

Methodology and consultation process

1. This joint submission by Independent Journalist Association of Vietnam (IJAVN) and Boat People SOS (BPSOS) addresses freedom of opinion, expression, media, the press, information and internet (herein referred to as freedom of thought and expression) relating to the following recommendations made at Vietnam's 2014 UPR:

143.74 (Mexico), 143.144 (Italy), 143.145 (Lithuania), 143.146 (Japan), 143.147 (Belgium), 143.148 (Netherlands), 143.149 (Luxembourg), 143.150 (Finland), 143.151 (Denmark), 143.152 (France), 143.153 (New Zealand), 143.154 (Ireland), 143.155 (Finland), 143.156 (Australia), 143.157 (Canada), 143.158 (Brazil), 143.159 (Estonia), 143.160 (Czech Republic), 143.161 (Austria), 143.162 (Norway), 143.163 (Norway), 143.164 (Hungary), 143.165 (Poland), 143.166 (Sweden), 143.167 (Tunisia), 143.168 (Chile), 143.169 (Spain), 143.170 (Pakistan), 143.171 (Germany), 143.173 (Ireland).

2. Contributions to this joint submission came from the following sources:
 - Independent Journalist Association of Vietnam (IJAVN)
 - Research by law students in the International Human Rights Law Clinic at the American University's Washington College of Law on behalf of Freedom Now, a non-profit organization that works to free prisoners of conscience around the world through legal, political, and public relations advocacyReport on the legal framework for digital surveillance, conducted by BPSOS, with the support of the International Center for Not-for-Profit Law (ICNL)

Violations of rights to Freedom of thought and expression

3. With the introduction of internet services to Vietnam about two decades ago, online social platforms have become the "online public square" for Vietnamese people to share information, post news, and sometimes voice opinions critical of the government. With the messenger service these platforms have become an important means of for users. For them, protection of user's identity and other personal and private data is critical.
4. With recently passed laws and regulations, the government will know exactly who said what, where and when, and can use such information against any individual. The government has targeted several individuals for using the social media to support democracy and democratic rights. Of the 165 cases documented by the NOW! Campaign, as of November 2017, 15 were charged under Article 88 of the Criminal Code-- "conducting propaganda against the state", 38 under Article 87 of the Criminal Code -- "infringing the unity policy [of Vietnam]", and 5 under Article 258 of the Criminal Code --"Abusing democratic freedoms to infringe upon the interests of the State".¹ Many of these individuals were arrested multiple times, interrogated and subjected to torture and ill-treatment.

¹ The NOW! Campaign, <https://www.vietnampocs.com/analysis>

5. The case of independent journalist Truong Duy Nhat (2013)² provides evidence of working relationship between the government and technology companies targeting dissidents. The case's indictment stipulates: "On May 25, 2013, FPT Communication Joint Stock Company sent a letter coded 294/CV-VP and other documents reporting that the website truongduynhat.vn with physical address at N°. 25 Tong Phuoc Pho, Danang City, posted many articles with content defaming the Party and State leaders, and providing negative views on the country's socio-economic situation, violating provisions of law".³
6. Evidence of telecommunications companies involved in digital communications surveillance is also shown in the case of The Free Journalist Club (*Câu lạc bộ Nhà báo Tự do*) in 2012.⁴ Nguyen Van Hai, Ta Phong Tan, and Phan Thanh Hai were political bloggers and members of a civil society organization called "The Free Journalist Club". In April 2012, they were sentenced to twelve, ten, and three years of imprisonment respectively, for "conducting propaganda against the state" under Article 88 of the 1999 Penal Code. The indictment against them stated: "Through the investigation, the accused Phan Thanh Hai originally did not confess, but then sincerely confessed and asked for clemency. However, Nguyen Van Hai and Ta Phong Tan did not confess or signed the testimonies minutes, but with witness' and related persons' testimonies, records provided by [the] network service provider[s], and the examination result, it was clear that Nguyen Van Hai and Ta Phong Tan had 'conducting propaganda against the state.'"⁵
7. On June 10, 2018 mass demonstrations broke out in major cities across Vietnam to protest against the draft Cybersecurity Law and the draft Special Economic Zones Law. Hundreds of demonstrators were arrested. In Ho Chi Minh City, where at least 310 demonstrators were arrested, there were reports that plainclothes and uniformed police officers punching, kicking, beating with batons and stomped on people who were exercising their right to peaceful assembly.

William Anh Nguyen, an American citizen and a graduate of Yale University who was pursuing a Master's degree at the University of Singapore, was brutally assaulted. Video footages showed Nguyen with a bleeding head wound being dragged by plainclothes police officers through the street into custody. On June 15, 2018, the police of Ho Chi Minh City announced that

²The Supreme People's Procuracy of Vietnam, Indictment against Truong Duy Nhat, December 17, 2013, p. 1, available at <https://www.danluan.org/tin-tuc/20140225/cao-trang-vu-an-truong-duy-nhat>, last accessed February 8, 2018.

³ Freedom Now, Using Law as a Tool of Oppression: Vietnam's Crackdown on Civil and Political Rights, (Draft version, July 6, 2018)(on file with author)

⁴The People's Procuracy of Ho Chi Minh city, Indictment against Nguyen Van Hai, Phan Thanh Hai, and Ta Phong Ta, February 29, 2012, available at <https://www.danluan.org/tin-tuc/20120418/ban-cao-trang-cua-vksnd-tphcm-ve-cac-bloggers-sai-gon-dieu-cay-anhbasg-va-ta-phong>, last accessed February 8, 2018.

⁵ Freedom Now, Using Law as a Tool of Oppression: Vietnam's Crackdown on Civil and Political Rights, (Draft version, July 6, 2018)(on file with author)

they had pressed charges against Nguyen for “disturbing public order.” If found guilty, he would face up to seven years in prison.

8. At least ten demonstrators were arrested in Hanoi. Among them, two female activists, Nguyen Thuy Hanh and Cao Vinh Tinh, were kidnapped on the street by plainclothes police officers. They were taken to Trung Tu ward police station where Hanh was tortured and humiliated by a security officer who kept threatening to beat her to death; he was later identified as Khuong, a public security agent of Dong Da District.
9. After the National Assembly passed the Cybersecurity Law on June 12, mass demonstrations broke out again on June 17. The peaceful demonstrators were again brutally assaulted by the police. Many of those arrested were reportedly tortured.⁶

Following is the account by a member of a marketing team that was photographing a model at Nguyen Van Binh Books Street, Ho Chi Minh City and was caught in the police crackdown: “At the detention center I saw a fairly large number of detainees. It was a temporary, large room with corrugated fiberglass roof and a tarp underneath, set up on Huyen Tran Cong Chua Street by the side of the Tao Dan Park’s soccer field... We were in a place crawling with police officers... A woman standing near me said that she had just come out from the cathedral after Mass and was recording the arrests of protesters when the police pulled her into their vehicle. A man tried to intervene; they also pulled him in. I noted that the police put individuals whom they did not believe were guilty or who did not try to resist in our quarters, and those whom they suspected of something or who resisted in the adjacent room. We heard the sounds of beating and screams coming through... A victim in the other room was beaten so badly that when his wife helped him come out, he collapsed and had to be taken to an emergency care facility.”

Dang Minh Ty (aka Tee Dang), an American citizen, was arrested as he took photograph of the demonstration in Ho Chi Minh City. He was taken to the police station of Ward 6, District 3. There, he was repeatedly punched by a public security officer named Nguyen Huu Phap, in the presence of many other public security officers. They wanted the password to his smart phone. He felt acute pain at one side of his ribcage and told his interrogators that one of his rib bones might have been broken. Phap continued to punch Ty and only stopped after Ty claimed that he was a U.S. citizen. At that point the public security of Ho Chi Minh City took over the interrogation. They threatened to damage the other side of his rib cage. As Ty refused to disclose the password to his smart phone, they connected it to a special equipment and opened his smart phone. For two days they interrogated him about many of the individuals that had communicated with him via texting or through his Facebook page. Only after he had admitted that he regretted having taken the photographs of the demonstration was he released.

⁶ Amnesty International, *Viet Nam: Authorities must investigate torture allegations following mass arrests*, (June 18, 2018) <https://www.amnesty.org/en/latest/news/2018/06/viet-nam-authorities-must-investigate-torture-allegations-following-mass-arrests/>

Vietnam's legal framework

10. In the past 15 years, the Vietnamese government has systematically codified the *de facto* restrictions on the Vietnamese peoples' right to free thought and expression.⁷ The government has passed laws to silence government critics under the pretext of national security. On their face, these laws clearly violated many UN treaties to which Vietnam is a state-party.
11. In addition to overt violations of human rights, the vagueness of many of these provisions makes it impossible for an individual to foresee what actions are criminalized, in violation of the principle of legality embedded in Article 15(1) of the International Covenant on Civil and Political Rights (ICCPR), 11(2) of the Universal Declaration of Human Rights (UDHR), and Article 20(2) of the ASEAN Human Rights Declaration (AHRD); these provisions prohibit prosecution for a crime "which did not constitute a[n] [] offense, under national or international law, at the time when it was committed."⁸ In General Comment No. 35, the UN Human Rights Committee confirmed that "[a]ny substantive grounds for arrest or detention must be prescribed by law and should be defined with sufficient precision to avoid overly broad or arbitrary interpretation or application."⁹
12. Moreover, the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism has explained that the standard for legality certainly requires framing laws "in such a way that [] the law is adequately accessible so that the individual has a proper indication of how the law limits his or her conduct; and [that] the law [be] formulated with sufficient precision so that the individual can regulate his or her conduct."¹⁰ Many of the laws that the Vietnamese government has frequently used to prosecute government critics appear purposefully vague so that the government can apply them to any action which it deems offensive. Without precise definitions it is impossible, for instance, to determine what expression the government might consider to be "propaganda" or what acts might be considered to be an "abuse" of democratic freedom. Not only does the range of potentially criminal acts include acts of expression, association or assembly which are protected under international law, but it is very difficult, perhaps by design,

⁷ See e.g. US Department of State, *Country Report on Human Rights Practices for 2015: Vietnam*, 1, 22-31 available at <https://www.state.gov/documents/organization/253025.pdf>; *Viet Nam 2017/2018*, *supra* note **Error! Bookmark not defined.**

⁸ UDHR, *supra* note **Error! Bookmark not defined.** at art. 11(2); ICCPR, *supra* note **Error! Bookmark not defined.** at art. 15(1); AHRD, *supra* note **Error! Bookmark not defined.** at art. 20(2).

⁹ Human Rights Committee, *General Comment No. 35*, ¶ 22, U.N. Doc CCPR/C/GC/35 (Dec. 16, 2014) available at goo.gl/p5Y8S6; See also Human Rights Committee, *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant: Russian Federation*, ¶ 24, U.N. Doc CCPR/C/RUS/Co/6 (Nov. 24, 2009) available at <http://www2.ohchr.org/english/bodies/hrc/docs/co/CCPR.C.RUS.CO.6.pdf> (noting the pattern of Governments using vaguely worded laws to pursue politically motivated claims).

¹⁰ See Martin Scheinin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶ 46, U.N. Doc. E/CN.4/2006/98 (Dec. 28, 2005).

for a conscientious Vietnamese activist or journalist to determine exactly what acts might be risking criminal prosecution. This lack of legality certainly not only enables the government to prosecute anyone for anything, it also casts a chill over all acts of expression, association or assembly.¹¹

The 2013 Constitution

13. The 2013 Constitution was adopted on November 28, 2013 by the National Assembly. Chapter II, from Article 14 to Article 49, titled “Human Rights, Fundamental Rights, and Obligations of Citizens”, provides the constitutional basis for the following human rights:
 - privacy of communication (Article 21);
 - freedom of movement (Article 23);
 - freedom of religion (Article 24);
 - freedom of speech, freedom of the press, freedom of association, freedom of assembly (Article 25);
 - right to be free from discrimination (Article 16);
 - right to a fair trial (Article 31).
14. Article 14 lays the contours of permissible limitations to human rights, including the right to freedom of expression: “Human rights and citizens’ rights may not be limited unless prescribed by a law solely in case of necessity for reasons of national defence, national security, social order and safety, social morality and community well-being.”
15. Article 21 makes it clear that intervention of private communications must be prescribed by law, with legitimate aim and only in case of necessity: “Everyone has the right to privacy of correspondence, telephone conversations, telegrams and other forms of private communication. No one may illegally break into, control or seize another’s correspondence, telephone conversations, telegrams or other forms of private communication.”
16. However, other articles of the Constitution impose hard boundaries on freedom of thought and expression. Article 4 casts the shadow of the Communist Party of Vietnam (CPV)’s ideology over the entire society: “The CPV -- the Vanguard of the working class, concurrently the vanguard of the working people and Vietnamese nation, faithfully representing the interests of the working class, people and entire nation, and acting upon the Marxist-Leninist doctrine and Ho Chi Minh Thought -- is the force leading the State and society.” Article 51 creates a “socialist-oriented market economy,” and Articles 102(3) and 107(3) require the People’s Courts and the People’s Procuracies to safeguard “the socialist regime”. These articles set the stage for the state to use its justice system to suppress fundamental freedoms otherwise recognized and guaranteed by the Constitution.

¹¹ Freedom Now, Using Law as a Tool of Oppression: Vietnam’s Crackdown on Civil and Political Rights, (Draft version, July 6, 2018)(on file with author)

Criminal Code

17. The 1999 Criminal Code criminalized violations of privacy. Article 159 imposes penalties of administrative fine of between VND 20 million and VND 50 million and imprisonment of between one and three years. This provision affirms the constitutional guarantee of privacy and criminalizes illegal communications surveillance, and therefore, complies with the principle of safeguards against illegitimate access.
18. On the other hand, the 1999 Criminal Code included broad provisions that were worded vaguely enough to criminalize a range of protected speech, religion, association, and assembly-related activities. A civil society activist peacefully protesting or a journalist or blogger reporting on government policy might be charged with some combination of “carrying out activities aimed at overthrowing the people’s administration,”¹² “undermining the unity policy,”¹³ “conducting propaganda against the state,”¹⁴ “disrupting security,”¹⁵ “abusing democratic freedoms to infringe upon the interests of the state,”¹⁶ “resisting persons in the performance of their official duties,”¹⁷ or a number of other national security or public order related provisions.
19. The revised Criminal Code of 2015, taking effect on January 1, 2018, preserves all of these problematic provisions, increases the length of the sentences and includes harsher penalties and more expansive provisions for the crimes with which government critics are most commonly charged. The punishment for “undermining the unity policy,” for example, was increased from a range of 5 to 15 years to a range of 10 to 20 years for serious cases and from a range of 2 to 7 years to a range of 5 to 12 years for less serious cases. Likewise, the punishment for “conducting propaganda against the state” rose its minimum time of imprisonment from 3 years to 5 years.
20. Article 109 criminalizes the mere act of joining an organization that acts against the government, a blatant violation of Article 22 of the ICCPR that guarantees freedom of association. Articles 116 and 117 criminalize the making, storing or dissemination of materials that, *inter alia*, defame or contain distorted information about the government, which is in violation of an individual’s right to “seek, receive and impart information and ideas of all kind” under Article 19(2) of the ICCPR. Article 331 even criminalizes the “[abuse of] freedom of speech, freedom of the press, freedom of religion, freedom of association and other democratic freedoms to infringe upon the

¹² Criminal Code (1999), No. 15/1999/QH10, art 79, (December 21, 1999)

http://www.wipo.int/wipolex/en/text.jsp?file_id=385615 (This provision was included in the amended Criminal Code at Article 109).

¹³ *Id.* at art. 87 (Criminal Code (2015) Article 116).

¹⁴ *Id.* at art. 88 (Criminal Code (2015) Article 117).

¹⁵ *Id.* at art. 89 (Criminal Code (2015) Article 118).

¹⁶ *Id.* at art. 258 (Criminal Code (2015) Article 331).

¹⁷ *Id.* at art. 257 (Criminal Code (2015) Article 330).

interests of the state, lawful rights and interests of organizations and/or citizens” which impermissibly restricts all civil and political rights within the bounds of the government’s interest.¹⁸

21. The amended Criminal Code also includes a new range of “preparatory” offenses, which criminalized “any person who makes preparation for the commitment of this criminal offense”; this new category of offense was added to, *inter alia*, the crimes of “carrying out activities aimed at overthrowing the people’s administration,”¹⁹ “undermining the unity policy,”²⁰ “conducting propaganda against the state,”²¹ and “disrupting security.”²² The Criminal Code does not include any requirement that such person has either specific intent to commit a crime or has taken direct action towards such crime’s completion for such “preparation” to have occurred, a vagueness which thus allows the government to prosecute anyone for any speech or action deemed to be preparatory. In theory, these provisions would permit prosecution not just for a person protesting or writing a critical blog post, but also for a person who is merely walking towards a demonstration or into a cybercafé.²³
22. Certain amendments to the Criminal Code impact defendants’ procedural rights. For example, Article 19(3) requires a defense attorney to report his clients’ “serious” or national security crimes—a provision which has a significant impact on a defendant’s right to confidentially communicate with counsel.²⁴

Criminal Procedure Code

23. The 2015 Criminal Procedure Code, which was adopted on November 27, 2015 and went into effect on January 1, 2018, creates “special methods of investigation and legal proceedings” specifically legalizing communications surveillance and collection of personal information so as to protect the government and the socialist regime. The special methods and proceedings include “secret recording by sound or sound-and-visual means”, “secret phone tapping,” and “secret collection of electronic data” (Article 223).
24. Article 224 specifies circumstances where communications surveillance can be conducted, including “breach of national security.” It refers to the Chapter XIII of the 2015 Criminal Code, “infringement of national security,” which addresses crimes

¹⁸ *Id.* at art. 331.

¹⁹ Criminal Code (2015), *supra* note **Error! Bookmark not defined.** at art. 109.

²⁰ *Id.* at art.116.

²¹ *Id.* at art. 117.

²² *Id.* at art. 118.

²³ Freedom Now, Using Law as a Tool of Oppression: Vietnam’s Crackdown on Civil and Political Rights, (Draft version, July 6, 2018)(on file with author)

²⁴ HWR, *Vietnam: New Law Threatens Right to a Defense*, (June 21, 2017)

<https://www.hrw.org/news/2017/06/21/vietnam-new-law-threatens-right-defense>

against the people's government, including crimes concerning expression of dissent, peaceful assembly and association.

25. Article 226 creates limitation of communications surveillance within two months. It can be extended but "shall not exceed the time limit for investigation as defined by this law." Moreover, Article 227 strictly limits the use of information and documents collected through communications surveillance within criminal prosecution and "documents and information irrelevant to the case must be disposed in timely manner." However, the code does not mention any rules on the destructions or erasure of surveillance data, and the bodies responsible for supervising the use of surveillance, which is the People's Procuracies, are not independent of the CPV.

Other laws

26. The 2004 Law on National Security, effective on July 1, 2005, defines (in Article 3) "national security" as "the stability and sustainable development of the socialist regime and the State of the Socialist Republic of Vietnam, the inalienability of the independence, sovereignty, unity and territorial integrity of the Fatherland." It also defines "activities of infringing upon the national security" as "acts of infringing upon the political regime, the economic regime, culture, security, national defence, external relations, independence, sovereignty, unity, territorial integrity of the Socialist Republic of Vietnam." Article 13 prohibits "organizing, operating, colluding with, instigating, controlling, inciting, buying off, deceiving or dragging other persons to oppose the people's administration, to abolish the leadership role of the Communist Party of Vietnam, to divide the country, to disrupt the national unity bloc." Article 5 puts national security protection under the leadership of the CPV. The law equates threats to the CPV and the party's ideology with threats to national security, and outlaws dissents and any mobilization of people outside of the CPV's control. It accordingly specifies constitutional limitations on the right to privacy, freedom of expression, freedom of assembly, freedom and association, and other civil and political freedoms.
27. It imposes communications intervention in cases of apparent threats to national security. In such cases, the authorities can take control of the communications means in certain areas (Article 21), or to check, requisition, suspend or stop means of communications, as well as to check computers and computer networks (Article 24). The law does not mention any clear and precise manner, time limits, specific procedures, or rules on the destructions or erasure of surveillance data, and fails to establish an independent mechanism to review and check on communications surveillance to ensure its legality. It can be used to target those who peacefully exercise fundamental civil and political freedoms, especially those who criticize and challenge the CPV.
28. It grants the government broad authority to intervene in telecommunication networks, computers, and computer network while not clarifying a legal process of issuing

orders. It does not require prior judicial authorization, fails to create a mechanism of check and balance for the intervention, and does not safeguard the right to notification.

29. The 2006 Law on Information Technology was adopted on June 29, 2006 and took effect on January 1, 2007. It grants the government broad authority to obtain and monitor digital information through technology companies without prior judicial authorization, and does not grant these companies the right to challenge government's orders. It requires server/hosting service providers to share with the authorities information of their clients upon government request. It also allows the authorities to monitor digital information and to ask technology companies to monitor digital information. Under Article 18, organizations and individuals that lease space for digital information storage have "to comply with competent state agencies' request to determine lists of owners that hire digital information storage space for the establishment of their websites and lists of owners of digital information stored by such organizations or individuals."
30. The 2009 Law on Telecommunications, adopted on November 23, 2009 and taking effect on July 1, 2010, provides legal grounds for the government to obtain and monitor digital information, including the name, address, telephone numbers of caller and recipient, location of caller and recipient, call duration and other private information of users upon request by the government. The law provides legal grounds for the government to obtain and monitor digital information without prior judicial authorization.
31. Decree 72, issued on July 15, 2013 and taking effect on September 1, 2013, mandated that blogs and social websites could only be used to share personal information and prohibited the sharing of news articles and material harmful to national security or opposing the Vietnamese government.²⁵ It provides guidance to the Law on Information Technology, the Law on Telecommunications, and other laws on managing the internet. Articles 24, 28 and 34 require companies, organizations that run news websites, social networks, mobile news services, and online games to have at least one server located in Vietnam for government's inspection. Companies have the obligation to provide their clients' data "upon request of competent authorities as prescribed by law". This regulation also applies to foreign companies.
32. Decree 174, effective since 2014, imposes fines on anyone criticizing the government or "spreading propaganda" on social media.²⁶

²⁵ BBC News, *Vietnam Internet Restrictions Come into Effect*, (September 1, 2013) <https://www.bbc.com/news/world-asia-23920541>; Committee to Protect Journalists, *New Cybersecurity Law Threatens Press Freedom in Vietnam*, (June 12, 2018) <https://cpj.org/2018/06/new-cybersecurity-law-threatens-press-freedom-in-v.php> (hereinafter CPJ).

²⁶ *Freedom in the World: Vietnam 2017*, *supra* note **Error! Bookmark not defined.**.

33. Decree 25/2011/ND-CP,²⁷ issued on April 6, 2011 and taking effect on June 1, 2011, requires telecommunication service providers to store the registered subscriber information in accordance with the Ministry of Information and Communications, and to provide the information to competent state agencies upon request. It specifies the types of information that the subscribers must provide to service providers: (1) for individuals, full name, date of birth, number, date and place of issuance of identity cards for the Vietnam citizens or passport for foreign citizens; (2) for organizations, organization name, operating address, registration number and date established, number and date of the license for operation or number and date of certificate of registration of business of the organization; the full name, date of birth, number, date and place of issuance of ID card or passport of the person acting as a representative and whose name is written in the contract for use of telecommunication services. The information can also be used to serve “the national security, social order and safety” and “other purposes as prescribed by the Ministry of Information and Communications.”
34. Decree 72/2013/ND-CP, issued July 15, 2013, imposes many restrictions on freedom of expression²⁸. It puts Internet users’ personal data at risk by requiring companies and organizations that run news websites (Article 24), social networks (Article 25), mobile news services (Article 28), and online games (Article 34) to have at least one server located in Vietnam for government’s inspection²⁹. Article 22 requires foreign organizations, enterprises, and individuals that provide public information across the border that is accessed by Vietnamese people or from people in Vietnam must comply with Vietnam’s law. Article 24 requires service providers to have at least one server in Vietnam for the inspection, storage, and provision of information at the request of competent authorities, and settlement of customers’ complaints in accordance with regulations of the Ministry of Information and Communications. Article 25 requires service providers to provide personal information of the users at the request of competent authorities, and to ensure that only the persons that provide accurately their personal information are allowed to establish personal websites or provide information on social networks. Articles 28 and 34 similarly require mobile phone and game service providers to place at least one server in Vietnam.
35. Decree 49/2017/ND-CP, issued on April 24, 2017 as amendment to Decree 25, requires clients to provide a portrait photo to their telecommunications providers, making it significantly easier for the government to identify and track down a user through the facial recognition technology while being able to monitor every single movement of any citizens without the use of a warrant. For example, through CCTV, the government can quickly identify participants in a protest by retrieving the person’s

²⁷<https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-25-2011-ND-CP-huong-dan-Luat-Vien-thong-121713.aspx>

²⁸<http://www.bbc.com/news/world-asia-23920541>

²⁹<https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Decree-No-72-2013-ND-CP-internet-services-and-online-information-202402.aspx?tab=1>

data from the service provider when the facial recognition matches the information from the CCTV footage with the database maintained by the service provider.

36. The 2015 Law on Cyber Information Security, No. 86/2015/QH13, was passed on 19 November 2015 and came into force on 1 July 2016. It regulates information network systems ostensibly to ensure the security of online information but includes provisions that require businesses providing encryption services to be based in Vietnam, and to provide user data, when requested, to the Ministry of Public Security. The government can thus monitor private communications and use them as basis for retaliatory actions against government critics.³⁰
37. The Law on the Press, effective January 2017, was designed to consolidate the CPV's control over the media. Presented as a law that "prescribes citizens' rights to freedom of the press and freedom of speech in the press,"³¹ in actuality it aims to ensure that the domestic media does not publish or promote ideas that are seen as challenging the CPV's ideology and national policies.³² Article 4(2) prescribes that the press should "propagandize and disseminate, and contribute to the protection of, the line and policies of the Party...and build and promote socialist democracy, strengthen the great national unity bloc, and build and protect the socialist Fatherland of Vietnam."³³
38. Decree 27/2018/ND-CP, issued on March 1, 2018 and taking effect on April 15, 2018, amended Decree 72. It maintains most of the regulations of Decree 72 and adds a requirement that social networks/news websites must ask their users to provide real identity and store their users' accounts' information, including IP and activity logs, for at least two years. Both decrees provide legal basis for communications surveillance without specifying any clear and precise manner, time limits, specific procedures, rules on the destructions or erasure of surveillance data, or any mechanism to review and check on communications surveillance activities independently. Both decrees grant the government broad authority to obtain and monitor digital information through technology companies without prior judicial authorization, and do not grant these companies the right to challenge the government's orders. Decree 27 requires users to provide real identity information, including full name, birthday, and identity card/passport information. It also forces social networks to store user account data, including log in – log out activities, Internet Protocol (IP) addresses, and content posting logs, for at least two years. Thus, requiring news websites, social media, mobile news services, and online games to store their data in Vietnam obviously

³⁰ Michael L. Gray, *The Trouble with Vietnam's Cybersecurity Law*, *The Diplomat*, (October 21, 2016) <https://thediplomat.com/2016/10/the-trouble-with-vietnams-cyber-security-law/>.

³¹ Law on the Press, No. 103/2016/QH13, (2016) art. 1, *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=447052; *see also* Vietnam Law & Legal Forum, *Revised Law on Press*, (November 1, 2017) <http://vietnamlawmagazine.vn/revised-law-on-press-5693.html>.

³² Law on the Press, *supra* note 31; *see also* Feliz Solomon, et al., *Press Freedom is Under Attack Across Southeast Asia: Meet the Journalists Fighting Back*, *Time*, (June 22, 2018) http://amp.timeinc.net/time/longform/press-freedom-southeast-asia?__twitter_impression=true.

³³ Law on the Press, *supra* note 31 at art. 4(2).

provides the authorities broad access to the data because the government can send requests to the local data centers and order them to comply while they cannot make such requests to foreign data centers.

39. In June 2018, the National Assembly passed another cybersecurity law that is to go into effect on January 1, 2019. This law requires online businesses, such as Google and Facebook, that currently store their data outside of Vietnam to store their data inside Vietnam, and to turn over user data to the Ministry of Public Security or the Ministry of Information and Communications upon request.³⁴ Equally concerning are provisions that make it illegal to “distort history, deny revolutionary achievements, [or] undermine national solidarity.”³⁵ These vague terms allow the government tremendous leeway to target those who use the internet or communication apps to discuss political and religious views.³⁶ The law will give the government enhanced authority to “surveil the internet, including the ability to force international technology companies with operations in the country to reveal their users' personal information and censor online information on demand.”³⁷

Recommendations

40. The Vietnamese government needs to make substantive and substantial changes to its current legal system to improve the protection of citizens' privacy and their freedom of thought and expression, including:

- a) Amending or removing the following provisions in the 2015 Criminal Code:
 - (i) “sabotaging implementation of socio-economic policies” (Article 115)
 - (ii) “sabotaging implementation of solidarity policies” (Article 116)

³⁴ IFEX, *Vietnam's Cybersecurity Law Threatens Free Speech and Digital Economy*, (June 26, 2018), <https://www.ifex.org/vietnam/2018/06/25/cybersecurity-law/> (noting that article 26 of the cybersecurity law requires companies to verify user information, and provide user information to the Ministry of Public Security upon request); see also Mai Nguyen, *Vietnam Lawmakers Approve Cyberlaw Clamping Down on Tech Firms, Dissent*, Reuters, (June 12, 2018) <https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-lawmakers-approve-cyber-law-tighten-rules-on-google-facebook-idUSKBN1J80AE>; Asian Correspondent, *Vietnam Passes Law Requiring, Google, Facebook to Reveal User Data*, (June 12, 2018) <https://asiancorrespondent.com/2018/06/vietnam-passes-law-requiring-google-facebook-give-user-data/#8iVQGlajBPOOk21.97>.

³⁵ Human Rights Watch, *Vietnam: Withdraw Problematic Cyber Security Law*, (June 7, 2018), <https://www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law> (citing to Article 8 of the law).

³⁶ Committee to Protect Journalists, *New Cybersecurity Law Threatens Press Freedom in Vietnam*, (June 12, 2018) <https://cpj.org/2018/06/new-cybersecurity-law-threatens-press-freedom-in-v.php> see also Bao Ha, *Vietnam says Cybersecurity Law Needed to Ensure National Security*, VN Express International, (June 12, 2018) <https://e.vnexpress.net/news/news/vietnam-says-cybersecurity-law-needed-to-ensure-national-security-3762377.html>.

³⁷ Committee to Protect Journalists, *New Cybersecurity Law Threatens Press Freedom in Vietnam*, (June 12, 2018) <https://cpj.org/2018/06/new-cybersecurity-law-threatens-press-freedom-in-v.php>.

- (iii) “making, possessing, spreading information, materials, items for the purpose of opposing the State of the Socialist Republic of Vietnam” (Article 117);
 - (iv) “disruption of security” (Article 118);
 - (v) “organizing, coercing, instigating illegal emigration for the purpose of opposing the people’s government” (Article 120); and
 - (vi) “illegal emigration for the purpose of opposing the people’s government” (Article 121).
- b) Amending the 2015 Criminal Procedures Code to grant the People’s Courts system the power of approving and/or rejecting all kinds of surveillance orders.
- c) Amending the 2015 Criminal Procedures Code to abolish all forms of digital communications surveillance that are not in line with the provisions on special methods of investigation and proceedings. As an alternative to amending the Code, the National Assembly may pass a resolution on the implementation of the Code that abolishes those forms of surveillance.
- d) Amending the 2015 Criminal Procedures Code to recognize the right to receive notifications of persons under surveillance and grant them the right to challenge the surveillance orders in the court.
- e) Removing all provisions that require service providers to place servers in Vietnam or to provide user information to the government.
- f) Recognizing the right to be forgotten, which guarantees that users can request technology companies to erase their personal data stored in the companies’ system.
- g) Removing provisions in the 2018 Cybersecurity Law that make “to distort history, deny revolutionary achievements, [or] undermine national solidarity” a criminal offense.