Indonesia

Key Developments: June 2016 – May 2017

- Internet access and speeds increased in 2017 (see Key Access Indicators).

- Blocks on web content affected gay dating apps and websites with information related to the West Papua region (see Blocking and Filtering).

- Social media users were jailed for defamation, while amendments to the problematic ITE law could make the situation worse (see Legal Environment and Prosecutions for Online Content).

- Religious activists intimidated and assaulted people they perceived to be challenging Islam online (see Intimidation and Violence).

- At least two civil society websites were disabled for weeks due to cyberattacks (see Technical Attacks).
Introduction

Internet freedom declined in 2017, even as access improved. The government introduced new measures to block content and punish online defamation, but failed to stem rampant manipulation and intimidation along ethnic and religious lines.

With more than 100 million internet users, Indonesia could become the fourth largest online market by 2020, according to a 2016 study by Google and Temasek. The internet has challenged the dominant role of traditional media, and has gradually been accepted as a reliable source of information. But among the estimated 43,000 digital news outlets operating in 2017, many circulated content of questionable standards. Some actors took advantage of the popularity of the internet and social media to publish an unprecedented quantity of fake reports, many disguised to look like legitimate news. Many of them sought to discredit ethnic and religious minorities.

The impact was alarming. The Christian governor of Jakarta, an ally of President Joko Widodo known as Ahok, lost his bid for reelection and was subsequently imprisoned for blasphemy after a viral video that mischaracterized his comments about Islam launched massive protests. In what observers described as “the Ahok effect,” religious activists traced people who questioned tenets of Islam or reputed scholars on social media, and forced them to publish written apologies, sometimes violently.

But measures that were introduced to curb these negative effects only undermined internet freedom further. A problematic Law on Information and Electronic Transactions (ITE) was amended to empower officials to directly block prohibited electronic information, reducing oversight over a framework that already lacks transparency. Rather than reforming the law’s defamation clause so that it fit international standards, it was expanded. Several individuals were placed in pretrial detention for lengthy periods as punishment for their online speech. A businessman was detained for privately asking a Facebook Messenger correspondent to repay a debt in 2017. In two other cases, women were held for several weeks each after being accused of defamation, and were only released after a public outcry.

Obstacles to Access

While smartphone use is increasing, the total internet penetration in Indonesia remained under 30 percent. This low access rate is mainly due to the geographic conditions of the country, which consists of 17,000 islands and a population that is concentrated in the major islands, namely Java and Sumatra.

Availability and Ease of Access

Although internet penetration is steadily increasing, connectivity remains highly concentrated in the western part of the archipelago, particularly on the island of Java. This trend continued in 2017, despite the fact that infrastructure development in the underserved eastern part of the country is an official priority.

Rising internet penetration is due to rapid growth in the number of mobile subscriptions. The low

---

number of fixed-line subscribers (see Key Access Indicators) is due to the lack of infrastructure, which limits coverage and keeps the price of monthly subscriptions high.

<table>
<thead>
<tr>
<th>Key Access Indicators</th>
<th>2016</th>
<th>2015</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet penetration (ITU)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>25.4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>22.0%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>12.3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mobile penetration (ITU)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>149%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>132%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>102%</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Average connection speeds (Akamai)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017(Q1)</td>
<td>7.2 Mbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016(Q1)</td>
<td>4.5 Mbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Most users access the internet through mobile phones (95 percent), while only 13 percent rely on personal computers, according to the Indonesia Association for Internet Providers (APJII). It’s common for mobile internet users to own multiple SIM cards and devices, as many shop around for better signal quality and lower prices. Affordable devices are also available; phones with Android operating systems start at US$30.

However, affordable prepaid mobile packages are not as readily available in underserved areas of the country. Mobile internet users in Papua, Nusa Tenggara, and the Moluccan islands pay more for the same amount of data than those in Java, due to market domination by Telkomsel. In April 2017, Telkomsel’s website was hacked by an unknown group calling on the company to lower their data prices. The attack received a positive response on social media, with many users expressing sympathy for the hackers’ demands. The company had already been forced to review prices for users in Eastern Indonesia following an online petition in 2015. The MCI also committed to allocating Universal Service Obligation Funds to subsidize internet access in the eastern part of the country.

Uneven costs exacerbate a significant digital divide. Over 70 percent of internet users are based in urban areas, according to official 2015 statistics. In 2016, the APJII reported that the combined number of internet users in the eastern provinces of Papua and Maluku amounted to 3 million, just 2.5 percent of the 133 million internet users nationwide. During the same period, 86 million users ac-

---

9 Central Statistic Bureau, 2015, Telecommunication Statistic in Indonesia 2015, 29.
Accessed the internet from Java, a 72 percent increase since 2014, according to APJII.\textsuperscript{11} In urban areas, most shops and cafes, public libraries, and schools provide free Wi-Fi.

According to a 2016 survey by APJII, there are 63 million of women online, an increase from 44 million reported in the same survey carried out in 2014. However, women still account for less than 50 percent of total users. Reports from the Central Statistic Bureau have consistently shown slightly fewer women accessing the internet than men.\textsuperscript{12}

### Restrictions on Connectivity

PT Telekomunikasi Indonesia Tbk, a partly state-owned company known as Telkom Indonesia, dominates the telecommunications market and is a major player in infrastructure development. Internet infrastructure in Indonesia is otherwise decentralized, with several connections to the international internet.\textsuperscript{13}

Most base transceiver stations (BTS) and other telecommunications infrastructure are built by private providers. In their 2017 annual report, Telkom Indonesia’s Telkomsel reported having 129,033 BTS across the country in 2016.\textsuperscript{14} Indosat reported 54,212 BTS, up from 40,756 in 2015.\textsuperscript{15} The government has sponsored development in less commercially viable areas. In 2016, for example, 92 out of a projected 197 new BTS were established in Papua, Kalimantan, and East Nusa Tenggara.\textsuperscript{16} The MCI’s Desa Broadband Terpadu project (formerly desa bordering) provides villages with internet connections in the most remote and disadvantages areas, including border regions.\textsuperscript{17}

Since 1998, the government’s Palapa Ring Project has sought to develop seven small internet backbone “rings” to connect 33 provinces and 460 regencies.\textsuperscript{18} After years of delay due to underinvestment, in 2014 the government issued a presidential regulation redirecting Universal Service Obligation funds to support the plan.\textsuperscript{19} Telkom Indonesia connected Papua and other eastern areas with the existing broadband network through the Moluccan Ring cable system,\textsuperscript{20} and launched the Sulawesi Maluku Papua Cable System (SMPCS) in 2015, an undersea fiber-optic cable that connects 34 million people formerly served by satellite connections with limited bandwidth.\textsuperscript{21} The development

\begin{footnotesize}
\begin{itemize}
  \item 11 APJII, 2016, Profil Pengguna Internet di Indonesia 2016, \url{http://bit.ly/2n8IlOQ}. In the 2015 APJII survey, Papua, the Mollucan Islands and East Nusa Tenggara were grouped as one area with 5.9 million users.
  \item 15 See \url{http://bit.ly/2o3mYrE}.
  \item 16 ICT white book 2016, 74, accessible at \url{http://bit.ly/2rMoXsF}.
  \item 17 ICT white book 2016, 73, accessible at \url{http://bit.ly/2rMoXsF}.
  \item 18 Ministry of Communication and Information, \url{http://bit.ly/2ePS765}.
  \item 19 The regulation can be accessed through \url{http://bit.ly/2qanDIs}.
\end{itemize}
\end{footnotesize}
was further expedited in 2016 after another presidential regulation that classified it as national strategic infrastructure.22 The western and central parts of the project were launched under a public-private partnership in June 2016,23 while the Eastern part was launched in March 2017, connecting 35 regencies in Papua, East Nusa Tenggara, and the Moluccan islands.

The first internet exchange point, the Indonesia Internet Exchange, was created by APJII to allow ISPs to interconnect domestically.24 An independent internet exchange point, Open IXP, was launched in 2005,25 and starting in 2016 membership to the IXP was opened up to non-ISPs.26

**ICT Market**

Internet and mobile service is generally provided by large telecom companies, some with partial state ownership.

In 2017, out of the total 500 telecommunication service licenses issued by the MCI, 312 companies were registered with ISP licenses.27 The APJII has criticized high costs associated with obtaining an ISP license under the Law on Post and Telecommunication.28

The fixed-line market is still in an early stage of development, with less than 2 percent penetration in 2016 (see Availability and Ease of Access: Key Indicators). The lack of infrastructure requires ISPs to invest heavily in development, so only major companies are able to compete. As a result, Telkom Indonesia dominated the market in 2016.29

As the mobile market approached saturation in 2016, four providers served 90 percent of subscribers.30 Market leader Telkom Indonesia, operating as Telkomsel, reported 174 million mobile subscribers in 2016.31 Its closest rival Indosat Ooredoo reported 86 million subscribers in the same period.32 Telkomsel and Indosat Ooredoo are 51 percent and 14 percent state-owned, respectively.33

---

26 Apji, “Rilis Media APJII 20th ANNIVERSARY,” https://apjii.or.id/content/read/17/204/Rilis-Media-APJII-20th-ANNIVERSARY.
In 2013 the CEO of one ISP, IM2, was jailed for eight years for selling bandwidth under a public frequency licensed only to its parent company, thereby avoiding a private tax rate. Both the MCI and the APJII opposed the prosecution; an APJII representative estimated that 200 other ISPs were operating under the same business cooperation agreement.

Regulatory Bodies

The Directorate General of Post and Telecommunication Resources and Directorate General for Informatics Application oversee internet services under the MCI. Their mandates include regulating the allocation of frequencies for telecoms and data communications, satellite orbits, ISP licenses, and overseeing private telecom providers. The latter also has some responsibility for content regulation. In 2016, new Directorate Generals were appointed in an internal restructuring.

In 2003, a more independent regulator, the Indonesia Telecommunication Regulatory Body (BRTI), was established to oversee fair competition among telecommunications business entities, to resolve industry conflicts, and to develop standards for service quality. However, the body lacks executive power, and can only make recommendations. As a result, it fails to intervene in relevant fraud or corruption cases, and its effectiveness remains challenged. The appointment of the head of the MCI’s Directorate General Post and Telecommunication as chair raised concerns over its independence; in 2016, following the MCI restructuring, both the BRTI chair and the vice chair represent the MCI. Otherwise, the composition of the 2015-2018 BRTI is fairly balanced, with members including three government officials and six from civil society.

---

Limits on Content

More political and social content was blocked, including content about West Papua during a period that saw large local rallies supporting an independence movement, and apps serving the LGBTI (lesbian, gay, bisexual, transgender, or intersex) community. Legal amendments strengthened the government’s power to censor content. Content manipulation and fake news spiked, especially around local elections in Jakarta in 2017.

Blocking and Filtering

Online content is frequently blocked for violating laws or social norms, including political information, criticism of the majority religion, Islam, and websites serving the LGBTI community. Blocking worsened in the past year with new restrictions on gay dating apps, and unacknowledged blocks on information related to Papua and West Papua.

Several government agencies can restrict online content under the Information and Electronic Transactions Law (ITE Law), provided that limitations are in the public interest and intended to maintain public order.42 A separate statute provides a legal framework to block content considered pornographic,43 while a 2014 decree issued under the ITE law expanded official powers to allow blocking of “negative content.”44 Amendments to ITE passed in November 2016 further strengthened the legal foundation for blocking content, but failed to improve transparency, oversight, or the process for appeal. (For more on the ITE law, see Legal Environment.)45

Under Article 40 of the amended law, the MCI may now prevent access to online information directly, or order ISPs to do so.46 The MCI had announced plans in 2015 to automate and potentially centralize the blocking process, but updates regarding the new censorship system had yet to be made during the coverage period.47 Separately, in May 2017, a presidential decree established a new National Cyber and Encryption Agency, which operates under the Ministry of Politics, Law and Security.48 The agency has the authority to filter and monitor online content, adding to the list of institutions empowered to censor the internet.

Under the existing framework, the government compiles sites for ISPs to block in a database known as Trust+ or Trust Positive. Operational since 2010, Trust Positive is managed directly by the ministerial office.49 The 2014 decree issued under the ITE law specified Trust Positive as the government’s “blocking service provider.” Members of the public or website owners can file complaints to remove a website’s URL address from the database, and complaints must be resolved within 24 hours. However, while all ISPs refer to Trust Positive, each can employ different software for blocking and thus

---

42 Law No. 11/2008, Article 40.
43 Civil society and cultural groups challenged the law before the Constitutional Court in 2009 for its narrow and obscure definition of pornography and pornographic content, which includes LGBTI content and folk traditions which expose the female form, such as the Jaipongan folk dance from West Java and Papuan traditional clothes; the Court upheld the law.
45 For details of the amended law, see, http://bit.ly/2olwo1S.
49 Trust Positif, website, http://trustpositif.kominfo.go.id/.
may blacklist additional sites at their own discretion. Under Article 7 of the 2014 decree, “[members of] society can participate in providing blocking facilities” which contain “at least” sites listed in the Trust Positive database.\(^{50}\) This has increased the practice of arbitrary, inconsistent blocking, creating uncertainty for users seeking redress when content is wrongfully blocked. Four multistakeholder panels which the MCI established to respond to public outcry on these issues completed their terms in 2015 and were not renewed.\(^{51}\)

This framework makes it harder to establish what content is affected. In 2016, the MCI reported 773,097 sites blocked, up from 766,394 sites in 2015.\(^{52}\) Most involved pornographic content (767,888), gambling (3,755), fraud and illegal trade (848), and content promoting radicalism.\(^{53}\) But political content is also subject to blocking. In 2017, the Internet Monitor at the Harvard University-based Berkman Center reported that “political sites focused on criticism of the government or of Islam” were pervasively blocked.\(^{54}\) Separately, the global Open Observatory of Network Interference (OONI) and the Sinar Project, a Malaysia-based civil society organization focused on digital rights in Southeast Asia, tested website blocking in Indonesia between June 2016 and March 2017. The report found 161 sites blocked, including “a blog expressing political criticism” and “multiple sites expressing criticism towards Islam.”\(^{55}\)

Websites with information about the provinces of Papua and West Papua, where military forces have been accused of violently suppressing a Papuan independence movement, were newly blocked during the reporting period, including five in April 2017.\(^{56}\) Earlier, the news site Suara Papua became inaccessible on some connections on October 30, 2016, and was completely blocked a few days later.\(^{57}\) Suara Papua had covered human rights issues in the West Papua region, among other issues. The website was not notified of any blocking order, but in November, an official told a media rights group that “suarapapua.com was blocked upon request by “a ministry/government institution authorized to determine whether a website has violated the law.”\(^{58}\) The MCI openly reported new blocks on 11 websites which contained support for religious radicalism and anti-ethnic sentiment in November, but Suara Papua was not among them.\(^{59}\) Five of those websites were later unblocked after they revised content.\(^{60}\) Suara Papua became available again later in the coverage period, but was separately subject to a disabling cyberattack in 2017 (see Technical Attacks).

One of the most common pretexts for blocking online information is pornography, and several information-sharing platforms have been entirely blocked by one or more ISPs based on explicit content shared by a small subset of users. For example, the Singapore-based streaming app Bigo Live was blocked in December 2016 after users broadcast video containing nudity.\(^{51}\) The app became available again one month later after the company agreed to remove content in cooperation

---


\(^{51}\) For the decree which contains members of the four panels, see [http://bit.ly/2shC3dd](http://bit.ly/2shC3dd).


\(^{54}\) [https://thenetmonitor.org/research/2017-global-internet-censorship/idn](https://thenetmonitor.org/research/2017-global-internet-censorship/idn).


\(^{59}\) “Kami Tidak Pernah Mendapat Pemberitahuan soal Pemblokiran.”


with the MCI (see Content Removal). Reddit and Vimeo were blocked by different service providers for the same reason in 2016, and remained partially affected during the reporting period. In another case, the MCI did not intervene when Telkom blocked Netflix in early 2016, declaring that the company was operating illegally without proper licensing, and that it was exposing internet users to violence and pornographic scenes prohibited by law. Netflix remained inaccessible on Telkomsel connections pending an agreement to partner with Telkom subsidiaries.

LGBTI-related content continued to be subject to blocking in the past year. In September 2016, the MCI ordered service providers to block social networking apps serving the LGBTI community, including Grindr, Blued, and BoyAhoy. MCI spokesperson Noor Iza said the apps would be blocked for promoting “sexual deviance,” and as many as 80 gay websites were being considered for a possible ban in late 2016.

After a proliferation of manipulated content online in 2016 and 2017 (see Media, Diversity, and Content Manipulation), the government implemented new blocks intended to combat fake news, hoaxes, and hate speech. The MCI reported blocking sites they characterized as designed to discredit minority ethnicities, races, or religions. Separately, a police cybercrime unit reported having blocked 300 social media accounts and websites for disseminating fake news; the procedure involved was not specified. While the threat to minorities was real, police were also cited using the term “hate speech” to include hostile expression against public officials such as the president and the national police chief.

Content Removal

The MCI requires companies providing “over-the-top” (OTT) services to remove negative content posted by users. That includes social media and communication apps, as well as other providers of apps that rely on an internet connection, though implementation is mixed. In a new development, the amended ITE law introduced a “right to be forgotten.”

Platforms that do not remove content risk being blocked entirely. In one example from the period of coverage, the video-streaming service Bigo Live was blocked for a month until its owners agreed to open a branch in Indonesia and recruit Indonesian staff to monitor and remove content that is against Indonesian regulations (see Blocking and Filtering).

Other platforms were threatened with similar outcomes as content manipulation targeting minority groups spiked in 2017. At an event promoting religious guidelines on social media use for Muslims

---

64 See http://bit.ly/2w8074
69 The agreement was cited in a statement made by Noor Iza, acting chief of the MCI public relations bureau. See, Vivanews.com http://bit.ly/2sLek6f
issued by the Ulema Council in June, the MCI reminded OTT service providers, particularly Facebook, to remove ‘negative content’ online or face closure.70

An MCI circular letter issued in March 2016 had warned OTT providers to filter content (point 5.5.4) and censor information transmitted on their services in accordance with existing laws and regulations (point 5.5.3).71 The warning targeted providers of games, videos, music, animation, images, and other forms of content available via streaming and download, and said such providers must establish domestic business entities and allow legal interception for law enforcement purposes.72 Officials said further regulations would follow, but none had been issued in mid-2017.73

The growing pressure on companies to police content has resulted in censorship of political and social content, although the extent is difficult to assess. In one documented example of content affected in February 2016, the LINE messaging app removed emojis depicting LGBTI themes from its Indonesian store at the MCI’s request.74

Amendments to the ITE law passed in November 2017 also have implications for content removal by intermediaries. Article 26 established a “right to be forgotten” for Indonesian citizens along similar lines to a 2014 decision by the Court of Justice of the European Union. Electronic system providers will be required to delete irrelevant electronic information on request, but only when supported by a court order. Further details were expected in subsequent regulations.75 In the EU, content in the public interest is exempt, but critics of the system say companies are more likely to take down content than they are to dispute removal requests that could undermine free expression.76

Other content removal requests are periodically documented. Google reported 214 items requested for removal between June and December 2016, a significant increase from the 76 items reported between January and June 2016, and the 11 reported between June and December 2015.77 The company complied in 25% of cases.

**Media, Diversity, and Content Manipulation**

Fake news and content manipulation had a dramatic effect on the online information environment in 2017.

Media freedom has been improving since the beginning of the political transition in 1998, with far less instances of government intervention. Interference from state agencies has significantly declined.

---

However, some trends are transforming and destabilizing the online news environment. A burgeoning digital media market has introduced thousands of unfamiliar outlets with variable standards, eroding user trust in the quality of information available online. The Press Council said there were about 43,000 media outlets actively operating online in 2017.\(^{78}\)

In this environment, content manipulation reached unprecedented levels during 2016 and 2017. Anonymous and pseudonymous social media accounts have circulated rumors and blackmail threats in the past, particularly around the presidential election in 2014. The coverage period also saw a spike in derogatory content about religious and ethnic minorities. Several examples were designed to provoke distrust of Indonesia's minority ethnic Chinese population by highlighting their supposed economic advantages.

The content was often disguised to appear as a news article or manipulated to make the subject appear to be attacking Islam. While many government officials espouse conservative religious views, the content was not state sponsored, and actually served as a vehicle to challenge elected politicians.

The phenomenon was vividly illustrated during the 2017 Jakarta gubernatorial election, when protests sparked by online content contributed to the electoral loss and subsequent imprisonment of the city’s first Christian, ethnic Chinese governor, Basuki Tjahaja Purnama, also known as Ahok.\(^{79}\) In October 2016, a YouTube video which purported to document Ahok's public statements defaming Islam went viral. News reports said it had been incorrectly subtitled,\(^{80}\) but it became the basis of widespread campaigns calling for his arrest.\(^{81}\) He lost the election in April 2017 and a panel of judges sentenced him to two years in prison in May, though prosecutors had recommended probation.\(^{82}\)

Online content triggered other offline results in a trend characterized by a local advocacy group as the “Ahok effect.”\(^{83}\) Right-wing religious activists organized online to harass and even attack individual internet users who they believed had offended them in social media comments (see Intimidation and Harassment).

In an attempt to combat fake news online, the Press Council created a barcode designed to help readers identify reliable media outlets. Outlets need to register with the Council and undergo further verification before being issued with a barcode, which users could scan to view registration details. The initiative got mixed reactions from journalists.\(^{84}\) Some feared it could be used to limit unregistered journalists from obtaining information and noted that it benefitted mainstream, professional institutions, while potentially excluding competitors. As of mid-2017, 74 websites had been issued with a barcode.\(^{85}\)

Increasing concentration of media ownership across print, broadcast, and online outlets heightens the potential impact of self-censorship, and undermines the diversity of viewpoints available for consumers. The fact that some major media owners are actively involved in politics contributes to

---


\(^{82}\) Hardline groups accused the prosecutors of leniency, driving further rallies to increase pressure on the court. See [http://bbc.in/2wUky56](http://bbc.in/2wUky56)


\(^{85}\) [http://www.freedomthenganet.org](http://www.freedomthenganet.org)
increasingly partisan information landscape online. At the local level, many online news outlets have become the extension of certain political parties, hampering their credibility and increasing the possibility of retaliatory criminal charges. Journalists from the West Papua region are also more likely to self-censor and undergo economic constraints due to the ongoing conflict between the government and indigenous independence movements.\(^\text{86}\)

Online media also face unique challenges due to enforcement of the ITE Law, particularly the threat of criminal sanctions in reprisal for information posted online. While it was unclear how many journalists faced such sanctions, the rapidly expanding online news market has resulted in several defamation suits. While the Press Council often intervenes to defend registered news outlets in criminal cases, less than 10 percent of digital news outlets are registered with the council.\(^\text{87}\) This is in part because many fall short of official requirements for establishing a media company, such as a legal entity like a limited liability company, a cooperative, or a foundation.

Indonesia otherwise enjoys a thriving blogosphere. The rapid increase of a tech-savvy urban middle class, fervent users of social media and communication apps, has fueled a diversity of applications and platforms. Local blog and website-hosting services are either free or inexpensive, and social media have provided an important alternative source of information. Tools to circumvent censorship are subject to some restrictions, though many others remain accessible. In one 2017 test, three tools offering virtual private network (VPN) services or anonymous browsing were subject to blocking.\(^\text{88}\)

**Digital Activism**

With the urban middle class expanding, digital activism has become a popular form of organizing support for social and political change. Internet users collaborated to counter hoaxes and disinformation after content manipulation spiked during the reporting period (see Media, Diversity and Content Manipulation). One community group, “Forum Anti Fitnah, Hasut, dan Hoax,” registered as an association with the Ministry of Law and Human Rights in November 2016;\(^\text{89}\) its public Facebook group had nearly 41,000 members interested in verifying online content by mid-2017.\(^\text{90}\) The group combined online activities with offline outreach to increase their influence by meeting with the Chief of the National Police, among other initiatives.\(^\text{91}\)

Conservationists increasingly take advantage of online tools. In one example, digital activists have supported a local community in central Java protesting against a PT Semen Indonesia cement plant in the groundwater basin Watuputih area; President Joko Widodo subsequently commissioned a study of the plant’s environmental impact. Advocacy around the issue has been ongoing in various forms since 2010, but intensified when the hashtag #savekendeng helped bring the case to national attention.\(^\text{92}\) The hashtag reached international audiences when it was used to promote a film about

\(^{86}\) West Papuan journalists working online have described self-censoring to avoid persecution. [https://www.ifex.org/indonesia/2016/12/15/press_west_papua/](https://www.ifex.org/indonesia/2016/12/15/press_west_papua/). Ad revenues that support media operations are frequently linked to powerful interests that could undermine independence. [https://www.ifex.org/indonesia/2017/02/13/papua_press_blocks/](https://www.ifex.org/indonesia/2017/02/13/papua_press_blocks/).

\(^{87}\) Interview with Press Council member Nezar Patria, February 26, 2016.


\(^{89}\) See, [www.turnbackhoax.id](http://www.turnbackhoax.id).


the activists in 2017, particularly in Germany, where local protesters adopted it during a meeting of company shareholders in Heidelberg in May.93

Activists have also used online petitions to promote internet freedom, with some success during the reporting period. On October 2, 2016, a housewife was arrested and charged with online defamation by a local politician for a Facebook post she had written in March (see Prosecutions and Detentions for Online Activity). Using the hashtags #gara2UUITE and #saveYusniar, as well as an online petition with over 6,500 signatures, civil society groups mobilized to secure her release from pretrial detention in late November.94 A court acquitted her of all charges in April 2017.

Violations of User Rights

Prosecutions under the ITE Law continued with long detentions attracting widespread public outrage. People frequently abuse the law’s defamation provisions to pursue vendettas, confusing public and private digital space. Amendments passed during the reporting period look set to perpetuate the problem, allowing criminal defamation charges to be brought for private electronic messages with only one reader. Attacks in reprisal for religious commentary published on social media increased, and civil society websites were disabled by cyberattacks.

Legal Environment

Freedom of expression was initially protected through the stipulation of the Law on Human Rights shortly after the 1998 reformation, and strengthened through the second amendment of the constitution in 2000. The third amendment guarantees freedom of opinion.95 The constitution also includes the right to privacy and the right to obtain information and communicate freely.96 These rights are further protected by various laws and regulations.97 Indonesia also ratified the International Covenant on Civil and Political Rights (ICCPR) in 2005.98

However, amended constitution included wording to allow the state to limit rights based on political, security, morality, and religious considerations.99 This provides broad space for interpretation by policymakers.100

Provisions of the 2008 ITE law have been used repeatedly to prosecute Indonesians for online expression. The law’s penalties for criminal defamation, hate speech, and inciting violence online are

94 The petition is available online at: http://bit.ly/2fm3dJJ
95 Constitution of 1945, Article 28E(3).
96 Constitution of 1945, Articles 28F and 28G(1).
98 The ICCPR was ratified through Law No. 12/2005. However, to date the government has yet to review and reform laws to comply with the covenant’s human rights standards.
99 “In exercising his/her right and freedom, every person must submit to the restrictions stipulated in laws and regulations with the sole purpose to guarantee the recognition of and the respect for other persons’ rights and freedom and to fulfill fair demand in accordance with the considerations of morality, religious values, security, and public order in a democratic society.” Article 28 (J) of 1945 Constitution, as amended in 2000. Retrieved from http://bit.ly/2dmpF4a
100 In 2009, the constitutional court generally affirmed that human rights are subject to limits as long as the limits are provided for in the law. See http://bit.ly/2cKuKPU. Other court decisions failed to narrow the definition of the broad considerations that provide for the state to introduce restrictions. See for example, http://bit.ly/2d5vOyO and http://bit.ly/2cJLgVf.
harsh compared to those established by the penal code for similar offline offenses. In November 2016, the amended ITE Law no 19/2016 introduced several changes (see Table).

<table>
<thead>
<tr>
<th>Article</th>
<th>Changes</th>
<th>Implications</th>
</tr>
</thead>
</table>
| 27(3)   | Clarified terms that describe the way defamation offenses may be committed.  
*Distributing* was defined as sending or distributing to many people;  
*Transmitting* was defined as sending electronic information to one party through an electronic system; and  
*Causing to be accessible* was defined as all acts other than distributing and transmitting which made the electronic information accessible to another party or the public. | These changes formally expand defamation to content published unintentionally or by third parties, including “tagging” names on publicly available Facebook posts. Facebook user Dody Sutanto had already been imprisoned for content posted by one of his contacts because he was tagged by name in the post, though he did not create, publish, or even actively share it (see Prosecutions and Detentions for Online Activity). The new definition of transmission means that private chat messages can be considered defamatory, and was the basis for at least one problematic prosecution during the coverage period. The potentially exhaustive list of possible actions covered under “all acts other than distributing and transmitting” introduces further scope for abuse. |
| 27 (3)  | Reduced the penalties for online defamation from 6 to 4 years in prison and from IDR 1 billion to IDR 750 million (US$ 75,000 to 55,000). | This partial reform fell short. Advocates had called for defamation to be decriminalized, but the penalty is still comparatively high. The maximum penalty for offline defamation under the penal code is also four years, but only in specific circumstances—most sentences are less than a year and a half and financial penalties are much lower. |
| 31 (4)  | Revised interception procedures in line with an earlier decision by the Constitutional Court. | See Surveillance, Privacy and Anonymity. |
| 43(5) and (6) | Brought the standard for arrests, warrants, and pretrial detention procedures in closer compliance with the penal procedural code. | Many suspects accused of defamation online have been held for weeks in pretrial detention, which can extend up to 110 days, even though it should only be used where there is strong potential for the suspect to eliminate evidence or flee the jurisdiction. Despite this amendment, pretrial detention continued to be applied extensively in ITE cases (See Prosecutions and Detentions for Online Activities). |
| 40 (2a) and 2(b) | Strengthened the powers given to prosecutors to cut off or limit access to electronic information which relates to cybercrimes. | See Blocking and Filtering. |
| 26      | Granted individuals the “right to be forgotten.” | See Content Removal. |

---

Other laws infringe on user rights, despite legal experts’ opinions that they conflict with the constitution. The antipornography law introduced in 2008 contains a definition of pornography which can be loosely interpreted to ban art and cultural expression perceived as explicit. A 2011 State Intelligence Law introduced penalties of up to 10 years’ imprisonment and fines of over US$ 10,000 for revealing or disseminating “state secrets,” a term which is vaguely defined in the legislation. Some civil society groups challenged this law in the Constitutional Court, which rejected their petition in 2012. This framework provides authorities with a range of powers to penalize internet users, even though not all are regularly implemented.

**Prosecutions and Detentions for Online Activities**

Safenet, a regional freedom of expression network, recorded at least six new charges under the ITE Law involving online expression in 2016. As most cases are tried at the district court level, experts believe that the numbers could be higher.

Revisions to the ITE Law passed in November 2016 were designed to decrease the use of pretrial detention measures in online defamation cases. But lengthy detentions continued to be documented during the coverage period, particularly in cases involving complainants with social and political leverage:

- A housewife in Makassar, the provincial capital of South Sulawesi, was detained on October 2, 2016 based on a Facebook post which complained about an unnamed “lawmaker” and “lawyer” she said had participated in a mob attack on her parents’ house. Most reports identified her with the single name Yusniar. Sudirman Sijaya, a member of a local legislative council and lawyer, reported her to the police. Her case received widespread attention, and she was released on November 24, following pressure from netizens (see Digital Activism). A court acquitted her of all charges in April 2017 after judges found no evidence of defamation against the councilor.

- In March 2017, Baiq Nuril Makmun, a public high school teacher in Mataram, the provincial capital of West Nusa Tenggara, was reported by her former principal for transmitting an allegedly defamatory recording of a private conversation to a third party, who published the recording and caused the principal to lose his job. Nuril said she made the recording, which detailed the man’s extramarital relationship with another woman, during one of several meetings he initiated with her in his private office. The National Commission on Violence against Women described Nuril as a victim of sexual violence.

---


107 Safenet, Daftar kasus Netizen Indonesia yang terjerat UU ITE per June 2017, not accessible online.


abuse in the workplace, yet prosecutors sought a sentence of 6 months in prison and a 500 million rupiah fine. Nuril, a mother of three, was detained for two months before being released to await trial following a public outcry. The trial was ongoing in June 2017.

A number of online defamation cases have been reported in West Nusa Tenggara, according to Safenet, despite the province’s comparatively low internet penetration. In another problematic example, businessman Azril Sopandi was detained in 2017 for a private communication sent through Facebook Messenger asking the recipient to repay a debt. The recipient reported the message to police as defamatory, despite the fact that it was completely private. The case was made possible by revisions to the ITE law which allowed defamation charges based on electronic information transmitted to a single party (see Legal Environment).

One Facebook user was sentenced to prison during the coverage period because his privacy settings allowed content tagged by a third party to appear on his timeline. In August 2016, a court in Medan, the capital of North Sumatra province, sentenced Dodi Sutanto to 14 months in prison and fine of IDR 5 million (US$ 380) after a friend tagged a news report with his name. The report detailed corruption allegations against Anif Shah, a local businessman, who filed the defamation charge on grounds that people could access the report from Dodi’s Facebook page. The decision created new precedent by holding an internet user criminally liable for information that he simply received through his social media account. Rather than correcting this scope for abuse, the amended ITE law passed in November introduced broader definitions of defamation, including “causing” defamatory content to be made available to others (see Legal Environment).

### Surveillance, Privacy, and Anonymity

Although recent amendments to the ITE law included some provisions governing interception, they did not immediately transform the procedures governing surveillance, but appeared to indicate that further regulations were pending.

Although privacy is constitutionally guaranteed, no particular privacy law is stipulated; on the contrary, many regulations carry potentially risks to the privacy of personal data. In May 2017, for example, the president issued a regulation in lieu of a law which granted the finance ministry new powers to access personal financial records in tax investigations. The lack of legal protections for digital privacy is compounded by internet users’ lack of awareness on privacy in general. Online news reports, for example, frequently fail to protect the identity of victims, including minors subject to sexual abuse, and criminal suspects.

---

112 The vice mayor of Mataram was required to provide a personal guarantee before her pretrial detention was suspended. See, [http://bit.ly/2xksvyl](http://bit.ly/2xksvyl)
115 As contained in the court proceeding; prosecution note submitted and delivered before the trial by the prosecutor’s office on July 25, 2016, p33.
116 A regulation is issued “in lieu of a law” in specific circumstances to fill a gap in legislation; it must be reviewed by parliament and ultimately stipulated as legislation. This one was issued to support a national amnesty providing taxpayers with relief from overdue tax obligations. For details of the regulation, see, [http://bit.ly/2smeRZV](http://bit.ly/2smeRZV)
In May 2017, following protests against the criminal sentencing of the governor of Jakarta (see Media, Diversity and Content Manipulation), the interior ministry released the identity of an individual demonstrator to journalists. This spurred public criticism as a clear breach of individual privacy by the government agency responsible for the national database of citizens’ identification.

Article 40 of Law No. 46/1999 on Post and Telecommunications prohibits the interception of information transmitted through any form of telecommunications channel. Yet there are at least 10 laws, including the ITE law, and seven executive regulations, which allow certain government or law enforcement agencies to conduct surveillance, including electronically. The agencies include the Indonesia Corruption Commission, the National Narcotic Board, and the National Intelligence Service, among others. However, the laws do not clearly explain the scope of interception, despite the fact that the Constitutional Court issued a decision in 2010 requiring that detailed interception procedures be regulated by law. In addition, the legal framework lacks judicial or parliamentary oversight, and does not provide a remedy for possible abuse.

In November 2016, amendments to the ITE law revised provisions governing interception in compliance with that Constitutional Court decision, introducing some penalties for interception not conducted in the context of law enforcement; but indicated that further details concerning interception procedures would be passed in future regulations.

Anonymity and pseudonymous activity in cyberspace are not formally prohibited by law. Mobile phone users are technically required to register their numbers with the government by text message when they buy a phone since the MCI introduced the requirement in 2005. In the past, this obligation was widely ignored, but in 2016, the MCI issued a regulation on the registration of telecommunication service subscribers. This followed on the back of a circular letter the BRTI issued to telecommunication providers in 2015 outlining new procedures for registering prepaid and postpaid customers. Unlike the 2005 regulation, the 2016 version put stringent emphasis on the responsibility of service providers to enforce registration.

A government regulation on telecommunications operations issued in 2000 requires telecommunications providers to retain records of customer usage for at least three months. Some telecommunications companies are known to have complied with law enforcement agencies’ requests for data. In 2011, amid concerns that Blackberry’s encrypted communication network would hinder antiterrorism and anticorruption efforts, the company reportedly cooperated with the authorities in isolated incidents and agreed to establish a local server, though in Singapore, not in Indonesia.
ment introduced a regulation in 2012 requiring electronic system providers offering “public services” to build local data centers, and a draft regulation in 2014 laid out technical requirements for any entity offering “information technology-based services” to comply. In March 2016, an MCI circular letter instructed providers of over-the-top (OTT) services to establish domestic business entities and allow legal interception for law enforcement purposes (see Content Removal).

**Intimidation and Violence**

The number of cases of intimidation and violence against netizens in reprisal for information they posted online increased significantly during the coverage period of this report. Journalists with digital outlets also faced harassment and online threats, driving at least one to temporarily relocate for security reasons.

Religious expression resulted in several incidents of harassment in late 2016. Organized groups surrounded victims and pressured them to produce formal, written apologies, the contents of which were later publicized on Facebook. Others were subject to social sanctions as a result of online posts. The situation escalated in 2017, when at least one assault was reported.

In one November 2016 example, members of an Islamic youth group located 25-year-old internet user Bachtiar Prasojo in his home following remarks he posted on Facebook about Gus Mus, a high profile religious scholar. He subsequently uploaded an apology statement on Facebook. A few weeks later, Pandu Wijaya, an employee at PT Adhi Karya, a state-owned construction company, received a warning from his employer after responding to the same scholar on Twitter. In May 2017, 37-year-old internet user Wahyu Cokro Buono produced a written apology for posts about Habib Lutfi, another well-known scholar, in the wake of a visit from religious youth activists.

Recent cases indicated escalating intimidation, particularly in the aftermath of the Jakarta Gubernatorial election in May 2017, which was coloured by highly politicized religious sentiment circulating online (see Media, Diversity, and Content Manipulation). In one high profile case, a group identifying themselves as members of the Islamic Defender Front (FPI) appeared to assault a teenager who had posted comments about an exiled religious scholar on Facebook and physically restrained him until he signed an apology. In another case in May, Fiera Lovita, a doctor in North Sumatra, sought to leave her home as a result of threats and intimidation received following a Facebook post.

Violence against journalists has also increased over the last two years. The journalists’ association AJI reported that 103 journalists suffered different forms of threats between January 2016 and June 2017. Some cases during the reporting period involved digital journalists, including at least two

---


INDONESIA

who suffered intimidation from groups of religious activists while interviewing Catholics. One subsequently fled her home after receiving threats online.134

Technical Attacks

At least two websites run by civil society groups were disabled by cyberattacks during the reporting period. Government and commercial websites have been targeted in the past, but these new attempts to silence human rights advocacy marked a concerning development. It was not clear who launched the attacks or what triggered them. While the incidents had different characteristics, they took place over the same period and kept content inaccessible for some time.

*Suara Papua*, a West Papua-based news website that was blocked by the government in 2016 (see Blocking and Filtering), became inaccessible again in February 2017. Investigations revealed a massive bot attack had overwhelmed the server and disabled the website.135 The impact lasted several weeks until the site eventually migrated to another server.

Also in February, the website operated by the Southeast Asia Freedom of Expression Network (Safenet) was defaced with Japanese text. On February 27, the website’s hosting service provider notified the group that the site had been blocked for sending a large quantity of spam emails. The site remained blocked despite several attempts to restore it, ultimately requiring it to be moved to a different hosting service. Further investigation showed that its PHP database was down due to a repetitive attack.136

Akamai ranked Indonesia as the fifth-largest source of web attacks in Asia Pacific region in 2017.137 Prominent institutions such as the Central Bank of Indonesia were also targeted during the reporting period,138 along with various government websites.

Some technical attacks were launched in protest, including one against the high price of internet access set by dominant telecommunications companies Telkomsel, and Indosat. In May 2017, websites run by the Press Council and the Attorney-General were hijacked by hackers who called on them to respond to the social fragmentation and politicization of religion after the Jakarta elections (see Media, Diversity and Content Manipulation).139

135  Statement taken from Arnold Belau, 27/8/2017
136  Details chronology obtained from communications with Almascatie, Safenet volunteer, 27/8/2017
137  http://akamai.me/2nM2UJd