Indonesia Law Review (2021) 3: 323 - 336
ISSN: 2088-8430 | e-ISSN: 2356-2129

ESTABLISHING A LEGITIMATE INDONESIAN GOVERNMENT ELECTRONIC SURVEILLANCE REGULATION: A COMPARISON WITH THE U.S. LEGAL PRACTICES

Citra Yuda Nur Fatihah*

* University of California, Berkeley, the United States

Article Info

Received : 15 September 2021 | Received in revised form : 20 October 2021 | Accepted : 11 December 2021

Corresponding author's e mail : fatihah.citra@gmail.com

Abstract

Cybersecurity and privacy have now become a matter of increasing concern for citizens, the private sector, and the Indonesian government. The government is currently struggling to combat cyberattacks and data breaches. Indonesia is, in fact, in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is still weak. The only legal basis for regulating cybersecurity, privacy, and security, in Indonesia so far is the Electronic Information and Transactions Law No. 11/2008 and its revised version Law No.19/2016. Furthermore, the government through the Indonesian Ministry of Communication and Information has just issued the implementing regulation called the Ministerial Regulation Number 5 of 2020. This Ministerial Regulation has several debatable articles and provisions, such as regarding the registration obligation, the content management and safe harbor concept, as well as the censorship issues, and the access availability to government. This article would like to address and examine whether it's lawful for Indonesian government institutions or law enforcers to request such access to electronic systems and users' personal data from the Electronic Systems Operators or internet service providers for surveillance and law enforcement purposes. The article then provides legal steps or procedures as well as legal recommendations that Indonesian government entities must follow before conducting such a legitimate electronic cyber operation. This article will also compare those Indonesia's digital surveillance practices with the United States' legal practices and lesson-learned on government surveillance.

Keywords: *cybersecurity, privacy, surveillance, cyber operation, electronic systems operators, legal practices.*

Abstrak

Keamanan siber dan privasi kini semakin menjadi perhatian utama masyarakat, sektor swasta, dan pemerintah Indonesia. Pemerintah saat ini sedang berjuang memerangi kejahatan siber dan pelanggaran data. Indonesia, pada faktanya, masih berada dalam tahap awal pengembangan strategi keamanan siber nasional. Kerangka hukum untuk keamanan siber di Indonesia masih lemah. Satu-satunya dasar hukum yang mengatur mengenai keamanan privasi dan keamanan siber di Indonesia sejauh ini hanyalah Undang-Undang Informasi dan Transaksi Elektronik No. 11/2008 yang sudah direvisi dengan Undang-Undang No.19/2016. Selanjutnya, pemerintah melalui Kementerian Komunikasi dan Informatika Indonesia baru saja mengeluarkan peraturan pelaksanaan, yaitu Peraturan Menteri Nomor 5 Tahun 2020. Peraturan Menteri ini memiliki beberapa pasal dan ketentuan yang masih diperdebatkan, seperti mengenai kewajiban pendaftaran, pengelolaan konten, konsep "safe harbor," serta masalah sensor, dan ketersediaan akses kepada pemerintah. Artikel ini ingin membahas dan menelaah apakah diperbolehkan bagi lembaga pemerintah atau penegak hukum Indonesia untuk meminta akses ke sistem elektronik dan data pribadi pengguna tersebut dari Penyelenggara Sistem Elektronik atau penyedia layanan internet untuk tujuan pengawasan dan penegakan hukum. Pasal tersebut kemudian memberikan langkah-langkah atau prosedur hukum serta rekomendasi hukum yang harus diikuti oleh entitas pemerintah Indonesia sebelum melakukan operasi siber elektronik yang sah tersebut. Artikel ini juga akan membandingkan praktik pengawasan digital di Indonesia dengan praktik hukum Amerika Serikat dan pembelajaran tentang pengawasan pemerintah.

Kata kunci: *keamanan siber, privasi, pengawasan, operasi siber, penyelenggara sistem elektronik, praktik hukum*

DOI : https://doi.org/10.15742/ilrev.v11n3.1

I. INTRODUCTION

It is clear that cybersecurity and privacy have now become a matter of increasing concern for citizens, the private sector, and the Indonesian government. The Indonesian National Cyber and Crypto Agency (Badan Siber dan Sandi Negara or BSSN), for example, reported 290.3 million cases of cyberattacks in 2019.[1] The number significantly increased compared to the 232.4 million cases during the previous year. Likewise, the Criminal Investigation Agency of the Indonesian National Police (Bareskrim) saw an increase in police reports of cybercrimes, as 4,586 police reports were filed on "Patrolisiber," a Bareskim website for reporting cybercrime, in 2019.[2] This makes Indonesia one of the world's most targeted countries for cyberattacks. Some media reports and headlines, furthermore, claim that the number of cyberattacks is now growing at an 'alarming' rate.

Not only struggling to combat those cyberattacks, but the Indonesian government has also been investigating major data breach cases, most recently a data breach that exposed the personal data of 1.3 million people registered in the country's electronic Health Alert Card (eHAC) system, a government tracing app used to tackle Covid-19.[3] These data breach cases potentially risk the user's data exploitation as they leaked names, home addresses, ID numbers, Covid-19 hospital tests, and more. This eHAC data breach case was not the first case, previously, in May of the same year, the personal data of Indonesian Healthcare and Social Security Agency (BPJS Kesehatan) users were sold in an online forum known as Raid Forums for the price of 0.15 bitcoins by a user called 'Kotz.'[4]Furthermore, last year, millions of personal data were stolen from the very famous two Indonesian biggest e-commerce, Tokopedia and Lazada. For Tokopedia, some even claimed the exposed 91 million personal data was sold on the dark web.[5] As for Lazada, at least 1.1 million data were sold illegally, which involved Redmart databased hosted by a third party.[6]

While lacking data protection regulations and any related cybersecurity provisions, Indonesia is, in fact, currently in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is still weak. For example, regarding the public-private partnership, there is no dedicated cybersecurity public-private partnership in Indonesia. Therefore, Indonesia lacks any joint public-private sector plan to address cybersecurity. Indeed, industry representative associations exist, but none are dedicated to cybersecurity in particular. And so far, there are no documented new public-private partnerships being planned in Indonesia. Furthermore, there is no clear classified security law or policy, and security practices spread across different legislation while there are no specific cybersecurity provisions in place.[7] All these situations and conditions make privacy and security in Indonesia truly at risk.

---

[1] "The Indonesian National Cyber and Crypto Agency, Annual Report 2020: Cybersecurity Monitoring" (Jakarta, 2020), 11.

[2] "The Indonesian National Cyber and Crypto Agency, Annual Report 2020: Cybersecurity Monitoring."

[3] Laila Afifa, "6 Major Data Breach Cases in Indonesia in Past 1.5 Years," *Tempo*, September 3, 2021, https://en.tempo.co/read/1501851/6-major-data-breach-cases-in-indonesia-in-past-1-5-years.

[4] Afifa, "6 Major Data Breach Cases in Indonesia in Past 1.5 Years," .

[5] Afifa, "6 Major Data Breach Cases in Indonesia in Past 1.5 Years,".

[6] Afifa, "6 Major Data Breach Cases in Indonesia in Past 1.5 Years,".

[7] "Asia-Pacific Cybersecurity Dashboard," The Software Alliance, accessed September 17, 2021, www.bsa.org/APACcybersecurity.

The only legal basis for regulating cybersecurity, privacy, and security, in Indonesia so far is the Electronic Information and Transactions Law No. 11/2008[8] and its revised version Law No.19/2016[9] (EIT Law). The EIT Law covers several offenses, such as distributing illegal content, unauthorized access to another computer system to gain information, and an illegal and unauthorized interception or wiretapping of other computer systems or electronic systems. The EIT Law provides legal protection for the content of electronic systems and electronic transactions. However, the EIT Law does not cover some critical aspects of cybersecurity, such as information and network infrastructure, and human resources with expertise in cybersecurity, as well as most importantly, it does not govern how to protect the data and privacy itself and the mechanism if there is a data breach or misuse of personal data.

From this EIT Law, furthermore, the government issued technical regulations in Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions (GR 71/2019).[10] GR 71/2019 contains updates related to the implementation of cybersecurity in electronic systems and transactions. Apart from several articles related to the offenses regulated by the EIT Law, GR 71/2019 contains stronger provisions regarding the protection of personal data and information and website authentication to avoid fake, fraudulent, or scam websites. Besides, GR 71/2019 emphasizes the need for the government to prevent any harm to public interests through the misuse of electronic information and electronic transactions and the need to develop a national cybersecurity strategy.[11]

And eventually, to apply this GR 71/2019, the government through the Indonesian Ministry of Communication and Information (the "Ministry") has just issued the implementing regulation called the Ministerial Regulation Number 5 of 2020 (MR5). This MR5 has several debatable articles and provisions, such as regarding the registration obligation, the content management and safe harbor concept, as well as the censorship issues, and the access availability to the government.

This paper will specifically address and examine the latter issue, whether it's lawful for Indonesian government institutions or law enforcers to request such access to electronic systems and users' personal data from the "electronic systems operators" (ESOs) or internet service providers for surveillance and law enforcement purposes and what legal steps or procedures as well as the legal recommendations that Indonesian government entities must follow before conducting such a legitimate electronic cyber operation. This paper will also compare the Indonesian digital surveillance practices with the United States' legal practices and lesson-learned on government surveillance.

---

[8] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

[9] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

[10] Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400.

[11] Noor Halimah Anjani, "Policy Brief: Cybersecurity Protection in Indonesia," Center for Indonesian Policy Studies, accessed July 10, 2021, https://www.cips-indonesia.org/post/policy-brief-cybersecurity-protection-in-indonesia.

II. A NEW POLEMIC REGULATION TO GOVERN DIGITAL SERVICES AND PLATFORMS

The Indonesian Ministry of Communication and Information (the "Ministry") has just issued the Ministerial Regulation Number 5 of 2020 (MR5), which came into force on November 24, 2020.[12] MR5 is established to govern all private electronic systems operators (ESOs) that are accessible in Indonesia. These are broadly defined to include social media and other content-sharing platforms, digital marketplaces, search engines, financial services, data processing services, and communications services providing messaging or video calls and games (Art. 2 (2)). The new regulation will affect many national and regional digital services and platforms, as well as multinational companies like Google, Facebook, Twitter, and TikTok.

This MR5 has seven chapters and an extensive scope covering several essential areas, most of them are still very debatable and problematic. Those highlighted concerns are including overbroad and vague definitions, registration obligation and data localization, sweeping notice and takedown orders, an excessive amount of penalty for those who fail to comply, and granting authorities data access without adequate procedural safeguards that we will be discussing later extensively in this paper.

First, it has an overbroad scope. The private ESOs in MR5 are broadly defined as 'any individual, business entity, or community' that operates an 'Electronic System' involved in the 'preparing, collecting, processing, analyzing, saving, displaying, announcing, sharing and/or distributing' of electronic information (Art. 1(4) and (6)). Individuals and companies connected to websites, social media platforms, email services, search engines, messaging services, mobile applications, and nearly any other online service or application fall within the scope of the definition. As such, the regulation encompasses the government's regulatory authorities over virtually any actor involved in any online activities.

Second, all private ESOs are required to register with and obtain a registration certificate from the Ministry before providing their services in Indonesia (Art. 2). Those that fail to register by May 24, 2021, will be blocked in Indonesia. Furthermore, the registration process even requires those private ESOs to provide the Ministry with information on the location of data management, processing, and storage and to guarantee and implement the requirement to provide access to their electronic systems and data in support of law enforcement and oversight efforts (Art. 3(4)).

Third, these private ESOs are also required to "ensure" that their platform does not contain or facilitate the distribution of "prohibited content," which would imply a general obligation to monitor content (Art. 9). Failure to do so can lead to blocking of the entire service as well (Art. 9 (6)). Just like famous Germany's 2017 "NetzDG" law and its followers in some other countries, MR5 also requires private ESOs to remove or take down content within four hours for "urgent" requests and all other prohibited content within 24 hours of being notified by the Ministry.[13] Failure to do so can lead to

[12] Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.

[13] Heidy Tworek & Paddy Leerssen, "An Analysis of Germany's NetzDG Law," A Working Paper of the Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression, 2019, https://www.ivir.n.

blocking of the service (Art. 15 (9)) or, in the case of service providers that facilitate user-generated content, substantial fines (Art. 15 (10)). Article 9 (3) furthermore defines prohibited information and content as anything that violates any provision of Indonesia's laws and regulations, or creates "community anxiety" or "disturbance in public order." Article 9 (4) grants the Ministry to define this notion of "community anxiety" and "public disorder." It also forces these private ESOs to take down anything that would "inform ways or provide access" to these prohibited documents.

Fourth, the regulation states that failure to comply with the various obligations set out in the law can, in my opinion, lead to heavy and disproportionate penalties. In particular, Art. 45 provides that private ESOs that fail to grant access to their electronic data under Art. 21 are at risk of administrative sanctions enforced by the Ministry. These may include a written warning, temporary termination, blocking of their services in Indonesia, and revocation of their operating license. Cloud computing operators who fail to grant access are only subjected to a written warning or revocation of their operating license (Art. 46).

Similarly, failure to respond to notice and takedown orders on prohibited content will first receive a written warning, either once every twenty-four hours or four hours depending on the takedown window, and after three written warnings, a fine will be issued. The fine amount is not explicitly established under the Regulation but is based on the Indonesian Non-Tax State Revenue Law. It is highly concerning, however, that the exact amount does not appear in the law and that the only guidance is provided by statements from the regulator reported in official media, as between 100 and 500 million IDR per piece of content ($6,950 – $34,740).

And finally, one of the most controversial provisions under this regulation, for the purpose of supervision and law enforcement, Indonesian ministries, institutions, and law enforcement agencies can request access to a private ESOs' electronic system and electronic data, and the private ESO must provide them access upon receipt of a request from the government authority. For this, private ESOs must choose at least one liaison officer who is domiciled in Indonesia to be in charge of handling requests for access from government authorities.

Those private ESOs must provide access to both their "systems" and their "data" for "supervision" purposes whenever requested to do so. They must also allow law enforcement authorities to access electronic data for criminal investigations into any offense carrying a penalty of at least two years in prison (Art. 32).[14] For access to electronic "systems," law enforcement must obtain a court order when investigating offenses that carry a penalty of between two and five years, but not for those with a possible sentence of more than five years. We do not understand the basis for this distinction, since court orders are even more important when the possible criminal penalties are greater (Art. 33).[15]

The majority of the public and independent NGOs claimed that those requirements that authorities have direct access to systems or massive amounts of information

[14] Electronic Data is defined to mean "data in electronic form, which is not limited to text, voice, image, map, design, photography, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the likes, alphabets, sign, number, access code, symbol, or perforation." MR5, Art. 2(3).

[15] Electronic Systems is defined to mean "a series of electronic devices and procedure having the function to prepare, collect, manage, analyze, store, display, announce, transmit, and/or distribute Electronic Information." MR5, Art. 2(4).

collected and stored by private actors are of serious concern.[16] They are particularly prone to abuse, tend to circumvent key procedural safeguards, and can exceed the limits of what can be considered necessary and proportionate.[17] Furthermore, MR5 authorizes enforcement officers to demand access to traffic data and electronic user information, including names, home addresses, email addresses, and billing information, for any investigation, without the need for a court order.

III. THE U.S. LEGAL PRACTICES ON GOVERNMENT SURVEILLANCE: A COMPARISON

In the U.S., the Fourth Amendment restricts the government's electronic surveillance. The Fourth Amendment is among the greatest constitutional limits on the government's ability to exercise power over individuals. If the government obtains evidence of a crime in a manner that violates the Fourth Amendment, as a general rule, none of the evidence gathered during that search or seizure can be admitted as evidence in the criminal trial of the individual whose rights were violated.[18] This Fourth Amendment's application is also relevant to government surveillance and other actions in cyberspace.

Furthermore, there are other U.S. legal restrictions on government surveillance, i.e., the Electronic Communications Privacy Act (ECPA) with its three components: (1) the Stored Communications Act, which restricts government and private sector access to communications and data that are stored on servers and in the cloud; (2) the Wiretap Act, which restricts governments' and the private sector's ability to monitor data while it is in transit; and (3) the pen register statute, which restricts the government's ability to obtain "noncontent" information, such as the to/from lines of emails.

There are also the Communications Assistance for Law Enforcement Act, which requires telecommunications carriers and equipment makers to assist U.S. law enforcement with lawful surveillance, and the All Writs Act, and the government's attempts to use the eighteenth-century law to compel smartphone manufacturers to help the government access encrypted information. Indeed, both constitutional and statutory restrictions on cyber-surveillance and operations are still developing, and courts often are unsure what limits on government cyber operations are appropriate. The complexities are compounded because many of the restrictions are drawn from decades-old statutes that did not contemplate cloud computing, social media, and other technologies.[19] However, this paper will only examine the comparison of the Fourth Amendment and the ECPA application for the purpose of government surveillance and law enforcement.

The Fourth Amendment application only restricts searches and seizures that are conducted by a government entity or by a government agent that is acting for the government. It is clear and definite through several Supreme Court decisions about what can be categorized as a "government entity" or factors that can determine

[16] "Indonesia: Suspend, Revise New Internet Regulation," Human Rights Watch, accessed September 21, 2021, https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation.

[17] 7 UN Human Rights Council, Report of the UN High Commissioner for Human Rights, A/HRC/39/29, para. 18.

[18] Kosseff Jeff, *Cybersecurity Law*, (United States: Wiley, 2019), 69.

[19] Kosseff Jeff, "*Cybersecurity Law".*

whether a private party can be considered a government agent. In other words, any federal, state, or local government agency or department agency or department is fully subject to the limits of the Fourth Amendment, including those agents or officers that conduct electronic surveillance for the purpose of a criminal investigation.

Furthermore, the ECPA might be the most comprehensive U.S. law relating to cyber-surveillance. It not only limits the ability of government agencies, such as law enforcement, to obtain emails, monitor networks, and obtain internet traffic logs, but it also imposes strict boundaries on the ability of service providers to provide other private parties or the government with access to customer emails and other records.

The Stored Communications Act (SCA) regulates the ability of governments to compel the release of-and service providers to disclose-stored communications such as email messages and cloud content. "As the U.S. Court of Appeals for the Ninth Circuit observed, the SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility."[20] Furthermore, the SCA covers three general categories: (1) access to stored communications;[21] (2) voluntary disclosure of stored communications by service providers;[22] and (3) law enforcement agencies' attempts to compel service providers to disclose stored communications."[23]

The first category can be seen as a supplement to the Computer Fraud and Abuse Act where criminal charges against computer hackers have been brought under both the SCA and CFAA. The second category involves the restrictions placed on a service provider's ability to disclose its users' information. In many ways, this is analogous to privacy law. The third category limits the government's ability to require service providers to provide users' information. Moreover, the SCA applies two types of services: electronic communication services (ECS) and remote computing services (RCS), since the definitions of these services are important for the SCA to impose different requirements depending on whether a service is classified as an ECS or RCS.[24]

The SCA defines both ECS and RCS clearly and distinctly, while ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[25] which are the "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce,"[26] the SCA defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system."[27]

Here, Section 2702 of the SCA restricts the ability of both ECS and RCS providers to voluntarily disclose both communications contents and consumer records. Disputes under this section commonly arise during discovery in civil cases; parties to litigation often subpoena service providers for emails, logs, and other records. It is obvious that the statute prohibits the ECS provider from knowingly divulging to

[20] *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).
[21] 18 U.S.C. § 2701 - Unlawful access to stored communications.
[22] 18 U.S.C. § 2702 - Voluntary disclosure of customer communications or records.
[23] 18 U.S.C. § 2703 - Required disclosure of customer communications or records.
[24] Kosseff, Jeff. *Cybersecurity Law.*
[25] 18 U.S.C. §§ 2510(15), 2711(1) - Crimes and Criminal Procedure.
[26] 18 U.S.C. §§ 2510(12), 2711(1) - Crimes and Criminal Procedure.
[27] 18 U.S.C. §§ 2510(12), 2711(2) - Crimes and Criminal Procedure.

either the government or private parties "the contents of a communication while in electronic storage by that service."[28] On the other hand, the RCS providers are also prohibited from knowingly divulging contents of communications that are "carried or maintained" on the service on behalf of—and received via electronic transmission from—a subscriber or customer, for the purposes of storage or computer processing, unless the customer has provided authorization for other services.[29] The statute broadly defines "contents" to include "any information concerning the substance, purport, or meaning of that communication."[30]

It is necessary to highlight that Section 2702 also contains several exceptions that allow service providers to disclose communications content under limited circumstances. In conclusion, the RCS and ECS providers still are prohibited from disclosing customer records to government entities, unless (1) subject to a valid warrant, subpoena, or order under Section 2703; (2) with the customer's consent; (3) "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;" (4) to the government, if the provider believes in "good faith" that an emergency exists; or (5) to NCMEC in connection with a child pornography investigation.

The next ECPA component is the Wiretap Act which restricts the ability of the government and private parties to intercept communications as they are in transit. However, the Wiretap Act's broad prohibitions also contain several exceptions, including for government purposes. It provides law enforcement with a limited ability to intercept a "computer trespasser's communications" with the service provider's authorization, as well as allows law enforcement to seek a court order for the interception of wire, oral, or electronic communications.[31] Under this exception, law enforcement must fulfill several requirements before obtaining an order that allows them to intercept communications, including a "full and complete statement of the facts" application for wiretap orders.

Moreover, before a court will grant a wiretap order, it must determine that probable cause exists for three different elements: (1) that the target has committed, is committing, or soon will commit a crime; (2) that the wiretap will lead to information about this crime; and (3) that the target will use the communications facilities specified in the wiretap application. In other words, although a court need not be certain that the wiretap will uncover evidence of a crime, law enforcement must make a substantial showing of probable cause to obtain a wiretap order. Furthermore, there is also a definite period for a wiretap order authorization, that it may be authorized for no longer than 30 days. If law enforcement needs an extension, then it must seek an extension of up to 30 more days.

The last ECPA component would be the Pen Register Act which imposes a general prohibition on the use of pen register and traps and trace devices, with a few key exceptions, including if the pen register or trap and trace device is related to the protection of the communications providers or their users to keep the service free of abuse or unlawful service use;[32] if the user has consented;[33] or if the government has

[28] 18 U.S.C. § 2702 - Voluntary disclosure of customer communications or records.
[29] 18 U.S.C. § 2702 (a)(2)(B) - Voluntary disclosure of customer communications or records.
[30] 18 U.S.C. §§ 2510 (8), 2711(1) - Crimes and Criminal Procedure.
[31] 18 U.S.C. § 2518 - Procedure for interception of wire, oral, or electronic communications.
[32] 18 U.S.C. § 3121 (b)(2) - General prohibition on pen register and trap and trace device use; exception.
[33] 18 U.S.C. § 3121 (b)(2) - General prohibition on pen register and trap and trace device use; exception.

obtained a court order under Section 3123 of the Pen Register Act.[34]

IV. LEGAL RECOMMENDATIONS FOR A LEGITIMATE GOVERNMENT ELECTRONIC CYBER OPERATIONS

As the previous part of this paper provides a brief explanation of how legitimate government surveillances are conducted in the U.S., as a comparison, here are some legal recommendations that can be considered to improve the application of MR5 in regulating the private ESOs in Indonesia, particularly when it deals with supervision (surveillance) and law enforcement.

First of all, Indonesia needs to establish and strengthen any joint public-private sector plan to address cybersecurity and privacy. As explained previously, there is no dedicated cybersecurity public-private partnership in Indonesia, whereas we all definitely agree that cyberspace is so unique in that it involves both public and private infrastructure, and therefore the government recognizes that it has a role in securing the internet. It's important to realize that the government's role in private sector cybersecurity is not merely that of a regulator, it may also operate several programs that are designed to help companies battle the ever-evolving field of cybersecurity and privacy threats. Moreover, the government can act as a central repository of cybersecurity and privacy information. Therefore, both the Indonesian government and private ESOs have significant roles and must collaborate to secure the internet and computer systems and fight cybercrimes.

Second, there is no such Fourth Amendment restriction in Indonesia that can restrict the actions of the government. In contrast, MR5 seems to have a very wide discretion for the government entity and agency that can get involved in conducting the surveillance and law enforcement and has not yet so far defined who can legally conduct the surveillance or which division of the ministries or entities. There are hundreds of ministries and entities in Indonesia, which majority of them do not even have any responsibilities for the purpose of law enforcement and taking appropriate measures in conducting electronic surveillance.

Third, MR5 also broadly defines private ESOs as 'any individual, business entity, or community' that operates an 'Electronic System' involved in the 'preparing, collecting, processing, analysing, saving, displaying, announcing, sharing and/or distributing' of electronic information. This very broad definition may increase the chance of the government's regulatory powers to virtually any actor engaged in any online activity. Therefore, the government must narrow the terms or description of what can be defined both as "Ministries" and "Private ESOs" for the sake of legal certainty.

Fourth, as explained above, the three sections of U.S. ECPA provide very different safeguards and constraints regarding the ability of the government, as well as the private sectors, to access an electronic communication, whether it is classified as "in transit" or "in storage," since it is crucial in determining how much privacy is afforded to that particular communication at any given moment. In contrast, MR5 does not define any classification of electronic communication or electronic data that can be accessed by the government, whether is in transit or storage. MR5 only gives a broad definition of the meaning of electronic data and electronic systems. Therefore, it's necessary for the Indonesian government to clearly distinguish each classification of electronic communication or electronic data that can be disclosed to the government,

[34] 18 U.S.C. § 3121 (a) - General prohibition on pen register and trap and trace device use; exception.

whether electronic data is classified as in transit or storage. It is because the distinction between each classification of such electronic data is vital. As we will see, the designation may play an important role in determining the privacy protections that the regulation affords to a service's users.

Fifth, most importantly, as described previously, almost all these surveillance statutes require the government to obtain a valid warrant, subpoena, or court order with a strict and high standard application. MR5, in fact, regulates the requirements for the government to obtain a court order, however, it does not explain clearly the prerequisites in applying such a warrant or court order, including the obligation to provide prior notice to the customers or subscribers; the legal conditions for the warrant requirement exception (i.e., exigent circumstances); or even the obligation for the government to prove whether there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

MR5 only states in its provision that for access to electronic "systems," law enforcement must obtain a court order when investigating offenses that carry a penalty of between two and five years, but not for those with a possible sentence of more than five years. It is even getting more doubtful to understand the basis for this distinction since court orders are even more important when the possible criminal penalties are greater. Therefore, it's important for the MR5 to include specific and legitimate requirements that are obliged for the government to fulfill before the court can grant its order, such as it must determine that probable cause exists for three different elements: (1) that the target has committed, is committing, or soon will commit a crime; (2) that the electronic data or transaction will lead to information about this crime; and (3) that the target will use the communications facilities specified in the ESO's applications or internet services.

Sixth, it's necessary to underline the importance of customers' or subscribers' presence in this issue. Under the U.S. SCA, for example, the RCS providers are prohibited from knowingly divulging contents of communications that are "carried or maintained" on the service on behalf of—and received via electronic transmission from—a subscriber or customer, for the purposes of storage or computer processing, *unless the customer has provided authorization* for other services.[35] In other words, the internet service providers are required to inform the subscribers or the customers before they can disclose their personal data to the government. It's also stated that for SCA purposes, in order to obtain communications via a subpoena or order, the government *must provide prior notice to the subscriber or customer*.[36] In contrast, the MR5 does not regulate the obligation to get any lawful consent from the customers or users before the private ESOs can give access or disclose any electronic data to the government. Therefore, it's crucial for the government to consider this requirement to be implemented, as the right to be informed is one of the fundamental rights of people in cyberspace that has to be respected.

And last but not least, there is a strict and definite period of validity. As for ECPA's section 2703's restrictions for the disclosure of communications content

[35] 18 U.S.C. § 2702(a)(2)(B) - Voluntary disclosure of customer communications or records (prohibiting the disclosure of communications contents that are on RCS "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.").

[36] 18 U.S.C. § 2705(1)(A) - Voluntary disclosure of customer communications or records.

depend on whether the provider is an ECS or RCS provider, and the length of time the communications content has been stored, the Wiretap Act also has a specific period of authorization. On the other hand, MR5 even does not specifically mention this period, for how long the government may conduct such surveillance or given the access to disclose the user's electronic data and transactions. Therefore, to improve the legal certainty and legitimacy of electronic surveillance, this MR5 must add a definite period for the government entities and agencies when they are involved in cyber operations.

There is also one interesting policy under this U.S. electronic surveillance regulation that the federal law will provide legal immunity to the online service providers for their fulfillment of one specific duty, in this case, the child pornography violation. So, if the online service providers (e.g., email services or internet service providers) obtain actual knowledge that a customer appears to have violated federal child pornography laws, they are required by federal law to file a report with National Center for Missing and Exploited Children (NCMEC).[37] NCMEC then reviews the report, as well as the apparent child pornography content, and if it determines that the content is in fact child pornography, it provides information to local, state, or federal law enforcement agencies. As the providers are provided with this legal immunity, they cannot be sued for filing an NCMEC report if a customer appears to violate the Child Pornography Laws on their services.[38] So, it would be a new positive attitude for the private ESOs in Indonesia if they can also be provided with such legal immunity once they find any serious criminal offenses, such as the pornography, terrorism, or narcotics abuse so that they will voluntarily file a report with assigned government entities.

V. CONCLUSION

The Indonesian government has a new legal framework for conducting electronic surveillance for the purpose of law enforcement. Indeed, it's part of the government's main tasks and responsibilities to regulate and secure the internet in this digital age together with the private ESOs. However, it is also crucial to maintain the essential rules that the digital rights of the civil society must always be respected no matter how the government's intention is actually to protect networks and users. Therefore, in order to establish a more legitimate government electronic surveillance activities, there are some legal recommendations that the Indonesian government may consider to improve the application of MR5 in regulating the private ESOs, particularly when it deals with supervision (surveillance) and law enforcement.

[37] 18 U.S.C. § 2258A - Reporting requirements of providers.
[38] 18 U.S.C. § 2258B - Limited liability for providers or domain name registrars.

BIBLIOGRAPHY

Legal Documents

Indonesia. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

_____. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

_____. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400.

_____. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.

Books

Djafar, W., Sumigar, F., & all. *Perlindungan Data Pribadi di Indonesia: Ulasan Pelembagaan Dari Perspektif Hak Asasi Manusia*. Jakarta: ELSAM Press, 2016.

Kosseff Jeff. *Cybersecurity Law*. United States: Wiley, 2019.

The Ministry of Defense of the Republic of Indonesia. *A Road Map to Cyber Defense National Strategy*. Jakarta: The Ministry of Defense of the Republic of Indonesia, 2013.

The Indonesian National Cyber and Crypto Agency. *Annual Report 2020: Cybersecurity Monitoring*. Jakarta: BSSN, 2020.

The Indonesian National Cyber and Crypto Agency. *Indonesia National Cyber Security Strategy*. Jakarta: BSSN, 2020.

The International Telecommunication Union. *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity*. Geneva: ITU Publications, 2021.

W. Owens Et Al., Eds. *Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. National Research Council, 2009.

Wight M. *System of States*. Leicester: Leicester University Press, 1979.

Articles

A. Fathan Taufik. "Indonesia's Cyber Diplomacy Strategy as A Deterrence Means yo Face the Threat in the Indo-Pacific Region." *Journal of Physics: Conference Series*. The International Conference on Defence Technology (Autumn Edition, 2020): 5. https://doi:10.1088/1742-6596/1721/1/012048

A. Nugroho. "Personal Data Protection in Indonesia: Legal Perspective." *International Journal of Multicultural and Multireligious Understanding* 7, No. 7 (2020): 183-189.

Martha Finnemore & Duncan B. Hollis. "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," *European Journal of International Law* (2020).

Muhamad Rizal and Yanyan M. Yani. "Cybersecurity Policy and Its Implementation in Indonesia." *Journal of ASEAN Studies* 4, No. 1 (2016).

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. "An Overview of the Development Indonesia National Cyber Security." *International Journal of Technology & Computer Science* (IJTCS) 6, (December 2012): 111.

Websites

Ashley Deeks. *Defend Forward and Cyber Countermeasures 2,* Hoover Inst. Working Group on Nat'l Sec., Tech., and L., *Aegis Series Paper* No. 2004, 2020. https://www.hoover.org/research/defend-forward-and -cyber-countermeasures (noting that "many states view the [Draft Articles] as reflecting customary international law").

Budi Rahardjo. "7 The State of Cybersecurity in Indonesia." In *Digital Indonesia.* Singapore: ISEAS Publishing, 2017. https://doi.org/10.1355/9789814786003-007.

Cabinet Secretariat of The Republic of Indonesia. "Indonesia's Foreign Policy Priorities in 5 Years Ahead," Accessed November 9, 2021. https://setkab.go.id/en/indonesias-foreign-policy-priorities-in-5-years-ahead/

Center for Indonesian Policy Studies. "Protecting People: Promoting Digital Consumer Rights." Accessed September 27, 2021. https://www.cips-indonesia.org/digital-consumer-rights-pp27.

Gliddheo Algifariyano Riyadi. "Policy Brief No. 7: Data Privacy in the Indonesian Personal Data Protection Legislation." *Center for Indonesian Policy Studies,* March 2021.

Heidy Tworek & Paddy Leerssen. "An Analysis of Germany's NetzDG law." *Transatlantic Working Group*, A working paper of the Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression (April 15, 2019). https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019. pdf.

Human Rights Watch. "Indonesia: Suspend, Revise New Internet Regulation." Accessed September 21, 2021. https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation.

Kementerian Komunikasi dan Informasi Republik Indonesia. "DPR telah Adakan Rapat Dengar Pendapat Umum terkait RUU PDP." Accessed September 27, 2021. https://aptika. kominfo.go.id/2020/07/dpr-telah-adakan-rapat-denger-pendapat-umum-terkait-ruu-pdp.

Laila Afifa. "6 Major Data Breach Cases in Indonesia in Past 1.5 Years." *Tempo*. September 3, 2021. https://en.tempo.co/read/1501851/6-major-data-breach-cases-in-indonesia-in-past-1-5-years.

NCSI Project Team e-Governance Academy. "National Cyber Security Index 2020." Accessed October 1, 20201. https://ncsi.ega.ee/country/id/

Nikkei Asian Review. "ASEAN Remains Prime Target for Cyberattacks." Accessed 8 February 2018. https://asia.nikkei.com/Business/Business-trends/ASEAN-remains-prime-target-for-cyberattacks.

Paul C. Ney Jr. General Counsel, Dep't of Def. DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (March 2, 2020). https://www.defense.gov/Newsroom/Speeches /Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

The ASEAN Post. "Southeast Asia Cybersecurity Emerging Concern." Accessed 20 May 2018. https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern

The Indonesian National Cyber and Crypto Agency. "Cyberattack Data (January – April

2020).” Accessed October 1, 2021. https://bssn.go.id/rekap- serangan-siber-januari-april-2020.

The Software Alliance. “Asia-Pacific Cybersecurity Dashboard.” Accessed September 17, 2021, www.bsa.org/APACcybersecurity.

The World Bank. “Ensuring a More Inclusive Future for Indonesia through Digital Technologies.” Accessed October 5, 2021. https://www.worldbank.org/en/news/press-release/2021/07/28/ensuring-a-more-inclusive-future-for-indonesia-through-digital-technologies.

UN Human Rights Council, Report of the UN High Commissioner for Human Rights, A/HRC/39/29, para. 18.

US Cyber Command. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command (2018). https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM %20Vision%20April%202018.pdf?ver=201806-14-152556-010.

US Cyber Command. The Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace: Hearing Before the H. Comm. on Armed Servs., Subcomm. on Intelligence and Emerging Threats and Capabilities, 116th Cong. 44 (2020).

US Department of Defense. Summary: Department of Defense Cyber Strategy (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY _FINAL.PDF

Others

Ido Kilovaty. *Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare, Cyber Warfare and The Jus Ad Bellum Challenges* (2014).

Noor Halimah Anjani. “Policy Brief No. 9: Cybersecurity Protection in Indonesia.” *Center for Indonesian Policy Studies,* March 2021.