Submission of International Justice Clinic at the University of California, Irvine School of Law; Open Net Association, Inc.; International Human Rights Clinic, Korea University School of Law; Southeast Asia Freedom of Expression Network to the HUMAN RIGHTS COMMITTEE for 140th session, 4 – 28 March 2024, in relation to Indonesia

Please contact Kyung Sin Park, kyungsinpark@korea.ac.kr

I. Reporting Organizations

A. The International Justice Clinic at the University of California, Irvine School of Law ("IJC") promotes international human rights law at the national, regional, international, and corporate levels, in the United States and globally. IJC is directed by Professor David Kaye, the former United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, who has written extensively on the enjoyment and protection of human rights in digital environments. IJC has extensive experience especially addressing threats to human rights in the digital realm, working alongside civil society organizations and other stakeholders from across the globe.

B. Open Net Association, Inc., is a non-profit organization based in South Korea that promotes free expression, privacy, network neutrality, and other digital rights in the country, Asia, and globally. It has participated in and worked with the UN Human Rights Committee and the special mandates on free speech of international human rights bodies on the issues of various countries, especially in Asia.

C. International Human Rights Clinic, Korea University School of Law promotes international human rights by reporting on the human rights conditions of various countries and filing lawsuits at relevant fora.

D. Southeast Asia Freedom of Expression Network ("SAFEnet") is a regional digital rights organization based in Denpasar, Indonesia. SAFEnet was founded with a vision of realization of a digital space that upholds human rights values for all people and mission to defend digital rights in the Southeast Asia region, including their rights to access the internet, rights to express freely, and rights to feel safe in digital spaces. SAFEnet has been actively advocating for victims of the digital right violations, especially critical groups who use the Internet as a tool for expression and opinion.

II. Issues Summary

A. In this submission, the aforementioned organizations have reviewed the Human Rights Committee's ("Committee") List of issues prior to submission of the second periodic report of Indonesia and Indonesia's responding report.[1] This submission will focus specifically on digital rights, including freedom of expression and internet access, and the Government of Indonesia's ("GoI") corresponding violations under the International Covenant on Civil and Political Rights ("ICCPR").

B. This submission begins with a discussion of the GoI's failure to protect the right of freedom of expression through the persecution of speakers for defamation, "fake news," dissidence under the pretext of "hate speech," religious discourse, LGBTQ+ individuals, and social media and internet users. It then discusses violations of freedom of expression through the suppression of speech. This includes actions that result in suppression on social media and the internet, including LGBTQ+ content, and a lack of anonymity for SIM card users. It follows with a discussion of the Government's failure to protect online safety in instances of gender-based violence, digital attacks, and the spread of disinformation, including that which targets Rohingya refugees in Aceh. It then moves to a discussion of the Government's impairment of access to the internet through restrictions on content and state-led connectivity disruptions, including the 2019 internet shutdowns in Papua and West Papua. The following section discusses state surveillance and violations of the right to privacy, including the absence of communications surveillance legislation, a lack of specificity, foreseeability, legal certainty, legitimate aim, and necessity regarding existing laws, and the GoI's access to personal data held by private companies. Finally, the submission concludes with an overview of recommendations.

[1] CCPR/C/IDN/QPR/2, 2 Sept. 2020.

III. Background

A. In 2019, the Committee released the Concluding observations on the initial report of Indonesia.[2] At that time, the Committee expressed concerns over:
   1. Onerous requirements for registration and compliance with the State's official philosophy of *Pancasila*, and restrictions on related expression of opposition.[3]
   2. Law No. 1 of 1965 on defamation of religion, the 2005 edicts by the Indonesian Ulema Council and the 2008 Joint Decree by the Minister for Religious Affairs.[4]
   3. The persecution of religious minorities.[5]
   4. The defamation provisions of the Criminal Code and Law No. 11 of 2008 on information and electronic transactions to stifle legitimate criticism of state officials.[6]
   5. Undue restrictions of the freedom of assembly and expression by protestors in West Papua.[7]

B. Current U.N. Human Rights Committee's List of Issues Prior to Reporting ("LOIPR") and the State Party's Response Summarized

1. **Free expression:** The Committee inquired in Paragraph 19 of LOIPR on (a) "prohibition of certain research topics in higher education institutions," such as Papua, the mass killings in 1965, and LGBTQ+ issues; (b) "restriction of access by foreign journalists to Papua and West Papua"; and (c) "the criminalization of defamation and the arbitrary application of the provisions in the law on electronic information and transactions ("EIT law") and the Criminal Code, used to curtail the freedom of expression" and the number of related prosecutions. GoI responded in paras. 216-223 of the State report that (1) people are free to discuss all the mentioned issues; (2) journalists' access restriction to Papua and West Papua were temporary; and (3) GoI is focusing on the victims of fake news and the EIT law is being amended.

2. **Internet access in Papua:** The Committee inquired in Paragraph 20 of LOIPR on the partial Internet shutdown in the Provinces of Papua and

[2] CCPR/C/IDN/CO/1, 21 Aug. 2013.
[3] *Id.* at para. 24.
[4] *Id.* at para. 25.
[5] *Id.* at para. 25.
[6] *Id.* at para. 27.
[7] *Id.* at para. 28.

West Papua in August and September 2019. The Government responded in paras. 226-228 in the State report that the Administrative Court's subsequent decision striking down the shutdown shows the "checks and balances" in the country.

IV. Violations to the International Covenant on Civil and Political Rights

A. **Persecution of Speakers:** The GoI failed to protect the right to freedom of expression by criminalizing defamation and the arbitrary application of the provisions in the EIT law and the Criminal Code, including those on treason, dissemination of fake information, and incitement of enmity under Article 19 of the ICCPR.

1. **Persecution for defamation**: Under General Comment 34 of the ICCPR, the criminalization of defamation is not preferred and incarceration should never be a remedy.[8] The GoI arbitrarily persecutes people on the basis of defamation. The criminal code holds that "anyone who verbally accuses another publicly with the intention of defaming them may be jailed for up to nine months or fined IDR 10 million. If the defamation was published for greater public exposure, then the maximum sentence is raised to one-and-a-half years."[9] Further, the 2008 EIT Law has "been used repeatedly to prosecute Indonesians for online expression,"[10] And the 2016 EIT Law expanded the scope of defamation to include statements made unintentionally such as by tagging someone in a social media post or through private messages. The price for committing online defamation is quite high at a maximum of six years in prison and a fine of 750 million rupiah, significantly harsher than the charges for offline defamation.[11] One example of this occurred "in March 2023, [where] the Kepanjen District Court in East Java sentenced Dian Patria Arum Sari to four months in prison and eight months of probation under the EIT Law. She was charged with spreading defamatory and insulting information after she used a 2019 Facebook post to accuse an acquaintance, with whom she had previously

[8] CCPR/C/GC/34 , 12 Sept. 2011.
[9] Coconuts Jakarta, *RKUHP Explainer: All the controversial articles in Indonesia's criminal code overhaul*, Coconuts Jakarta, 19 Sep. 2019, https://coconuts.co/bali/features/rkuhp-explainer-all-the-controversial-articles-in-indonesias-criminal-code-overhaul-2/.
[10] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at C2.
[11] Id.; Human Rights Watch, *Turning Critics into Criminals,* Human Rights Watch, 3 May 2010, https://www.hrw.org/report/2010/05/03/turning-critics-criminals/human-rights-consequences-criminal-defamation-law#_ftnref191.

done business, of committing fraud."[12] Similarly, "in November 2021, Muhammad Asrul, a journalist…was found guilty of violating Article 27 of the EIT Law, which punishes defamation, and was sentenced to three months in prison…he had written three news articles about corruption allegations involving the son of Palopo's mayor."[13] Although there are some protections for the media, they are enforced inconsistently by local law enforcement. While the government claims to reduce abuse by developing enforcement guidelines, civil society organizations ("CSO"s) hold that simply "creating guidelines to respond to the revision of a problematic law should not become a habit."[14]

2. **Persecution for "fake news"**: The Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda holds that the criminalization of false statements and "fake news" are unduly restrictive and that they should be abolished.[15] Further, the declaration states that "the human right to impart information and ideas is not limited to "correct" statements."[16] General prohibitions on "fake news" are not compatible with the international standards regarding restrictions on the freedom of expression.[17] The GoI criminalizes the dissemination of information they claim to be "fake news." Examples of the use of these penalties include activists who posted a podcast regarding illegal military operations in Papua and were charged with spreading false news under the 1946 False News Law which has a ten year maximum sentence.[18] Other examples include a YouTuber accused of spreading false information criticizing Islam after he converted to Christianity and was sentenced to

[12] *Id.* at C3.
[13] *Id.* at C3; Kuswandi, *3 Month Sentence Against Journalist Asrul Injures Press Freedom*, JawaPos.com, 25 Nov. 2021, https://www.jawapos.com/nasional/01356265/vonis-3-bulan-terhadap-jurnalis-asrul-ciderai-kemerdekaan-pers; SafeNet Voice, Journalist Safety Committee Condemns the Criminalization of Journalists under the ITE Law, SafeNet, 18 Feb. 2020, https://safenet.or.id/id/2020/02/rilis-pers-komite-keselamatan-jurnalis-kecam-pemidanaan-jurnalis-dengan-uu-ite/.
[14] KontraS, *Guidelines for Implementing the ITE Law Do Not Resolve the Root of the Problem, Revision the ITE Law Immediately*, KontraS, 24 Jun. 2021, https://kontras.org/2021/06/24/pedoman-implementasi-uu-ite-tidak-menyelesaikan-akar-masalah-segera-revisi-uu-ite/.
[15] United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, *Joint declaration on freedom of expression and "fake news", disinformation and propaganda*, Organization for Security and Co-operation in Europe, 3 Mar. 2017, https://www.osce.org/fom/302796.
[16] *Id*. at 1.
[17] *Id*. at 3.
[18] Human Rights Watch, *Indonesia: Activists on Trial for Criminal Defamation*, Human Rights Watch, 14 Apr. 2023, https://www.hrw.org/news/2023/04/14/indonesia-activists-trial-criminal-defamation.

ten years in prison.[19] Further, in September of 2022 "the [court] sentenced Edy Mulyadi to seven months and 15 days [in prison]. The defendant was found guilty of spreading false information"[20] through a YouTube video she posted criticizing the Indonesian government's decision to relocate the capital.[21] Further, "the General Election Supervisory Agency, or BAWASLU (*Badan Pengawas Pemilu*), announced that it was committed to monitoring and countering buzzers" prior to the 2024 elections in order to monitor falsehoods and fake news.[22] The EIT Law also "does not define 'misleading content' or 'falsehoods' leaving it open to authorities' interpretation. The EIT Law has been used to jail journalists and editors for critical reportage of the authorities."[23] Further, the 2022 Criminal Code criminalizes the dissemination of fake news resulting in riots with a sentence of up to six years.[24] The GoI seeks to repress speech and publication because the law also holds that "making 'uncertain,' 'exaggerated,' or 'incomplete' news that those who share such information reasonably know or suspect may cause unrest.. can [lead to imprisonment of] up to two years. Again, the vague definitions used in the Criminal Code may open the door to its abuse by law-enforcement agencies."[25]

---

[19] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at C3.

[20] Aerie Dwi Satrio, *Kalimantan Case Where Jin Abandoned Child, Edy Mulyadi Sentenced to 7.5 Months in Prison*, Sind News, 12 Sep. 2022, https://nasional.sindonews.com/read/882771/13/kasus-kalimantan-tempat-jin-buang-anak-edy-mulyadi-divonis-75-bulan-penjara-1662955740.

[21] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at C3.

[22] Yatun Sastramidjaja, Pradipa P. Rasidi, and Gita N. Elsitra, *Peddling Secrecy in a Climate of Distrust: Buzzers, Rumours and Implications for Indonesia's 2024 Elections*, ISEAS, 2022.

[23] Andrea Carson & Andrew Gibbons, *The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore*, 24 Journalism Studies 14, 3 May 2023, https://www.tandfonline.com/doi/full/10.1080/1461670X.2023.2192299.

[24] Andreas Ufen, *The Rise of Digital Repression in Indonesia under Joko Widodo*, GIGA Focus Asia, No. 1, Hamburg: German Institute for Global and Area Studies (GIGA), 2024, https://doi.org/10.57671/gfas-24012.
Article 263 of the Criminal Code amended 2023: (1) Every person who broadcasts or disseminates news or notification even though he knows that the news or notification is a lie which results in unrest in society, is punishable by a maximum imprisonment of 6 (six) years or a maximum fine of category V.
(2) Any person who broadcasts or disseminates news or notifications even though it is reasonable to suspect that the news or notification is a lie which could cause riots in society, shall be punished with a maximum imprisonment of 4 (four) years or a maximum fine of category IV.
Article 264: Any person who broadcasts news that is uncertain, exaggerated or incomplete while he knows or reasonably suspects that such news may cause riots in society, shall be punished by imprisonment for a maximum of 2 (two) years or a fine of a maximum category III.

[25] *Id*.

These "fake news" laws have a clear "chilling effect on journalism,"[26] as well as on society as a whole.

3. **Persecution of dissident voices under the pretexts of "incitement of enmity," "hate speech," and "treason"**: As held in the Special Rapporteur's report on online hate speech, "[m]any Governments use 'hate speech', similar to the way in which they use 'fake news', to attack political enemies, non-believers, dissenters and critics."[27] Further, the report holds that "States should generally deploy tools at their disposal other than criminalization and prohibition, such as education, counter-speech and the promotion of pluralism, to address all kinds of hate speech."[28] The GoI arbitrarily applies the Criminal Code in order to suppress "online discourse that is critical of the government by labeling it as hate speech"[29] and treason, limiting the willingness of journalists and other internet users to critique and "challenge political leaders online."[30] The 2008 EIT Law has been used to persecute Indonesians for supposed "hate speech" at disproportionate levels based on already established criminal codes, facing them with criminal and civil penalties for legitimate activity.[31] "Throughout 2022, there were at least 97 cases of criminalization against expression in the digital realm, with a reported number of 107 people. This number has tripled compared to last [year's] 30 cases with 38 victims of criminalization. This drastic increase also places 2022 as the year with the highest number of convictions in the last 9 years."[32] Between 2008 and 2018, the EIT Law was used 263 times primarily against civil society, journalists, and media.[33] "Human rights groups and media professionals have argued that such laws curtail public debate, threaten freedom of expression, and give the government 'unchecked power' over public discourse."[34] The following cases exemplify the extreme criminalization of this online activity.

---

[26] Andrea Carson & Andrew Gibbons, *The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore*, 24 Journalism Studies 14, 3 May 2023, https://www.tandfonline.com/doi/full/10.1080/1461670X.2023.2192299.
[27] A/74/486, 9 Oct. 2019, at para. 1.
[28] *Id*. at para. 28.
[29] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B4.
[30] *Id.* at B3.
[31] *Id.* at C3.
[32] SafeNet Voice, *The Digital Rights Situation in Indonesia Had Worsened*, SafeNet, 2022.
[33] Andrea Carson & Andrew Gibbons, *The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore*, 24 Journalism Studies 14, 3 May 2023, https://www.tandfonline.com/doi/full/10.1080/1461670X.2023.2192299.
[34] *Id*.

a) "In April 2023, the Solo City District Court…sentenced Sugi Nur Rahardja to six years in prison for disseminating hate speech and blasphemy. He was charged under the EIT Law and the Criminal Code over a podcast he posted on YouTube in which he claimed that Jokowi's diploma was forged."[35]
b) "In December 2022, former youth and sports minister Roy Suryo [was sentenced] to nine months in prison because he posted a meme mocking the president. He was charged under the EIT Law, and the prosecution announced that it would appeal the decision to seek a longer sentence."[36]
c) "Other laws [criticizing the state also] infringe on user rights. The 2011 State Intelligence Law prescribes penalties of up to 10 years' imprisonment and large fines for revealing or disseminating 'state secrets.' This legal framework provides authorities with a range of powers to penalize internet users."[37]
d) The GoI further persecutes critics of the government by implementing harsh sentences for those they claim insult high officials. These include a maximum five year prison sentence and fines up to 200 million rupiah under the Criminal Code for "insulting" the president or vice president, and a maximum three year prison sentence and fines of up to 200 million rupiah for "insulting" public institutions and authorities.[38] This has caused a major chilling effect among civil society activists who must

[35] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at C3; Agus Raharjo, *Sentenced to Six Years in Prison, Gus Nur: It's okay, God wills it*, Republik, 19 Apr. 2023.
[36] *Id.* at C3; Antara, Roy Suryo Divonis 9 Bulan Penjara di Kasus Ujaran Kebencian Meme Stupa, TEMPO, 28 Dec. 2022, https://nasional.tempo.co/read/1673326/roy-suryo-divonis-9-bulan-penjara-di-kasus-ujaran-kebencian-meme-stupa.
[37] Andrea Carson & Andrew Gibbons, *The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore*, 24 Journalism Studies 14, 3 May 2023, https://www.tandfonline.com/doi/full/10.1080/1461670X.2023.2192299.
[38] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at C2; Law (UU) on the Criminal Code No.1/2023.
Article 218 (1) Any person who in public attacks honor or dignity and personal dignity of the President and/or Vice President, shall be punished with a maximum imprisonment of 3 (three) years or a maximum fine of category IV. (2) It does not constitute an attack on honor or dignity as intended in paragraph (1), if the act is carried out in the public interest or self-defense.
Article 219 Any person who broadcasts, displays or attaches writing or images so that they are visible to the public, listens to recordings so that they can be heard by the public, or disseminates using information technology means an attack on the honor or honor and dignity of the President and/or Vice President with the intention of making its contents known or as is more commonly known, shall be punished with a maximum prison sentence 4 (four) years or a maximum fine of category IV.
Article 220 (1) Criminal acts as intended in Article 218 and Article 219 can only be prosecuted based on a complaint. (2) Complaints as intended in paragraph (1) can be made online written by the President and/or Vice President.

constantly be aware of potential legal prosecution as well as potential surveillance.[39] A report done by the Lembaga Survei Indonesia in 2019 shows that 43% of respondents (a rise from 17% five years prior) "were reluctant to express dissenting opinions on political matters."[40] Likewise, a survey done by Indikator Politik "found that almost 63 percent of Indonesians are afraid of expressing their opinions…due to a growing, quite obvious instrumentalisation of the country's laws and courts."[41]

4. **Persecution of those identifying as LGBTQ+**: The report of the Office of the United Nations High Commissioner for Human Rights on discrimination and violence against individuals based on their sexual orientation and gender identity stated that UN mechanisms call upon States to repeal laws criminalizing homosexuality. Further, the High Commissioner recommends that States address violence by "revising criminal laws to remove offenses relating to consensual same-sex conduct and other offenses used to arrest and punish persons on the basis of their sexual orientation and gender identity or expression."[42] "In August 2022, the Makassar District Court sentenced influencer Dimas Adipati to 18 months in prison and a fine of 25 million rupiah for violating Article 27(1) of the EIT Law by allegedly disseminating LGBTQ+ and pornographic content on Instagram."[43] Article 27(1) of the EIT criminalizes the distribution of "content that violates propriety"[44] and socially acceptable conduct. Members of the LGBTQ+ community are also often persecuted by the Antipornography Law.[45]

5. **Persecution of religious discourse:** In General Comment 34, it is held that blasphemy laws and other laws prohibiting displays of lack of respect for a religion are incompatible with the ICCPR.[46] This statement is qualified by the exception of "religious hatred that constitutes incitement

[39] Andreas Ufen, *The Rise of Digital Repression in Indonesia under Joko Widodo*, GIGA Focus Asia, No. 1, Hamburg: German Institute for Global and Area Studies (GIGA), 2024, https://doi.org/10.57671/gfas-24012.
[40] *Id*.
[41] *Id*.
[42] *Id*. at 21.
[43] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023.
[44] International Commission of Jurists, *Indonesia: Newly revised ITE Law threatens freedom of expression and must be amended*, International Commission of Jurists, 12 Jun. 2023, https://www.icj.org/indonesia-newly-revised-ite-law-threatens-freedom-of-expression-and-must-be-amended/.
[45] Human Dignity Trust, *Indonesia*, Human Dignity Trust, https://www.humandignitytrust.org/country-profile/indonesia/.
[46] CCPR/C/GC/34, 12 Sept. 2011, at para. 48.

to discrimination, hostility or violence."[47] However, this is not at issue. Here, those with critical views of religion are also suppressed by the GoI. The newly adopted revision of the criminal code ("RKUHP") expands the 1965 Blasphemy Law from one provision to six, including "defaming a religion, [and] persuading someone to be a non-believer…[these] articles violate the right to freedom of religion or expression and, like the current blasphemy law, [are] used to discriminate against religious minorities."[48] For example, "In April 2022, a court convicted YouTuber Muhammad Kece of spreading false information and sentenced him to 10 years' imprisonment. Kece, who had converted from Islam to Christianity and regularly criticized his former religion, was first arrested in August 2021 over videos that [Ministry of Communication and Informatics ("MoCI")] deemed to be blasphemous."[49] Also in June 2022, Abdul Qadir Hasan Baraja, the leader of Khilafatul Muslimin, an Islamist group whose teachings were in direct contradiction to *Pansacila*, was sentenced to 10 years in prison. The GoI also blocked the organization's website and YouTube channel.[50]

6. **Persecution of users on social media and the Internet:** General Comment 34 holds that the freedom of opinion and the freedom of expression are "indispensable conditions for the full developed person."[51] Further, the freedom to an uncensored press and media is also essential to ensure these freedoms.[52] A new criminal code adopted in December 2022 threatens to motivate self-censorship through its provisions on spreading false information, treason, and insulting the president, among other speech-related offenses."[53] Journalists have observed a culture of self-censorship among online media users.[54] "Editor-in-chief of Tempo

[47] United Nations (General Assembly). (1966). International Covenant on Civil and Political Rights. Treaty Series, 999, 171, at art. 20.
[48] Andreas Harsono, *Indonesia to Expand Abusive Blasphemy Law*, Human Rights Watch, 31 Oct. 2019, https://www.hrw.org/news/2019/10/31/indonesia-expand-abusive-blasphemy-law.
[49] *Id.* at C3; Rachmawati, *Ditangkap di Bali, Siapakah Youtuber Muhammad Kece?*, Kompas.com, 25 Aug. 2021, https://regional.kompas.com/read/2021/08/25/161000578/ditangkap-di-bali-siapakah-youtuber-muhammad-kece.
[50] Isal Mawardi, *Abdul Qadir Hasan Baraja, Leader of Khilafatul Muslimin Sentenced to 10 Years in Prison*, DetikNews, 25 Jan. 2023, https://news.detik.com/berita/d-6533247/abdul-qadir-hasan-baraja-pimpinan-khilafatul-muslimin-divonis-10-tahun-bui.
[51] CCPR/C/GC/34, 12 Sept. 2011, at para. 2.
[52] *Id*. at para. 13.
[53] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B4.
[54] Andrea Carson & Andrew Gibbons, *The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore*, 24 Journalism Studies 14, 3 May 2023, https://www.tandfonline.com/doi/full/10.1080/1461670X.2023.2192299.

Magazine, Wahyu Dhyatmika, observed that the laws in Indonesia were (paradoxically) constraining freedom of expression online because people feared they would be targeted by government actors for the content they posted."[55] Further regarding political issues and electoral debate, "a proliferation in harassment by networks of paid commentators, or 'buzzers,' may further incentivize self-censorship on political topics." Citizens are likely to self-censor on a variety of other topics that can be criminalized as well. "Individuals who write, promote, or broadcast information about contraceptives or abortion face up to six months in prison and a fine of 10 million rupiah. Individuals can face up to four years in prison for spreading information about communism, and up to 10 years for 'associating' with communism."[56]

7. **GoI's failure to respond to LOIPR on EIT Law issues:** GoI fails to address in their report EIT Law being used to intimidate journalists and critics and GoI also fails to provide the number of relevant prosecutions. Currently, Article 27A, Article 28 (3), and Article 45A (3) of the 2023 amended EIT Law criminalizing "speech attacking the honor or reputation of others/defamation" and "false information causing social unrest" can be utilized to intimidate journalism. GoI wrote in the State Party report that EIT Law will work "as a bridge" to regulate the crimes specified in the 2022 amended Criminal Code which will become effective much later in 2026. Indeed, during the transition period, EIT Law will be used for intimidation towards journalism, and such intimidation effect will be even greater when the similarly phrased Penal Code becomes effective. GoI answered that "a review team by the Coordinating Minister for Political, Legal and Security completed its task by recommending several articles in the EIT Law to be revised and formulating guidelines for their implementation." But GoI should clearly answer that Article 27A, 45(4) (criminalizing defamation), 28(3), 45A (criminalizing fake news) will be reviewed. Also, guidelines for EIT Law implementation is not effective since it is not a binding regulation. Judges and prosecutors in EIT Law cases do not consider the implementation guidelines to punish legitimate expression.

B. **Suppression of Speech**

[55] *Id*.
[56] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at C2.

1. **Suppression on social media and the Internet**: The report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recommends that State's should not establish laws which require "proactive" monitoring and filtering of content.[57] Further, States should "refrain from adopting models of regulation where government agencies [such as MoCI], rather than judicial authorities, become the arbiters of lawful expression."[58] The GoI, through MoCI rather than the judiciary, has cracked down on social media and internet posts and sites. "Websites are frequently blocked for hosting what the government defines as 'negative' content."[59] "In 2022, MoCI ordered the blocking of 213,735 web pages, including…1,266 pages that were identified as 'negative' by government agencies."[60] This blocking occurs through Domain Name System ("DNS") hijacking through virtual private networks ("VPN"s) and targets content including "LGBTQ+ content, news media, and human rights content."[61] Regarding the suppression of LGBTQ+ content, data collected through an OONI web connectivity test conducted between January and June of 2022 found that LGBTQ+ content was often blocked by the government as "negative content," "a broad term used to describe material that is defamatory or that violates social or moral norms."[62] For example, MoCI has blocked multiple LGBTQ+ dating apps such as Grindr and Blued.[63] Further in 2021, MoCI requested that YouTube "remove a video deemed to promote LGBT+ content on YouTube Kids."[64] People have also been arrested for disseminating LGBTQ+ content. More generally, according to Google's transparency report, between January and June of 2022 the GoI "sent 119 content removal requests covering 567 items; Google removed 86.6 percent of the content in question. In the second half of the year, the government issued 190 takedown requests concerning 1,995 items, and Google complied in removing 48.7 percent of them."[65] Additionally, "in the second half of

[57] A/HRC/38/35, 6 Apr. 2018, at para. 3
[58] *Id*. at para. 4.
[59] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B1.
[60] *Id*.
[61] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B1.
[62] *Id*.
[63] Isal Mawardi, *Kominfo Blocks 3 Applications Related to Porn Content: Blued to Grindr*, DetikNews, 25 Nov. 2020, https://news.detik.com/berita/d-5269068/kominfo-blokir-3-aplikasi-terkait-konten-porno-blued-hingga-grindr.
[64] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B2.
[65] *Id*.; Google Transparency Report, *Government requests to remove content*, Google, https://transparencyreport.google.com/government-removals/government-requests/ID?hl=en&lu=country_item_amo

2022…TikTok received 2,713 requests for content and account removal from the Indonesian government."[66] MoCI has also blocked major websites and financial services that were not directly licensed by the government.[67] "The government's broad definition of negative content that can be blocked or removed and its intensifying pursuit of legal penalties for online activity contribute to an environment of self-censorship among journalists and ordinary users alike. Many social media users have expressed their fear of the EIT Law. According to an April 2022 survey from Indikator Politik Indonesia, 62.9 percent of respondents thought that today's society is increasingly afraid to express opinions."[68]

2. **Suppression through lack of anonymity of SIM cards**: In the report on encryption, anonymity, and the human rights framework, encryption and anonymity create "a zone of privacy" which is used to protect people's opinions and beliefs.[69] Anonymity protects journalists, CSOs, and others from surveillance and harassment.[70] Anonymity furthers the interests of the rights to privacy, opinion, and expression all of which are codified in treaty bodies, regional courts, and by the Human Rights Council ("UNHRC").[71] Furthermore, the report discusses how governments should refrain from SIM card registration with personally identifiable data which directly undermines anonymity.[72] "In 2017, MoCI introduced a new regulation requiring SIM card users to register by submitting their national identity numbers and their family registration numbers, thereby limiting anonymity. Beginning in late February 2018, failure to comply with this requirement could lead to the temporary blocking of data services to the unregistered SIM cards. If users fail to register within 15 days of the block's initiation, the SIM cards can be permanently blocked from any telecommunications services. In 2020, the government announced a plan

---

unt&country_item_amount=period:2022H1;group_by:requestors&country_request_amount=group_by:requestors;period:2022H1.

[66] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B2; TikTok, *Government Removal Request Report January 1, 2022-June 30, 2022*, TikTok, https://www.tiktok.com/transparency/id-id/government-removal-requests-2022-1/.

[67] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B4.

[68] *Id*.; Moh. Khory Alfarizi, *Indonesian Political Indicator Survey: 62.9 Percent of People Are Increasingly Afraid to Have an Opinion*, tempo.co, 9 Apr. 2022, https://nasional.tempo.co/read/1580168/survei-indikator-politik-indonesia-629-persen-rakyat-semakin-takut-berpendapat.

[69] A/HRC/29/32, 22 May 2015, at para. 12.

[70] *Id*. at para. 12.

[71] *Id*. at para. 14.

[72] *Id*. at para. 51.

to roll out the use of biometric data for SIM card registration in 2021, but there were no updates on the implementation of this plan during the coverage period."[73]

C. **Failure to Protect Online Safety:** The GoI failed to protect online safety of vulnerable groups, prevent digital attacks, and stop the spread of dangerous disinformation.

1. **Online gender-based violence:** The international community has expressed increasing concern over the safety of women and girls in digital spaces. While international law is still developing in this area, the UNHRC recognizes the principle that human rights protected offline should also be protected online.[74] Additionally, the Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective identifies online gender-based violence ("OGBV") as a violation of women's human rights, and affirms that states should protect women online "through the prohibition of [online] gender-based violence."[75] The Report simultaneously recognizes the importance of balancing protections of other international human rights obligations, and clarifies "that any State-imposed content restrictions should be provided by law, pursue one of the purposes set out in article 19, paragraph 3 of the Covenant, and respect the principles of necessity and proportionality."[76] Taken together, the UNHRC's various relevant reports and resolutions indicate that states have an obligation to prevent OGBV without unnecessarily and arbitrarily encroaching on other rights. The GoI's shortcomings in addressing OGBV have resulted in a hostile online environment that stifles digital expression. There is a slight gender divide in Indonesian internet use, with only 48.81% of internet users being women[77] despite making up 49.7% of the population.[78] This divide could be due in part to the 1,052 complaints of OGBV, primarily made by women, recorded by SAFEnet in 2023.[79] These complaints encompass a range of abuses, including image-based sexual abuse (559 cases), non-consensual distribution of intimate images (155

[73] *Id*. at C4.
[74] A/HRC/RES/32/13, 1 Jul. 2016.
[75] A/HRC/38/47, 18 Jun. 2018, at para. 17.
[76] *Id.* at para. 52; A/HRC/17/27, 16 May 2011, at para. 24; A/66/290, 10 Aug. 2011, at para. 15.
[77] *Digital Rights in Indonesia Situation Report 2023*, SAFEnet, Feb 2024, p.2.
[78] The World Bank, *World Bank staff estimates based on age/sex distributions of United Nations Population Division's World Population Prospects: 2022 Revision.*
[79] *Digital Rights in Indonesia Situation Report 2023*, SAFEnet, Feb 2024, p.30.

cases), extortion using sexual images (133 cases), flaming (35 cases), doxing (31 cases), and others (138 cases).[80] Vulnerable groups, such as sexual and gender minorities, are particularly at risk for online harassment.[81] Also concerning is that 21.87% of children aged 12-17 reported incidents of gender-based violence across the archipelago.[82] Most victims report being targeted "by strangers on social media, with communications progressing to messaging applications before sending or making video calls of a sexual nature… [which] are often recorded by the perpetrator without the knowledge of the victim."[83]

2. **Digital attacks:** The UNHRC **"**[c]alls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online… in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development."[84] In Indonesia, digital attacks directly compromise individuals' internet safety and privacy. SAFEnet documented at least 625 digital attacks throughout 2022-2023, primarily aimed at public organizations, academia, journalists and media.[85] More than 75% of these attacks involved technical methods such as hacking, data breaches, and phishing.[86] One example of these attacks occurred in September 2022, when a significant cyber attack targeted the Twitter accounts of the current affairs television program Mata Najwa and approximately 30 Narasi TV journalists, staff, and former staff.[87] Additionally, the personal data of 105 million Indonesians, about 40% of the country's population, was reportedly stolen from the General Elections Commission and sold in September 2022.[88] A minimum of 40 cases of data breaches in 60 Indonesian public institutions occurred during 2022, underscoring the alarming state of cybersecurity in the country.[89]

---

[80] *Id.* p.33.
[81] Digital Rights in Indonesia Situation Report 2022, *The Collapse of Our Digital Rights,* SAFEnet, Feb. 2023.
[82] *Id.* p.32.
[83] Digital Rights in Indonesia Situation Report 2022, *The Collapse of Our Digital Rights,* SAFEnet, Feb. 2023.
[84] A/HRC/RES/32/13, 1 Jul. 2016, at para. 8.
[85] *Digital Rights in Indonesia Situation Report 2023*, SAFEnet, Feb 2024, p.23.
[86] *Digital Rights in Indonesia Situation Report 2023*, SAFEnet, Feb 2024, p.24.
[87] Digital Rights in Indonesia Situation Report 2022, *The Collapse of Our Digital Rights,* SAFEnet, Feb. 2023.
[88] Vilius Petkauskas, *Hackers leak sensitive data of over 105m Indonesian citizens,* Cybernews, 7 Sept. 2022, https://cybernews.com/news/hackers-leak-sensitive-data-of-over-105m-indonesian-citizens/.
[89] SAFEnet, *Laporan Situasi Hak-hak Digital Indonesia 2023,* Feb. 2023, https://safenet.or.id/id/2023/03/safenet-pemenuhan-hak-hak-digital-di-indonesia-kian-memburuk/.

3. **Spread of disinformation:** Disinformation is often a tool to incite hatred or violence. Article 20 (2) of the ICCPR states that advocacy of national, racial, or religious hatred constituting incitement to discrimination, hostility, or violence should be prohibited by law, but does not call for criminalization.[90] In 2021, the Special Rapporteur addressed the growing issue of disinformation and its relationship to freedom of expression.[91] Again affirming the importance of balancing state action to combat disinformation with state obligations under international human rights law, the Rapporteur emphasizes that "States should not make, sponsor, encourage or disseminate statements that they know or should reasonably know to be false."[92] The spread of disinformation, particularly in the context of elections and government affairs, is a rampant issue in Indonesia. Reports from the Oxford Internet Institute identified the country as a hotspot for "buzzers,"[93] online propagandists who are paid to disseminate fake news, defame individuals, or influence public opinion on certain political measures, products, or candidates. Buzzers, as well as representatives of political parties and supporters of certain candidates, form digital networks to manipulate trending topics and suppress ones that would otherwise appear organically.[94] By pushing targeted trends and topics, a small number of people exert great influence over major social and political narratives. The consequences of such manipulation were starkly evident in the 2019 presidential election, when Prabowo Subianto made baseless accusations of systemic fraud.[95] Coupled with an online disinformation campaign, this led to riots in Jakarta resulting in six deaths and hundreds of injuries.[96] The spread of disinformation in Indonesia is not just perpetrated by private individuals; in 2020, the GoI allocated 90 billion rupiah (approximately $5.7 million USD) to hire buzzers for

[90] A/HRC/47/25, 13 Apr. 2021.
[91] *Id*.
[92] *Id*. at para. 88.
[93] Samantha Bradshaw, Ualan Campbell-Smith, Amelie Henle, Antonella Perini, Sivanne Shalev, Hannah Bailey and Philip N. Howard, *Country Case Studies Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*, Oxford Internet Institute/University of Oxford, 2020, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/03/Case-…; Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation,* Oxford Internet Institute/University of Oxford, 26 Sept. 2019, https://demtech.oii.ox.ac.uk/research/posts/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/.
[94] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023, at B5.
[95] Andreas Ufen, *The Rise of Digital Repression in Indonesia under Joko Widodo*, GIGA Focus Asia, No. 1, Hamburg: German Institute for Global and Area Studies (GIGA), 2024, https://doi.org/10.57671/gfas-24012.
[96] *Id.*

promoting its policies.[97] Another state-sponsored disinformation campaign which distributed pro-government propaganda in Papua through various social media platforms was discovered in 2019.[98] In January 2020, a military-funded network of online news sites was exposed for spreading propaganda, criticizing dissidents and human rights advocates, and mobilizing support for the government's violent response to the 2019 Papua protests.[99]

4. **Government's lack of action on spread of disinformation against Rohingya in Aceh:** The GoI has failed to adequately address the spread of disinformation targeting Rohingya refugees in Aceh, exacerbating hate speech against all refugees and culminating in harmful actions such as their forced eviction.[100] Despite widespread reports of false and inflammatory content circulating on social media platforms, authorities have not taken sufficient steps to combat this harmful phenomenon. The dissemination of disinformation not only exacerbates tensions and contributes to the stigmatization of Rohingya refugees but also undermines efforts to promote social cohesion and respect for human rights.

D. **Impairment of Access to the Internet:** The Government of Indonesia failed to protect the right to information by impairing or failing to remove impairments to access to the internet.

1. **Government restrictions on content:** Article 19 of the ICCPR establishes that any restrictions on internet content must (1) be contained within an unambiguous law, (2) pursue a legitimate purpose, and (3) respect the principles of necessity and proportionality.[101] Additionally, General Comment 34 clarifies that any restrictions "must be the least

[97] Indonesia Corruption Watch, *Government Digital Activities: Reviewing Social Media and Influencer Budgets,* 1 Sept. 2020, https://antikorupsi.org/index.php/en/article/government-digital-activities-reviewing-social-media-and-influencer-budgets/; *Measuring Reasons for the Jokowi Government to Budget IDR 90 Billion for Buzzers*, VOI, 21 Aug. 2020, https://voi.id/berita/11723/menakar-alasan-pemerintahan-jokowi-anggarkan-rp90-miliar-untuk-i-buzzer-i/.
[98] Benjamin Strick and Famega Syavira, *Papua Unrest: Social Media Bots 'Skewing the Narrative,'* BBC News, 11 Oct. 2019, https://www.bbc.com/news/world-asia-49983667.
[99] Tom Allard and Jack Stubbs, *Indonesian Army Wields Internet 'News' as a Weapon in Papua*, Reuters, 7 Jan. 2020, https://www.reuters.com/article/us-indonesia-military-websites-insight/indonesian-army-wields-internet-news-as-a-weapon-in-papua-idUSKBN1Z7001/.
[100] Darmawan, R. K., *Kronologi Mahasiswa Usir Pengungsi Rohingya di Banda Aceh,* https://regional.kompas.com/read/2023/12/28/160157878/kronologi-mahasiswa-usir-pengungsi-rohingya-di-banda-aceh, KOMPAS.com, 28 Dec. 2024.
[101] Article 19.

intrusive instrument amongst those which might achieve their protective function" and "must be proportionate to the interest to be protected."[102] A 2018 Special Rapporteur report also advised states against heavy-handed crackdowns on Internet intermediaries given the significant chilling effect of such measures.[103] In Indonesia, websites are frequently blocked for hosting content classified as "negative," encompassing material deemed defamatory or violating social and moral norms.[104] Concerns have been raised about MoCI's independence as a regulator since the 2020 dissolution of the Indonesian Telecommunication Regulatory Body.[105] MoCI's website blocking activities have targeted massive platforms such as Yahoo, PayPal, and Netflix. The blocking of Netflix in 2016, citing improper licensing and exposure to violent and pornographic content, showcases their questionable censorship efforts.[106] LGBTQ+ dating sites Grindr and Blued have also previously been targeted with Grindr still downloadable but not operable.[107] Despite the accessibility of tools to circumvent online censorship and the prevalence of VPN services, 36 websites providing anonymization and circumvention tools were blocked in 2022.[108] VPN restrictions limit citizens' ability to access diverse content and viewpoints, thereby hindering their right to freely express themselves and engage with global discourse. The GoI also scrutinized VPN providers after authorities placed restrictions on social media during the May 2019

[102] CCPR/C/GC/34, 12 Sept. 2011, at para. 34.
[103] A/HRC/38/35, 6 Apr. 2018.
[104] *Ragam Konten yang Bisa Diadukan Melalui aduankonten.id,* kominfo.go, 16 Aug. 2017, https://www.kominfo.go.id/content/detail/10331/ragam-konten-yang-bisa-diadukan-melalui-aduankontenid/0/videografis/.
[105] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at A5.
[106] Fadly Yanuar Iriansyah, *Why Only Telkom and Telkomsel Block Netflix?,* Tech In Asia, 27 Jan. 2016, https://id.techinasia.com/talk/kenapa-hanya-telkom-dan-telkomsel-yang-memblokir-netflix; Eko Wahyudi, *Telkom Reveals the Cause for Not Yet Unblocking Netflix Until Now,* Tempo.com, 24 Feb. 2020; https://bisnis.tempo.co/read/1311632/telkom-ungkap-penyebab-belum-buka-blokir-netflix-hingga-saat-ini; Yoga Hastyadi Widiartanto, *Netflix Blocked by Telkom, Minister of Communication and Information Issues Regulations,* Kompas, 27 Jan. 2016, https://tekno.kompas.com/read/2016/01/27/20040007/Netflix.Diblokir.Telkom.Menkominfo.Beberkan.Regulasi; Amal Nur Ngazis, *IndiHome Can Access Netflix, Telkom: Block Stay Applies,* Viva, 21 Jan. 2019, https://www.viva.co.id/digital/digilife/1113717-indihome-bisa-akses-netflix-telkom-blokir-tetap-berlaku/.
[107] CNN Indonesia, *List of 'Victims' Blocking Kominfo Throughout 2018,* 26 Dec. 2018, https://www.cnnindonesia.com/teknologi/20181226001641-192-356335/daftar-korban-blokir-kominfo-sepanjang-2018; Isal Mawardi, *Kominfo Blocks 3 Applications Related to Prorn Content: Blued to Grindr,* Detik News, 25 Nov. 2020, https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.
[108] Rob Marvin, *Breaking Down VPN Usage Around the World*, PC Mag, 21 Sept. 2018, https://www.pcmag.com/news/breaking-down-vpn-usage-around-the-world; *iMAP State of Internet Censorship Country Report 2022 - Indonesia*, Sinar Project, 2022, https://imap.sinarproject.org/reports/2022/the-state-of-internet-censorship-in-indonesia-2022/.

protests.[109] This move represents a concerted effort to control the flow of information and curtail citizens' ability to bypass censorship measures. Furthermore, MoCI utilizes various tools for content regulation including the 2018 launch of Cyber Drone 9, an AI-driven crawler system to proactively detect content violations.[110] Ministerial Regulation 5 ("MR 5/2020"), which took effect in November 2020, requires private scope electronic system operators ("ESO"s) (any foreign or domestic entity that operates electronic systems for Indonesian users) to ensure that they do not contain "any content that violates domestic law, creates community anxiety, or disturbs public order."[111] Upon a violation being detected, ESOs are given a strict 24-hour notice (or just four hours in "urgent" situations) to comply with the removal of the prohibited content.[112] Failure to do so may result in fines or blocking. The law was amended in 2021 to require ESOs to register with the Indonesian government upon launching a platform in the country.[113] In July 2022, several major platforms, including Amazon, Yahoo, Bing, Steam, and PayPal, faced temporary blocking for failing to register.[114] The Jakarta Legal Aid Institute and Digital Freedom Advocacy filed a lawsuit against MoCI in November 2022 challenging the law's enforcement, claiming harm to users and an overly broad legal interpretation.[115] Additionally, Article 40 of the EIT Law permits MoCI to

[109] Yudha Pratomo and Reska K. Nistanto, *Kominfo Bakal Atur Penggunaan VPN di Indonesia*, Kompas, 14 Jun. 2019, https://tekno.kompas.com/read/2019/06/14/07555487/kominfo-bakal-atur-penggunaan-vpn-di-indonesia; Coconuts Jakarta, *Blocking the unblocker: Indonesia tells VPN providers to obtain local license or face ban*, 4 Jul. 2019, https://coconuts.co/jakarta/news/blocking-the-unblocker-indonesia-tells-vpn-providers-to-obtain-local-license-or-face-ban/.

[110] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at B1.

[111] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at B3; Regulation of the Minister of Communications and Information Technology Number 5 of 2020, kominfo.go, May 2021, https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

[112] Fanny Potkin and Stefanno Sulaiman, *Indonesia preparing tough new curbs for online platforms -sources*, Reuters, 23 Mar. 2022, https://www.reuters.com/world/asia-pacific/exclusive-indonesia-preparing-tough-new-curbs-online-platforms-sources-2022-03-23/.

[113] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at B3.

[114] Stanley Widianto, *Google yet to register for Indonesia's new licensing rules,* Reuters, 20 Jul. 2022, https://www.reuters.com/technology/google-twitter-yet-sign-up-indonesias-new-licensing-rules-ministry-2022-07-20; *Pendaftaran Penyelenggara Sistem Elektronik (PSE) Lingkup Privat,* Kominfo, 29 Jul. 2022, https://m.kominfo.go.id/content/detail/43385/siaran-pers-no-308hmkominfo072022-tentang-pendaftaran-penyelenggara-sistem-elektronik-pse-lingkup-privat/0/siaran_pers.

[115] Rizki, Mochamad Januar, *Buntut Pemblokiran 8 Platform Digital, Tim Advokasi Kebebasan Digital Gugat Kominfo.,* hukumonline.com, 1 Dec. 2022.

directly block access to certain content or order internet service providers ("ISP"s) to do so.[116] MoCI provides regular press briefings listing the websites it has blocked, but provides no insight into why.[117] Several other government agencies, including BSSN, are permitted to restrict online content under the EIT Law.[118] Article 26 establishes a "right to be forgotten," requiring ESOs to delete information upon MoCI's request, provided the ministry obtains a court order.[119] Critics have expressed concern that this practice could hamper the public's right to information. Finally, the implementation of national DNS filtering technology has been criticized for its potential resemblance to China's repressive filtering system known as the Great Firewall.[120]

2. **State-authorized connectivity disruptions:** The UNHRC "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law."[121] The Special Rapporteur has discouraged the use of state-authorized internet shutdowns, noting the danger they pose to the

https://www.hukumonline.com/berita/a/buntut-pemblokiran-8-platform-digital--tim-advokasi-kebebasan-digital-gugat-kominfo-lt638889cb3d0e1/.

[116] The Jakarta Post, *Revised ITE Law could hamper freedom of expression: Researcher,* 31 Oct. 2016, https://www.thejakartapost.com/news/2016/10/31/revised-ite-law-could-hamper-freedom-of-expression-researcher.html/.

[117] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at B3.

[118] Oka Anantajaya, *Amendment to the Electronic Information and Transaction Law,* MKK Newsletter, Feb. 2017, http://www.mkklaw.net/newsletter/2017_02_newsletter_en.pdf.; Ihsanuddin, *Jokowi Signs the Presidential Decree, National Cyber Agency Directly Under the President,* Kompas, 1 Feb. 2018, https://nasional.kompas.com/read/2018/01/02/17103991/jokowi-teken-perpres-badan-siber-nasional-langsung-di-bawah-presiden; Presidential Regulation of the Republic of Indonesia Number 53 Year 2017 Concerning National Cyber and Crypto Agency, JDIH, 23 May 2017, https://jdih.bssn.go.id/arsip-hukum/presidential-regulation-of-the-republic-of-indonesia-number-53-year-2017-concerning-national-cyber-and-crypto-agency; Presidential Decree Number 133 of 2017 Concerning Amendments to Presidential Regulation Number 53 of 2017 Concerning the National Cyber and Crypto Agency, JDIH, 16 Dec. 2017, https://jdih.bssn.go.id/arsip-hukum/peraturan-presiden-nomor-133-tahun-2017-tentang-perubahan-atas-peraturan-presiden-nomor-53-tahun-2017-tentang-badan-siber-dan-sandi-negara; Badan Siber dan Sandi Negara (BSSN), *Duties of BSSN,* 2018, https://bssn.go.id/tugas-dan-fungsi-bssn/.

[119] Baker McKenzie, *Electronic Information and Transactions Law Amended in Indonesia*, 8 Nov. 2016, https://web.archive.org/web/20170109171800/http://www.bakermckenzie.com/en/insight/publications/2016/11/amendment-to-law-no-11-of-2008/; CNN Indonesia, *Kominfo Will Issue "Right to Be Forgotten" Regulation*, 31 Oct. 2018, https://www.cnnindonesia.com/teknologi/20181031200550-213-343043/kominfo-bakal-keluarkan-permen-hak-untuk-dilupakan; LBH Press, *The Right to Deletion of Information in Indonesia, Jakarta,* 2018, http://lbhpers.org/wp-content/uploads/2018/09/e-book-RTBF.pdf; Jens-Henrik Jeppesen, *EU Court: Privacy Rights Trump Free Expression and Access to Information,* Center for Democracy and Technology, 14 May 2014, https://cdt.org/insights/eu-court-privacy-rights-trump-free-expression-and-access-to-information/.

[120] Javier Fernando, *Crazy National DNS, Indonesian Internet Access Becomes Limited?,* GameBrott, 31 Jul. 2022, https://gamebrott.com/dns-nasional-akses-internet-indonesia-jadi-terbatas/.

[121] A/HRC/RES/32/13, 18 Jul. 2016, at para. 10.

free flow of information.[122] Connectivity disruptions during religious events and protests further highlight the GoI's attempts to control freedom of expression. Examples include disruptions in Wadas in February 2022 amid anti-mining project protests, and the blocking of websites and blogs affiliated with the Papuan Student Alliance during the 60th anniversary protests in May 2023.[123] The GoI's recent content-censoring practices are of particular concern following the partial internet shutdowns in Papua and West Papua in August and September of 2019.[124] In their report, the GoI partially addresses these concerns by noting that the shutdown was put in place to stop the "spread of hoax and disinformation [that] may escalate ongoing violence."[125] Amid significant backlash, Indonesia's Administrative Court reviewed the decision and regarded the internet shutdown as unlawful.[126] As the GoI points out, however, this decision was based on procedural rather than substantive aspects of the policy, and the Court otherwise legitimized the substantive reasoning for the shutdown. Moreover, the ruling overturned a 2020 precedent set by the Jakarta State Administrative Court which held that "the EIT Law should only be used to restrict online information or documents that are 'unlawful,' not to terminate access in its entirety."[127] This broad decision warrants continued scrutiny over any state-authorized connectivity disruptions.

3. **GoI fails to respond to the Committee's concern about the Internet shutdown in Papua:** Although GoI touts its "checks and balances" system that struck down the Internet shutdown, GoI does not mention

[122] A/HRC/47/25, 13 Apr. 2021, at para. 88.
[123] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at A3; Rani Rahayu and May Rahmadi, *Derasnya Penindasan Hak Digital di Wadas,* detikX, 21 Feb. 2022, https://news.detik.com/x/detail/investigasi/20220221/Derasnya-Penindasan-Hak-Digital-di-Wadas/.
[124] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at A3; BBC News Indonesia, *PTUN Jakarta Rules Internet Blocking in Papua and West Papua "Violates the Law,"* 3 Jun. 2020, https://www.bbc.com/indonesia/majalah-52901391; SAFEnet, *PTUN Jakarta Declares the Termination of Internet Access in Papua Unlawful,* 4 Jun. 2020, https://safenet.or.id/id/2020/06/rilis-pers-ptun-jakarta-menyatakan-pemutusan-akses-internet-di-papua-melanggar-hukum/.
[125] CCPR/C/IDN/2, Distr. 27 May 2022, at para. 225.
[126] FreedomHouse, *Freedom on the Net 2023: Indonesia*, 2023, https://freedomhouse.org/country/indonesia/freedom-net/2023 at A3; Abdul Manan, *Jakarta State Administrative Court Rules Government Internet Shutdown in Jakarta Unlawful,* Alliance of Independent Journalists, 4 Jun. 2020, https://aji.or.id/read/press-release/1078/jakarta-state-administrative-court-rules-government-internet-shutdown-in-papua-unlawful.html.
[127] *Id.*

what it will do to prevent further unlawful shutdowns or to compensate the victims of the Internet shutdown.

4. **SIM card registration requirements for refugees:** The GoI requirement for SIM card registration with valid identification has effectively cut off refugees' access to the internet, as they lack recognized national identity documents to fulfill this requirement. This policy violates fundamental human rights, including the right to freedom of expression and access to information, as well as refugees' digital rights essential for communication and integration.

E. State Surveillance and Violation of the Right to Privacy

1. Privacy serves as a basis for other fundamental human rights, such as freedom of expression, freedom of association and assembly, and freedom of movement, and without which the other rights would not be effectively enjoyed.[128] Therefore, Article 12 of the Universal Declaration of Human Rights and Article 17 of the ICCPR both ensure the protection of the right to privacy, stating that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation," and that "everyone has the right to the protection of the law against such interference or attacks." Indonesia recognizes the right to privacy as a constitutional right in Article 28G(1) of the 1945 Constitution, and guarantees the protection of communication and information under Article 28F. The protection of the right to privacy is also defined in the provisions of Law No. 39 of 1999 on Human Rights[129], which was further strengthened by the ratification of the ICCPR into Indonesian national law through Law No.12 of 2005. Nevertheless, the possibility of arbitrary or unlawful surveillance and violation of the right to privacy by Indonesian government authorities are found in many aspects.

Article 17 of the ICCPR is subject to the "permissible limitations test," which has been applied equally to Article 19 (freedom of expression) and Article 22 (freedom of association). The permissible limitations test includes, inter alia, the following elements: legality; legitimacy of the aim; and necessity (which has been held to include requirements of adequacy

[128] A/HRC/13/37, 28 Dec. 2009, at para. 33.

[129] Article 29(1), Article 30, Article 31(2), Article 32.

and proportionality).[130, 131] Indonesian legislations and the government's practices of communications interference fail to follow the principles.

2. **Lack of legality and legal certainty:** In Indonesia, the practice of communication interception is allowed by various legislations for law enforcement, state intelligence, and enforcement of judges' code of ethics.[132] However, The Human Rights Committee has affirmed that "arbitrary interference" in Article 17 of the ICCPR can also extend to interference provided for under the law.[133] That is, merely passing a law that authorizes state surveillance does not make the surveillance lawful. The Human Rights Committee and the European Court of Human Rights both clarified that "law" requires accessibility, specificity and foreseeability.[134] Since secret surveillance distinctively threatens the essence of democracy,[135] the above requirements take a special meaning in the context of surveillance — minimum safeguards against intrusive surveillance, such as the subject, time limit, precaution, or supervision in the use of surveillance power, must be specifically laid down in the statute.[136]

    a) **Absence of communications surveillance legislation:** Ben Emmerson, in his report to the UN General Assembly in 2014 as Special Rapporteur, stated that a "quality of law" requirement imposes three conditions: "(a) the measure must have some basis in domestic law; (b) the domestic law itself must be compatible

[130] A/HRC/13/37. 28 Dec. 2009, at paras. 16-18; A/HRC/23/40, 17 Apr. 2013, at paras. 28-29.

[131] International Principles on the Application of Human Rights to Communications Surveillance provides 13 principles to apply when evaluating whether the surveillance laws and practices around the world are compatible with human rights: (1) Legality; (2) Legitimate Aim; (3) Necessity; (4) Adequacy; (5) Proportionality; (6) Competent Judicial Authority; (7) Due Process; (8) User Notification; (9) Transparency; (10) Public Oversight; (11) Integrity of Communication and Systems; (12) Safeguards for International Cooperation; (13) Safeguards Against Illegitimate Access and Right to Effective Remedy. The first version of the Principles was finalised on 10 July 2013, officially launched at the UN Human Rights Council in Geneva in September 2013, and was revised, re-launched in May 2014. Up to present, the Principles have been signed by over 400 organizations and 300,000 individuals throughout the world. The full text is available at: https://necessaryandproportionate.net/principles/.

[132] Wahyudi Djafar, Bernhard Ruben Fritz Sumingar, Blandina Lintang Setianti, *Legal Reform of Interception of Communications: An initiative to establish an interception of communications law from human rights perspective*, Institute for Policy Research and Advocacy (ELSAM) Privacy International, 2016, p.34.

[133] HRI/GEN/1/Rev.9 (Vol. I), 2008, pp.191-193, at para. 4.

[134] CCPR/C/GC/34, 12 September 2011, at para. 25.; *The Sunday Times vs. The United Kingdom*, no. 6538/74; 26 Apr. 1979, at para. 49.

[135] *Klass and Others v. Germany*, no. 5029/71, 6 Sept. 1978, paras. 37, 42, and 49.

[136] EEF, Article 19, *International Principles on the Application of Human Rights to Communications Surveillance: Background and Supporting International Legal Analysis*, May 2014, p.17.; *Weber & Savaria v. Germany*, no. 54934, 29 Jun. 2006, at para. 95.

with the rule of law and the requirements of the Covenant; and (c) the relevant provisions of domestic law must be accessible, clear and precise." However, there is no single legislation in Indonesia that specifically regulates the interception of communications. The 2008 EIT Law stipulated that the provisions on procedures for interception shall be regulated by Government Regulation. After the Constitutional Court decision in 2010 stated that communications surveillance requires control at the level of statute, not by regulation,[137] Law No. 19 of 2016 on the Amendment of 2008 EIT Law (hereinafter "2016 Amendment Law") specified that interception to be regulated under the law. Yet, no further legislation has been adopted.

b) **Lack of specificity and foreseeability:** Indonesian laws that regulate state surveillance do not clearly define the scope and the manner of interception, despite the Constitutional Court decision in 2010 that asserted government agencies must have detailed and regulated interception procedures[138] and several amendments in response to it.[139] For example, 2008 EIT Law Article 31(3) widely recognised "interception carried out in the framework of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as stated by laws" as a legal act, without any requirement for permission or oversight. It does not mention the scope of the intercepted materials or the categories of situations in which the act is done. Meanwhile, the 2016 Amendment Law broadens the authorities of civil servant investigators under Article 43, by allowing them to request information and access restricted data or electronic systems that are engaged in crimes, and to carry out raids without court

[137] Decision of the Constitutional Court No. 5/PUU-VIII/2010, 24 Feb. 2011, https://www.mkri.id/public/content/persidangan/putusan/Putusan%20%205_PUU_VIII_2010%20_edit%20panitera_.pdf; ELSAM, *The Right to Privacy in the Indonesia - Stakeholder Report Universal Periodic Review 27th Session: Indonesia*, Sept. 2016, at para 18.
[138] *Id.*

[139] 2016 amendments to the Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Electronic and Transaction (EIT Law); 2018 amendments to the Law No. 15 of 2003 on the Eradication of the Crime of Terrorism (Anti‑Terror Law).

warrants.[140] An immense power is granted to various state actors without adequate safeguards.

There are at least twelve legislations that provide the authority of interception of communications, including the Criminal Procedural Code and Telecommunications Law[141], but none of them include the restriction of people accessing, detailed procedure of interception and using intercepted materials as court evidence, relevant materials, the length of storage time, or destruction of irrelevant intercepted materials.[142] Also, only half of them required permission by a competent judicial authority and time limitation; only three of them included remedy against illegitimate access; and the State Intelligence Law was the only legislation that included an oversight mechanism.[143]

c) **Lack of legal certainty:** Furthermore, each of the legislations gives the authority for communications interception for different state agencies, and also has different procedures. There is no unity between the laws, thereby resulting in a lack of legal certainty in the practice of communications interception in Indonesia.[144]

3. **Lack of legitimate aim and necessity:** Although Article 17 does not explicitly stipulate the permissible limitations, both the UN Special Rapporteur on Counter-Terrorism and the UN Special Rapporteur on

---

[140] Hadiputranto, Hadinoto & Partners, Member of Baker & McKenzie International, *Legal Updates - Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, Global Business Guide Indonesia*, 8 November 2016, http://www.gbgindonesia.com/en/main/legal_updates/amendment_to_law_no_11_of_2008_on_electronic_information_and_transactions.php.

[141] Law No. 8 of 1981 on the Criminal Procedural Code (KUHAP); Law No. 5 of 1997 on Psychotropic (Psychotropic Law); Law No. 31 of 1999 on the Eradication of the Crime of Corruption (Anti-Corruption Law); Law No. 36 of 1999 on Telecommunications (Telecommunications Law); Law No. 30 of 2002 on the Commission for the Eradication of Corruption (Anti-Corruption Commission Law); Law No. 15 of 2003 on the Eradication of the Crime of Terrorism (Anti‑Terror Law); Law No.21 of 2007 on the Eradication of the Crime of Trafficking in Persons (Anti-Trafficking Law); Law No. 35 of 2009 on Narcotics (Narcotics Law); Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering (Money Laundering Law); Law No. 17 of 2011 on State Intelligence (State Intelligence Law); Law No. 18 of 2011 on the Judicial Commission (Judicial Commission Law); Law No. 19 of 2016 on the Amendment of Law No. 11 of 2008 on Electronic and Transaction (EIT Law).

[142] Wahyudi Djafar, Miftah Fadhli, *Surveillance and Human Rights: Recommendations on Integrating Human Rights Standards in the Formulation of Surveillance Policies in Indonesia*, Institute for Policy Research and Advocacy (ELSAM) Privacy International, 2016, p.20-21.

[143] Wahyudi Djafar, Bernhard Ruben Fritz Sumingar, Blandina Lintang Setianti, *Legal Reform of Interception of Communications: An initiative to establish an interception of communications law from human rights perspective*, Institute for Policy Research and Advocacy (ELSAM) Privacy International, 2016, p.34.

[144] *Id*., p. 38-39.

Freedom of Expression have stated the limitations under Article 19 — the protection of national security or of public order, or of public health or morals — are equally applicable to Article 17.[145] Accordingly, the restriction on the right to privacy is only permissible for the purpose of protecting national security and law enforcement.[146]

However, the Indonesian government, MoCI, and the National Police of Indonesia have often implemented online surveillance in political contexts. Whereas the measures were based on criminal law or ITE Law, and touted as "maintaining security," they actually aimed to remove critical content towards the president and the government, silence negative public expression, and engage in pro-government counter-narratives.[147] Such restrictions not only lack legitimate aim, but also cannot ever be said to be appropriate, necessary, or proportionate considering that surveillance has a profound chilling effect on freedom of expression, association, and movement and might also lead to miscarriages of justice, violations of due process and wrongful arrests.

a) In October 2018, MoCI created a "war room" that employed 70 engineers to monitor social media platforms in real-time, in preparation for the 2019 election.[148] After the election, it developed as a hub for "combating fake news," where a hundred staff trawl through the net to identify and ban rumours, cooperating with the Indonesian National Police to identify the creators and disseminators.[149]
b) In June 2019, after the Jakarta riot which was followed by the government's partial internet shutdown, Rickynaldo Chairul, head of the cybercrime unit of the Indonesian National Police reported

[145] A/HRC/13/37. 28 Dec. 2009, at para. 11.

[146] Wahyudi Djafar, Bernhard Ruben Fritz Sumingar, Blandina Lintang Setianti, *Legal Reform of Interception of Communications: An initiative to establish an interception of communications law from human rights perspective*, Institute for Policy Research and Advocacy (ELSAM) Privacy International, 2016, p.19.

[147] KontraS, SAFEnet, *Indonesia Submission for Universal Periodic Review of the United Nations Humans Right Council (Fourth Cycle) 41th Session - Right to Dissent*, at paras. 36-40; Freedom House, *Freedom in the World 2023: Indonesia*, at D4, https://freedomhouse.org/country/indonesia/freedom-world/2023; Rizki Fachriansyah, *Police telegram urges control over protests against controversial jobs bill*, The Jakarta Post, 5 Oct. 2020, https://www.thejakartapost.com/news/2020/10/05/police-telegram-urges-control-over-protests-against-controversial-jobs-bill.html.

[148] Tassia Sipahutara and Karlis Salna, *Inside the Government-Run War Room Fighting Indonesian Fake News,* Bloomberg, 24 Oct. 2018, https://www.bloomberg.com/news/articles/2018-10-24/inside-the-government-run-war-room-fighting-indonesian-fake-news.

[149] Medha Basu and Shirley Tay, *Inside Indonesia's Fake News 'War Room'*, GovInsider, 24 Aug. 2020, https://govinsider.asia/intl-en/article/inside-indonesias-fake-news-war-room-kominfo-johnny-plate.

that the police decided to carry out cyber patrols on WhatsApp chat groups, to combat hoaxes.[150]

c) In February 2021, the National Police launched a Virtual Police program to monitor social media and chat apps for hoaxes and incitement, with a circular letter No. SE/2/11/2021 concerning Awareness of Ethical Culture to Create Clean, Healthy, and Productive Indonesian Digital Space. The police chief of the public relations division, Senior Commission Ahmad Ramadhan confirmed that the contents on the Whatsapp messenger app will be monitored once there is a report from the public, and that Whatsapp is not the only platform the virtual police can monitor, noting that "the virtual police warn accounts whatever the platform is."[151] Since the establishment of virtual police, at least 476 accounts have received a warning for allegedly containing hate speech, which were, based on KontraS's monitoring, mostly people who actively criticize the government,[152] including one who made a comment directed against the president's son.[153]

4. **Government's access to personal data held by private companies:** Personal data held by private companies can easily become the subject of state surveillance. In November 2020, MoCI issued MR 5/2020, which requires all Private Electronic System Operators (Private ESOs) to register with MoCI before providing their services in Indonesia and to provide MoCI with information on the location of data management. After the enactment, 48 applicants and platforms including Yahoo and PayPal were blocked when they failed to comply with the registration requirement,[154] raising concerns about the subordination of Private ESOs to the government.

   In addition, MR 5/2020 requires Private ESOs to guarantee direct access to their electronic systems and users' personal data when requested for

[150] SCMP, *Indonesia's listening in on private internet chat groups. WhatsApp with that?*, Business Insider India, 24 Jun. 2019, https://www.businessinsider.in/whatsapp-privacy-and-law-in-indonesia/articleshow/69921818.cms.

[151] Laila Afifa, *Indonesian Police Monitor Hate Speech on WhatsApp Groups,* TEMPO.CO, 13 Mar. 2021, https://en.tempo.co/read/1441817/indonesian-police-monitor-hate-speech-on-whatsapp-groups.

[152] KontraS, SAFEnet, *Indonesia Submission for Universal Periodic Review of the United Nations Humans Right Council (Fourth Cycle) 41th Session - Right to Dissent*, at paras. 38-40.

[153] Forum Asia, *January to March 2021 - Repressive Laws Summary*, 2021, p.8, https://hrlaw.forum-asia.org/wp-content/uploads/2021/07/Q1-Repressive-laws-summary-1.pdf; Coconuts Jakarta, *'Virtual Police' nab netizen over criticism of President Jokowi's son*, 16 Apr. 2021, https://coconuts.co/jakarta/news/virtual-police-nabs-netizen-over-criticism-of-president-jokowis-son/.

[154] Gayatri Suroyo, *Indonesia blocks Yahoo, Paypal, gaming websites over licence breaches,* Reuters, 2 Aug. 2022, https://www.reuters.com/technology/indonesia-blocks-yahoo-paypal-gaming-websites-over-licence-breaches-2022-07-30/.

monitoring and law enforcement purposes. The access must be provided by no later than five calendar days upon the request by MoCI and/or the law enforcement authorities, which implies the difficulty for Private ESOs to investigate and decide whether the request is lawful or not. Governmental Regulation No. 71 of 2019 on Organization of Electronic Systems and Transactions also states that the data related to government administration, defense, and security are subject to data localization requirements.[155]

V. **Chilling Effects on Journalists and News Media**: According to "the former head of the Indonesian Press Council, the late Professor Azyumardi Azra…the EIT law [has] led journalists to practice 'self-censorship'" and the constant threat of being imprisoned or criminally penalized under the EIT essentially "criminalizes" their work[156] Journalists and civilians explained that the EIT laws allow the GoI to simply remove content they don't approve of.[157] Because of this, many Indonesians are afraid to speak out against the GoI.[158] Professor Azra claimed that, "[i]f you criticise certain… high official[s]"[159] you will often be reported to the police, and actions like this leads to restrictions on freedom of speech and democracy. One Indonesian editor, "'worries' her newsroom will be targeted by EIT Law and that it would jeopardise their public credibility and formal media accreditation. Consequently, she did not publish stories unless fully verified. [Another]...editor explained how one of their stories, which was critical of police, was digitally stamped as a hoax by police and circulated on social media to discredit the story."[160] Many Indonesia news outlets experience anonymous hacking after publicizing stories that criticize the government.[161] Journalists, activists, and news outlets are also at constant risk of "online harassment, prosecutions, and technical attacks" which further deters "free expression and information sharing"[162] and self-censorship.

VI. Conclusion and Recommendations

A. Persecution of Speakers: Conclusions and Recommendations

[155] CNN Indonesia, *PP PSTE: Mandatory Registration List & Government Right to Disconnect,* 28 Oct. 2019, https://www.cnnindonesia.com/teknologi/20191028102006-185-443409/pp-pste-wajib-daftar-aplikasi-hak-pemerintah-putus-akses.
[156] Andrea Carson & Andrew Gibbons, *The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore*, 24 Journalism Studies 14, 3 May 2023, https://www.tandfonline.com/doi/full/10.1080/1461670X.2023.2192299.
[157] *Id*.
[158] *Id*.
[159] *Id*.
[160] *Id*.
[161] *Id*.
[162] *Id*.

1. **Persecution of defamation:** Given the ongoing criminalization of defamation, this submission is troubled by the GoI's failure to address its arbitrary persecution of citizens on the basis of defamation, and its extreme response under the criminal code. The GoI should consider the following measures:
    a) The GoI should repeal criminal defamation laws and the laws criminalizing criticism of the State, State institutions, and officials. Criminalization of speech (in all cases other than the most egregious cases of violence and hatred) is always disproportionate, creates a chilling effect upon journalism, and damages democratic discourse and public participation.[163]
    b) The GoI should repeal criminal defamation laws which have stronger penalization for online defamation than offline defamation.

2. **Persecution for "fake news":** Given the ongoing criminalization of statements claimed by the GoI to be "fake news," this submission is troubled by the GoI's failure to address its arbitrary persecution of citizens of disseminating "fake news," and its unfounded claim that the spread of what they claim to be "fake news" will "escalate ongoing violence"[164] in Papua, as well as their use of the EIT Laws to prosecute "fake news" in addition to the Penal Code. The GoI is further imposing criminal penalties on journalists, activists, and civilians for spreading information the government claims to be "fake news." The GoI should consider the following measures:
    a) Abolish general prohibitions on the dissemination of information based on vague and ambiguous ideas, such as "false" or "fake" news, which are incompatible with international standards for restricting the freedom of expression.[165]
    b) Repeal criminal laws regarding the dissemination of "fake news" and only utilize criminal law in the most exceptional cases in which "fake news" is used to incite violence, hatred or discrimination.[166]
    c) Promote digital literacy as a part of the national school curriculum and engage all parts of the citizenry in order to combat disinformation and build resiliency against it.[167]

[163] A/HRC/50/29, 20 Apr. 2022.
[164] CCPR/C/IDN/2, Distr. 27 May 2022.
[165] A/HRC/47/25, 13 Apr. 2021.
[166] *Id.*
[167] *Id*.

3. **Persecution of dissident voices under the pretexts of "incitement of enmity," "hate speech," and "treason":** Given the ongoing persecution of dissident voices under the pretexts of "incitement of enmity," "hate speech," and "treason," this submission is troubled by the GoI's arbitrary persecution of citizens using the EIT Laws to supplement the Penal Code in criminalizing dissident voices for speech that the GoI disapproves of or which challenges the GoI or its representatives.[168] The GoI should consider the following measures:
    a) Review existing law to make sure that its legislation on "hate speech" meets the requirements for legality, necessity, and proportionality, and legitimacy.[169]
    b) Repeal the criminalization of "hate speech," other than in its most egregious forms, and refrain from using "hate speech" law to attack political enemies, non-believers, dissenters and critics.
    c) Avoid demanding internet intermediaries to take actions that are in opposition to the freedom of expression and opinion as found in the ICCPR.
    d) "Actively consider and deploy good governance measures, including those recommended in UNHRC resolution 16/18 and the Rabat Plan of Action, to tackle hate speech with the aim of reducing the perceived need for bans on expression."[170]
    e) Strengthen independent judicial mechanisms to ensure individuals accused of "hate speech" have access to adequate justice.[171]

4. **Persecution of those identifying as LGBTQ+**: While the second periodic report submitted by Indonesia discusses the freedom of expression regarding LGBTQ+-focused content, this submission is concerned with the continued persecution of LGBTQ+ individuals and the criminalization of disseminating LGBTQ+ content.[172] The GoI should consider the following measures:
    a) Revise criminal laws to remove offenses relating to consensual same-sex conduct and other offenses used to arrest and punish persons on the basis of their sexual orientation and/or gender identity or expression; ordering an immediate moratorium on

[168] CCPR/C/IDN/2, Dist. 27 May 2022.
[169] A/74/486, 9 Oct. 2019.
[170] *Id*. at 22.
[171] *Id*.
[172] CCPR/C/IDN/2, Distr. 27 May 2022.

related prosecution and expunging the criminal records of persons priorly convicted of such offenses.[173]

b) Repeal/revise the EIT Laws so as not to target and criminalize LGBTQ+ content and those who create it.

5. **Persecution of religious discourse:** While the second periodic report discusses freedom of religion, the GoI fails to fulfill this value by continuing to criminalize people under blasphemy laws for online statements in opposition to *Pansacila*.[174] The GoI should consider the following measures:
    a) Repeal any criminal law provisions and criminal penalties that penalize blasphemy as they prevent persons belonging to religious or belief minorities from fully enjoying their freedom of religion or belief.[175]
    b) Avoid applying blasphemy laws in a discriminatory manner to target religious and minority groups.[176]
    c) Promote respect for religious and cultural diversity, as well as intra- and inter-faith dialogue.[177]

6. **Persecution of users on social media and the Internet:** Given the ongoing criminalization of freedom of expression and opinion online, this submission is troubled by the GoI's weak statements of support for the freedoms of opinion and expression in the second periodic report. We are also concerned by the chilling effect of criminalization of opinion and expression on social media and the Internet.[178] The GoI should consider the following measures:
    a) Repeal any law that criminalizes or unduly restricts online expression.[179]
    b) Develop and implement national action plans to advance the freedom, independence, and pluralism of the media, and set up protection mechanisms for the safety of journalists.[180]

[173] A/HRC/29/23, 4 May 2015.
[174] CCPR/C/IDN/2, Distr. 27 May 2022.
[175] Heiner Bielefeldt, UN Special Rapporteur on Freedom of Religion or Belief.
[176] Karuna Nundy, *On Religious Freedom and Discontent: Report on International Standards and Blasphemy Laws,* International Bar Association Human Rights Institute, May 2023, https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2023/04/Blasphemy-Laws-report-2023.pdf.
[177] *Id*.
[178] CCPR/C/IDN/2, Distr. 27 May 2022.
[179] A/HRC/38/35, 6 Apr. 2018.
[180] A/HRC/50/29, 20 Apr. 2022.

c) Revise existing laws related to freedom of expression online to ensure they align with international standards[181], especially Articles 27A, 28(3), 45(4), 45A(3) of the newly amended EIT Law.

B. Suppression of Speech: Conclusions and Recommendations

1. **Suppression on social media and the Internet:** Given the ongoing suppression of the freedom of expression and opinion on social media and the Internet, this submission is troubled by the GoI's weak statements of support for the freedoms of opinion and expression in the second periodic report, and is concerned by the blocking, shutdowns, and removal of websites, social media posts, and other online material that the GoI deems "negative content."[182] The GoI should consider the following measures:
    a) Refrain from imposing disproportionate sanctions on Internet intermediaries when "negative content" is found on their services.[183]
    b) Refrain from allowing the MoCI to become the arbiter of lawful expression, rather than judicial authorities, through the blocking of websites and other online material the GoI views as "negative content."[184]

2. **Suppression through lack of anonymity of SIM cards:** Given ongoing suppression of the freedom of opinion and expression online through a lack of anonymity of SIM cards, this submission is troubled by the GoI's failure to address the importance of anonymity on the right to privacy, expression, and opinion on the Internet.[185] The GoI should consider the following measures:
    a) Adopt policies of non-restriction regarding anonymity and only adopt restrictions on a case-specific basis rather than through a broad regulation requiring registration of citizens' national identity numbers to their SIM cards.[186]
    b) Avoid restricting or banning anonymity-protecting technology. Legislation and regulations regarding journalists and civil society organizations should also include provisions enabling access to use technologies to secure their communications.[187]

[181] *Id*.
[182] CCPR/C/IDN/2, Distr. 27 May 2022.
[183] *Id*.
[184] Id.
[185] CCPR/C/IDN/2, Distr. 27 May 2022.
[186] A/HRC/29/32, 22 May 2015.
[187] *Id*.

C. Failure to Protect Online Safety: Conclusions and Recommendations

1. **Online gender-based violence:** This submission takes note that the international community is still developing principles and norms regarding prevention of OGBV. It also recognizes the GoI's efforts to address OGBV through the 2021-2025 National Human Rights Action Plan.[188] However, the high rates of OGBV in Indonesia and the effects they have on women and girls' freedom of expression and access to information are disconcerting. In line with international developments on this issue, we recommend the following measures:
    a) Formally recognize that OGBV is a human rights violation, and incorporate anti-OGBV measures into relevant action plans addressing violence against women and domestic violence.[189]
    b) Enact laws and measures to prohibit emerging forms of OGBV in accordance with the principle of due diligence and in line with the parameters set out in Article 19 and relevant comments and resolutions.[190]
    c) Increase access to justice services for victims by continuously reviewing the Guidelines No. 1/2021 concerning Access to Justice for Women and Children in Handling Criminal Cases.[191]
    d) Increase the capacity of relevant institutions/ministries to handle increasing instances of OGBV.[192]
    e) Develop cooperation with private internet intermediaries, human rights institutions, and CSOs to facilitate a holistic approach to OGBV in accordance with international human rights obligations.[193]

2. **Digital attacks:** Given alarming rates of data breaches, hacking events, and digital attacks against private individuals and public figures alike, this submission is troubled by the GoI's failure to protect online security. Digital attacks are concerning as they stifle public discourse and intimidate internet users. The GoI should consider the following measures:

[188] CCPR/C/IDN/2, Distr. 27 May 2022, at para. 7.
[189] The GoI in their report does not specifically address online gender-based violence within their response to para. 8 of the LOIPR; *see* CCPR/C/IDN/2, Distr. 27 May 2022.
[190] A/HRC/38/47, 18 Jun. 2018, para. 95.
[191] CCPR/C/IDN/2, Distr. 27 May 2022, para. 55.
[192] The GoI in their report confirms that among increasing instances of gender-based violence, relevant ministries/institutions have only been able to follow up on half of the 190 discrimination reports received between 2018-2021; *see id.* at para. 64.
[193] *Id.* at para. 109.

a) Ensure privacy protection and transparency in the GoI's collection and use of data by pushing forward Laws on Data Protection.[194]
b) Designate state-owned data centers as a vital state object and invest in proper digital and physical infrastructure to enhance security.[195]
c) Unequivocally condemn the use of digital attacks by and against political candidates and their supporters.
d) Ensure that all digital attacks are investigated promptly and impartially, and increase specialized capacity to address digital attacks against journalists.[196]

3. **Spread of disinformation:** This submission is concerned by the spread of disinformation in Indonesia and specifically the GoI's use of government funds to encourage and disseminate information. Additionally, provisions in the EIT Law are applied inconsistently, posing a risk to the free flow of information. The GoI must balance its international human rights obligations with the need to combat the spread of disinformation. We recommend the following measures:
    a) Clarify formulations for identifying and addressing disinformation and increase consistency in the application of relevant laws.[197]
    b) Prohibit the use of government funds for disinformation campaigns.
    c) Increase public media literacy and awareness of buzzers and propaganda.
    d) Focus state regulation of social media on enforcing transparency, due process rights for users, due diligence on human rights by companies, and ensuring that the independence of regulatory bodies are clearly defined, guaranteed and limited by law.[198]
    e) Restore public trust in the integrity of the information order by increasing the availability of diverse and reliable information on the internet through enhanced protections for freedom of expression.
    f) Avoid criminalizing of "fake news", which will infringe upon other international human rights obligations.

---

[194] Submission for Universal Periodic Review 41st session - Indonesia (Fourth Cycle), J*oint stakeholder contribution: Freedom of expression, freedom of religion and belief, and digital rights,* Association of Progressive Communications (APC), EngageMedia, and SAFEnet, at 9.
[195] *Id.*
[196] A/HRC/50/29, 20 Apr. 2022, at paras. 114-17.
[197] Submission for Universal Periodic Review of the United Nations Human Rights Council (Fourth Cycle) 41st Session, Indonesia, *Right to Dissent,* The Commission for the Disappeared and Victims of Violence (KontraS) and SAFEnet, at 5.
[198] A/HRC/47/25, 13 Apr. 2021, at para. 91.

D. Impairment of Access to the Internet: Conclusions and Recommendations

1. **Government restrictions on content:** This submission is concerned with the GoI's restrictions on online content. The GoI has repeatedly utilized overly broad laws and regulations to arbitrarily block access to certain websites and platforms, stifling the free flow of information. We recommend the following measures:
    a) Address overly-broad defamation, hate speech, and blasphemy laws and issue clear guidelines regarding what content will be restricted and why.
    b) Avoid restricting access to entire websites and platforms by blocking only specific content that violates established guidelines.
    c) Encourage the development of technology, including anonymity tools such as VPNs, to protect the rights and security of internet users.
    d) Refrain from allowing the MoCI to become the arbiter of lawful expression, rather than judicial authorities, through the blocking of websites and other online material the GoI views as "negative content."[199]
    e) Make publicly available the reasons why content is blocked through existing MoCI press briefings listing targeted content.
    f) Repeal laws that allow blocking of websites for administrative violations such as prior registration, e.g., Article 40 of EIT Law.

2. **State-authorized connectivity disruptions:** This submission is concerned with the GoI's use of state-authorized connectivity disruptions. These disruptions are particularly concerning in the context of protests and religious activities, as they stifle dissent and disrupt the free flow of information. We recommend the following measures:
    a) Avoid using state-led connectivity disruptions except in the most serious of situations in accordance with international law.
    b) Revise laws addressing hoaxes or "fake news" to prevent unnecessary bandwidth throttling and full shutdowns, specifically under Article 40 of EIT Law.
    c) Reaffirm the principle recognized in the overturned 2020 Jakarta State Administrative Court decision, which held that the EIT Law should only be used to target specific "unlawful" content, not to terminate access entirely.

[199] A/HRC/38/35, 6 Apr. 2018.

d) Refrain from utilizing shutdowns in instances of lawful dissent, contentious religious and political discourse, and protest.
e) Encourage independent investigation into and criticism of the 2019 Papuan and West Papuan shutdowns by protecting and empowering journalists in the region.

E. State Surveillance and Violation of the Right to Privacy: Conclusion and Recommendations

1. **Lack of legality and legal certainty:** This submission is concerned with the GoI's lack of legality and legal certainty when it comes to state surveillance and privacy legislation. We recommend the following measures:
    a) Adopt communications surveillance legislation that specifies minimum safeguards against intrusive surveillance, such as the subject, time limit, precaution, or supervision in the use of surveillance power within statutes regarding communication interception.
    b) Modify existing legislation to clearly define the scope, procedure, and manner of interception, and to include oversight measures such as court warrant requirements.
    c) Provide victims of violations of the right to privacy with access to adequate remedies.

2. **Government's access to personal data held by private companies:** This submission is concerned with the GoI's unrestricted access to personal data held by private companies. We recommend the following measures:
    a) Modify MR 5/2020 to eliminate registration requirements on ESOs.
    b) Modify MR 5/2020 to subject the government's data request to court warrant requirements.