

INDONESIA READINESS IN DATA PRIVACY ENFORCEMENT

Anbar Jayadi¹

Abstract

Being the third country, after the United States and the Philippines, that was affected by Facebook-Cambridge Analytica scandal, Indonesia does not have a strong national enforcement mechanism (at least not yet) to ask for Facebook's accountability in sharing the data of Indonesian citizens "improperly" to the firm Cambridge Analytica. While there is Indonesia Ministry of Information and Communication that is in charge of data privacy enforcement, it is deemed not enough due to its authorities *only* comprises of giving administrative sanctions. As such, in the current Draft Law on Personal Data Protection, Indonesia is planned to establish a national independent commission so that there is a stronger data privacy enforcement. Against this background, this paper asks the main question: to what extent Indonesia data privacy enforcement mechanisms are adequate in handling the increasing challenges of data privacy cases such as Facebook-Cambridge Analytica scandal? To answer this question, this paper will start by outlining the challenges with regard to data privacy cases. Then, this paper will give a general overview of data privacy regime in Indonesia e.g. main applicable laws such as EIT Law and the Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic System ("Ministerial Regulation on Personal Data Protection"), and the Draft Law on Personal Data Protection. Moreover, this paper will describe existing data privacy enforcement mechanisms in Indonesia that include administrative and criminal proceedings. Additionally, this paper will explain the enforcement mechanisms under the Draft Law on Personal Data Protection. Then, this paper will compare the existing enforcement mechanisms and the ones under the Draft Law in which in that comparison, this paper will analyze the differences and similarities of the mechanisms. This paper will end with the discussion on the possible advantages and disadvantages of having an independent commission focusing on personal data protection.

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

CONTENT

1. Introduction
2. Data Privacy in Indonesia: It Gets Challenging
 - 2.1. Current issues
 - 2.2. Overview of existing laws
 - 2.3. Draft law on personal data protection
3. Data Privacy Enforcement Mechanisms
 - 3.1. Relevant stakeholders
 - 3.2. Existing legal avenues: administrative sanctions and criminal proceedings
 - 3.3. The independent commission for data privacy issues in the draft law on personal data protection
 - 3.4. Evaluating data privacy enforcement mechanisms in Indonesia
4. Concluding Thoughts

¹ Anbar is a junior member in Department of International Law, Faculty of Law, Universitas Indonesia. Contact: anbarjayadi@ui.ac.id. In terms of research, her interests include data privacy, gender, and public international law. 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.

1. Introduction

Being the third country, after the United States and the Philippines, that was affected by Facebook-Cambridge Analytica scandal, Indonesia does not have a strong national enforcement mechanism (at least not yet) to ask for Facebook's accountability in sharing the data of Indonesian citizens "improperly" to the firm Cambridge Analytica.² This is due to the fact that Indonesia does not have its own national data protection authority.³

As of the writing of this paper, the current and main institution that is in charge of making sure the compliance in data privacy protection is Indonesia Ministry of Information and Communication ("the Ministry"). By making sure it means that the Ministry has the authority to deal with complaints about the failure to protect data privacy and to give administrative sanctions to the concerned party in a form of warning letters, suspension of activities and public announcement in websites for any discompliance.⁴

Nevertheless, it is unclear as to how the exercise of such authority will ensure an effective remedy and the right compensation for the party affected by the discompliance. Not to mention, if the case is in a global scale like Facebook-Cambridge Analytica scandal, it is unsettled as to how the Ministry will exercise such authority i.e. to what extent the Ministry can employ an extraterritorial reach? To this date, what Ministry can do, particularly in the context of Facebook-Cambridge Analytica scandal, is asking Facebook to provide the Ministry with necessary information and urging them to block its third-party providers.⁵

To address the issue of enforcement, Indonesia is currently developing its own national law on personal data protection (Draft Law on Personal Data Protection).⁶ One of the provisions in the Draft Law on Personal Data Protection is about the establishment of an independent national commission.⁷ The commission has two main functions namely ensuring compliance of data

² 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 DLA Piper, 'National Data Protection Authority: Indonesia' <<https://www.dlapiperdataprotection.com/index.html?c2=&c=ID&t=authority>> accessed 30 May 2018. Another contributing reason as to the weak data privacy enforcement in Indonesia is that Indonesia does not have a special legislation in data privacy protection. The privacy protection is regulated in various sectoral laws such as banking law, etc. I will not discuss about 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.

⁴ See Article 26 para. 1 and Article 36 para. 1 of the Ministry Regulation No. 20 of 2016 on Personal Data Protection in Electronic System [*Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik*]. Available at https://jdih.kominfo.go.id/produk_hukum/unduh/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016 accessed 1 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 The draft law on personal data protection in Bahasa Indonesia is available here <<http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html>> last accessed 6 June 2018.

⁷ Chapter XI of the Draft Law on Personal Data Protection. *Id.*

controllers and urging relevant stakeholders to respect the “privacy of personal data”.⁸ Especially on ensuring compliance, the commission has the authority to determine whether there is violation or not and take necessary measures to handle such violation.⁹

Nonetheless, there are questions toward the commission’s authorities among others: (i) how will the commission cooperates with other relevant institutions in Indonesia? (ii) how will the commission fit in with the other enforcement means available within Indonesia’s legal system such as administrative sanctions by the Ministry and criminal proceedings under the Law on Electronic Information and Transaction (“EIT Law”)? and (iii) does the commission has an extraterritorial reach? If so, how will the commission exercise it? Additionally, it is also worth to inquire whether the commission will become a place for Indonesian citizens, as victims of data misuse, to seek for an effective remedy in a case with a quite gravity like Facebook-Cambridge Analytica scandal.

This paper will examine the existing and upcoming data privacy enforcement mechanisms in Indonesia. In doing so, this paper asks the main question: : to what extent Indonesia data privacy enforcement mechanisms are adequate in handling the increasing challenges of data privacy cases such as Facebook-Cambridge Analytica scandal? To answer this question, this paper will start by outlining the challenges with regard to data privacy cases. Then, this paper will give a general overview of data privacy regime in Indonesia e.g. main applicable laws such as EIT Law and the Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic System (“Ministerial Regulation on Personal Data Protection”), and the Draft Law on Personal Data Protection. Moreover, this paper will describe existing data privacy enforcement mechanisms in Indonesia that include administrative and criminal proceedings. Additionally, this paper will explain the enforcement mechanisms under the Draft Law on Personal Data Protection. Then, this paper will compare the existing enforcement mechanisms and the ones under the Draft Law in which in that comparison, this paper will analyze the differences and similarities of the mechanisms. This paper will end with the discussion on the possible advantages and disadvantages of having an independent commission focusing on personal data protection.

2. Data Privacy in Indonesia: It Gets Challenging

2.1. Current issues

In the past years (2008-2014), cases pertaining privacy and internet users in Indonesia are revolved around the issue of online defamation, blasphemy, and online threats.¹⁰ Social media users such as Facebook users became the center of attention of those cases. For example the online defamation case involving Prita Mulyasari, a patient of a hospital, that felt unsatisfied with the service of the hospital that she shared such unsatisfaction through Facebook (and her mailing lists).¹¹ She was then sued by the hospital for online defamation.¹²

Other than online defamation, blasphemy, and online threats, another issue that catches national attention is about wiretapping particularly on suspects of among other corruption and drugs

⁸ Article 41 of the Draft Law on Personal Data Protection.

⁹ Article 42 of the Draft Law on Personal Data Protection.

¹⁰ 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 2017.

¹¹ CNN Indonesia, ‘Deretan Nama yang Dibui dan Lolos dari Jeratan UU ITE’ [*List of Names Who Are Convicted and Not Convicted under EIT Law*] <<http://www.cnnindonesia.com/nasional/20161128092100-12-175737/deretan-nama-yang-dibui-dan-lolos-dari-jerat-uu-ite/>> accessed 31 March 2017.

¹² *Id.*

transactions.¹³ With regard to this issue, there was an important ruling from the Constitutional Court of Indonesia about wiretapping that, in general, the Court ruled that the wiretapping must be specifically regulated in a specific Law as wiretapping impacts the right to privacy of Indonesian citizens.¹⁴

While the abovementioned privacy related issues are still dominating national discussion, the issue of the protection of personal data is now starting to catch Indonesian people attention. One of the contributing reasons for this is that, as the Government of Indonesia increasingly gathers personal data (i.e. through electronic national identity card program and cell phone number registration), Indonesian citizens have become more aware for instance with regard to the security of their data.¹⁵ Not to mention, with the Facebook-Cambridge Analytica scandal where it was estimated that the data of around 1 million people is shared “improperly”, the protection of personal data is regarded as an important matter.¹⁶ One of the evidences of this increase of awareness is the ongoing class action lawsuit filed against Facebook in South Jakarta District Court led by Indonesia ICT Institute, a Non-Governmental Organization focusing on internet issues, and the Indonesian Society for Information Empowerment Development.¹⁷

With the diversification of attention, from cases like online defamation and wiretapping to the personal data protection, there comes challenges especially for Indonesia law enforcement. For one, judges might not be familiar as to how to adjudicate a case on personal data protection. Arguments like protecting one’s privacy in the light of data misuse by companies like Facebook that has its headquarter outside Indonesia’s territory might difficult for judges to understand. Additionally, for compensation, as Indonesian courts usually measure material losses, the intangibility of data privacy might bring troubles for the judges to calculate the right compensation.¹⁸

[...]

2.2. Overview of existing laws

¹³ See Privacy International Report, ‘A New Dawn Privacy in Asia’ (December 2012) <https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf> accessed 20 May 2018. See also ELSAM and Privacy International, ‘The Right to Privacy in Indonesia’ (Stakeholder Report Universal Periodic Review 27th Session – Indonesia) <<https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=3914&file=EnglishTranslation>> accessed 9 June 2018.

¹⁴ To read further on how the Constitutional Court of Indonesia rules about cases related to right to privacy including wiretapping and online blogging, 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>.

¹⁵ See 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*, p. 143-157.

¹⁶ Desy Setyowati, ‘Empat Urgensi UU Perlindungan Data Pribadi di Indonesia’ [*Four Urgencies of Having a Law on Personal Data Protection in Indonesia*] (10 April 2018) <<https://katadata.co.id/berita/2018/04/10/4-urgensi-uu-perlindungan-data-pribadi-di-indonesia>> accessed 1 June 2018.

¹⁷ 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.

¹⁸ I am indebted to Luthfi Sahputra for the discussion about this.

As identified by Graham Greenleaf, the protection of personal data in Indonesia is spread in the sectoral laws.¹⁹ Nonetheless, there are two main existing laws that regulate about the protection of personal data namely the Law No. 11 of 2008 on Electronic Information and Transaction (“EIT Law”) –later amended by Law No. 19 of 2016, and the Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic System (“Ministerial Regulation on Personal Data Protection”) enacted by Indonesia’s Ministry of Information and Communication (“the Ministry”).

First and foremost, the EIT Law defines “privacy rights” as the following:

- a. privacy rights are the rights to enjoy personal life and free from disturbances.
- b. privacy rights are the rights to communicate with other people without surveillance.
- c. privacy rights are the rights to access the information about personal life of and data on a person.”²⁰

[...]

On the personal data itself, the EIT Law stipulates that the use of personal data must be based on the consent of the concerned person.²¹ Nevertheless, the EIT Law does not give a definition of what constitutes as personal data and what “consent” means. One must refer to the Ministerial Regulation on Personal Data Protection. Following are important terms and their definition.

Table 1²²

Personal Data	“particular individual data that are stored, maintained and kept for its authenticity” (Article 1 no. 1 of the Ministerial Regulation)
Particular Individual Data	“any authentic and actual information that relates to any individual and is identifiable directly or indirectly to be manipulated under the laws and regulations” (Article 1 no. 2 of the Ministerial Regulation)
Consent	“a written statement both manually and/or electronically provided by the Data Subject after receiving comprehensive explanation about the act of obtaining, collecting, processing, analyzing, storing, displaying, publication, transmission and disseminating as well as on the confidentiality or non-confidentiality of the Personal Data” (Article 1 no. 4 of the Ministerial Regulation)
Data Subject	“any individual to whom Particular Individual Data relate” (Article 1. No. 3 of the Ministerial Regulation)

¹⁹ 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.

²⁰ The elucidation of Article 26 of EIT Law.

²¹ Article 26 of EIT Law.

²² This is unofficial translation (with some adjustments from me) available here < <https://www.scribd.com/document/333874776/Permenkominfo-No-20-2016-on-Indonesia-Protection-of-Electronic-Personal-Data-Translated-by-Wishnu-Basuki>> accessed 9 June 2018.

[...]

2.3. Draft law on personal data protection

One of the reasons behind the drafting of the law on personal data protection in Indonesia, as stated in the academic paper prepared by Indonesia Ministry of Law and Human Rights through its office on national legal development [*Badan Pembinaan Hukum Nasional*]²³, is that “to protect the interests of Indonesian consumers and give economical benefits to Indonesia”.²⁴ This is a vague purpose indeed. Nonetheless, such purpose refers to the booming of for instance start-ups in Indonesia that massively gather data of their consumers and there is still no regulation that address this (both the start-ups and their activities).²⁵ As such, the lawmakers want to, on one hand, support the development of the start-ups, and on the other hand, protect the interests of consumers e.g. their personal data.

Furthermore, the draft is also written for the purpose of making Indonesia able “to provide personal data protection standards that are equal with other countries”.²⁶ On this, Indonesia mainly look up to European Union (EU) and its standards of personal data protection.²⁷ For instance, in the Academic Paper for the draft law on personal data protection, there are quite references to EU cases, handbook and legal documents such as the Handbook on European Data Protection Law and EU Data Protection Directive.²⁸ Taking this into account, it is not surprising that the formulation of certain terms in the draft law is similar to the ones in the EU.²⁹ This will be shown in the explanation on key points below.

Key points of this draft law on personal data protection that will change the existing regulations – EIT Law and the Ministerial Regulation on Personal Data Protection:

- a. The draft law provides a different definition of the term “Personal Data” in comparison with the definition in the current Ministerial Regulation on Personal Data Protection; the EIT Law does not provide the definition on “Personal Data”.

Table 2

The Draft Law on Personal Data Protection	The Ministerial Regulation on Personal Data Protection
Personal Data: any data about a person that identifiable and/or can be identified individually or combined with other information either direct or indirectly through electronic and/or non-electronic system.	Personal Data: particular individual data that are stored, maintained and kept for its authenticity.

²³ The Academic Paper for the draft law on personal data protection is available here <https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf> and for the Draft Law is available here <<http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html>> last accessed 9 June 2018.

²⁴ Academic Paper for the draft law on personal data protection, *Id.*, p. 6.

²⁵ *Supra* note 23.

²⁶ *Supra* note 24.

²⁷ See for example the opinion of Shinta Dewi Nursadi, a privacy law expert in Indonesia in the *Supra* note 16.

²⁸ Academic Paper for the draft law on personal data protection, *Supra* note 23, see for example footnotes in p. 19, p. 20, and p. 23.

²⁹ I will elaborate further about this elsewhere as I am currently researching on the legal transplantation and the draft law on personal data protection in Indonesia.

--	--

- b. The definition of “data subject” is slightly different between the one in the Draft Law on Personal Data Protection and the Ministerial Regulation on Personal Data Protection:

Table 3

The Draft Law on Personal Data Protection	The Ministerial Regulation on Personal Data Protection
Data subject: any natural or legal person who is the legitimate owner of the Personal Data.	Data subject: any individual to whom Particular Individual Data relate.

- c. The draft law use the terms and provides definition of “data controller” and “data processor”. These two terms are unknown in the EIT Law and the Ministerial Regulation on Personal Data Protection. The term that has closer concept with “data controller” and “data processor” used in those two existing laws is the term of “Electronic System Provider”.

Table 4

The Draft Law on Personal Data Protection	EIT Law and the Ministerial Regulation on Personal Data Protection
“Data controller” : Any natural or legal persons, public authority, business entities, and/or civil society organizations which control the processing of Personal Data.	“Electronic System Provider” : 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.
“Data processor” : Any natural or legal persons, public authority, and/or civil society organizations which processes personal data on behalf of the controller.	

[...]

3. Data Privacy Enforcement Mechanisms

3.1. Relevant stakeholders

There are at least three important stakeholders when it comes to data privacy enforcement mechanism in Indonesia. By stakeholders it means institutions that are involved in data privacy enforcement. Those institutions are the Ministry of Information and Communication, Indonesia National Police, and the courts.

[...]

3.2. Existing legal avenues: administrative sanctions and criminal proceedings

Administrative

The Ministerial Regulation on Personal Data Protection regulates about the administrative sanctions. Article 36 para. 1 of the Regulation stipulates as follow:

“Any person who obtains, collects, processes, analyzes, stores, displays, publishes, transmits, and/or disseminates Personal Data in an unauthorized manner or other than

in accordance with 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, and/or public announcement in a website.³⁰ These sanctions are carried out by the Ministry and on a step-by-step basis. Concretely, for any unauthorized activity as stipulated in the Article 36 para. 1 of the Ministerial Regulation, the Ministry will first give a verbal warning. If the person concerned does not pay attention to this, then the Ministry will give written warnings (usually up to three times), and if the warnings are still ignored by the concerned person, the sanction goes until the sanction of a public announcement in a website.

[...]

Criminal

On criminal prosecution in the context of personal data protection, it is still unclear as to whether and to what extent a breach to personal data protection can be criminalized. Nevertheless, a legal staff from the Ministry of Information and Communication argues that the EIT Law can be used as a basis to bring criminal proceedings.³¹ The legal staff explained this in the context of Facebook-Cambridge Analytica scandal that for the data breach, Facebook can face criminal proceedings. The basis for this, as the legal staff explained, is Article 30 of EIT Law.³² Article 30 para. 2 of EIT Law states that:

“Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever with the intent to obtain Electronic Information and/or Electronic Records.”

Persons who do prohibited activities prescribed in the Article 30 para. 2 of EIT Law will be facing imprisonment up to 7 years and/or a fine up to seven hundred million rupiah (around 50,230 USD).³³

[...]

3.3. The independent commission for data privacy issues in the draft law on personal data protection

As mentioned before, in the draft law on personal data protection, Indonesia plans to establish a national independent commission that will handle personal data protection hence data privacy issue. In terms of enforcement, the commission has the following authorities:

“a. Gives warnings to the data controller for violations; b. Recommends to the legal enforcement officers with regard to lawsuits pertaining personal data protection; c.

³⁰ Article 36 para. 1 the Ministerial Regulation on Personal Data Protection.

³¹ See Tempo co, ‘Kemkominfo: Facebook Bisa Dipidana dengan UU ITE’ [*Facebook can be criminalized by the EIT Law*] (7 April 2018) <<https://nasional.tempo.co/read/1077256/kemkominfo-facebook-bisa-dipidana-dengan-uu-ite>>. See also The Jakarta Post, ‘Will Facebook Indonesia face criminal charges for data breach?’ (19 April 2018) <<http://www.thejakartapost.com/news/2018/04/19/will-facebook-indonesia-face-criminal-charges-for-data-breach.html>>

³² *Id.*

³³ Article 46 para. 2 of EIT Law.

Conducts necessary measures to facilitate the data privacy enforcement; d. Provides opinions and suggestion toward the formulation and implementation of other regulations that relate to the personal data protection; and e. Decides and determines whether there is breach of personal data; and f. Negotiates agreements with data privacy authority of other countries on the cross-border enforcement and implementation of the Law on Personal Data Protection of each country.”³⁴

[...]

3.4. Evaluating data privacy enforcement mechanisms in Indonesia

[...]

4. Conclusion

[...]

³⁴ Article 42 of the Draft Law on Personal Data Protection.