission (referring to the current version of the PDP Draft Law) make any difference? Alternatively, would the PDP Draft Law help in that matter? On the extraterritoriality problem, the PDP Draft Law is no different since it more or less repeats the provision of the EIT Law. Regarding the data subject right to sue for compensations, while the PDP Draft Law is more elaborate than existing regulations (EIT Law, GR 82/2012, and the MCI 20/2016), it is not perfect, since data subjects still have to go through virtually the same mechanism as under the existing regulations. The only difference so far is that instead of the MCI, the independent commission for personal data protection becomes the primary authority. The independent commission itself might not be the best option for ensuring compliance with the personal data protection as there are foreseeable burdens if the commission is the one that is ensuring compliance. At the very least, the commission must cooperate with the MCI. Not to mention, as Sirie suggests, a Data Protection Officer can be an option to be included in the PDP Draft Law.[66]

64 The Supreme Court of Indonesia (2009), **Supra note 62**.
65 I am indebted to Damianagatayuvens for the discussion about this issue.
66 Muhammad Iqsan Sirie, 'The Mandatory Designation of a Data Protection Office in Indonesia's Upcoming Personal Data Protection Law', **Supra note 63,** p. 45-46.

# 7. Concluding Thoughts

This paper discusses the Facebook-Cambridge Analytica scandal in Indonesia. As the third country that is allegedly affected by the issue, Indonesian law enforcement authorities seem at loss; relying primarily on Facebook (Indonesia) for information about the scandal rather than actively investigate a potential non-compliance with existing rules. Using the Facebook-Cambridge Analytica scandal as an example, this paper explores how the Indonesian law enforcement works and examines the future challenges for law enforcement when it comes to data privacy cases. The issues are a failure of protection of secrecy of personal data and the exercise of data subject's right to sue for compensations. This paper concludes that while the existing efforts (the class action lawsuit, the parliamentary hearing, and the MCI's complaint-mechanism) ignite optimism about the protection of personal data in Indonesia, challenges are still existing. These challenges are because of the limits of the existing laws, and the vagueness of the competences of the relevant Indonesian institutions. On top of that, upcoming Indonesia's data protection law, as identified throughout this paper, is still in much need of improvement.

# The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri & Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommuni-cations operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou & Paul de Hert (14 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

# The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html



**Contact:** info@brusselsprivacyhub.org

See list on previous page