ICNL

www.icnl.org
info@icnl.org

LEGAL ANALYSIS: CAMBODIA

Draft Law on Cybercrime, 2022

Introduction

The Royal Government of Cambodia (RGC) has been discussing the adoption of a Cybercrime Law for several years. In August 2022, ICNL received an English version of a revised draft of the Law on Cybercrime (Law).[1] This newest draft, dated June 29, 2021, is the fourth iteration of the Law. While this fourth draft version of the Law contains some improvements from the third iteration of the Law,[2] there remain significant concerns that the Law, as currently drafted, restricts the freedom of expression and violates the right to privacy of Cambodians.

This analysis compares the Law to international law, standards and best practices related to the freedom of expression and right to privacy. It does not address every issue within the Law.

There are several articles in the Law that may lead to impermissible restrictions on the freedom of expression and right to privacy. If amended to respect the freedom of expression and right to privacy in accordance with Cambodia's international legal obligations, the Law would still enable the RGC to prevent, investigate and prosecute criminal activity occurring on computer systems.

ICNL is concerned that the Law may impermissibly restrict the freedom of expression or right to privacy in four main areas:

- **Vague restrictions on certain categories of speech limit the freedom of expression**. The Law criminalizes certain types of speech based on vague language, which invite unlawful restrictions to the freedom of expression.
- **Unreasonable obligations of "service providers."** The Law requires service providers to manage "subscriber information" and turn that information over to RGC authorities. Depending on how the Law is interpreted, these requirements could make using the internet anonymously impossible and prevent the use of encryption and other safety features.
- **Limited judicial oversight or time limits for surveillance activities**. The Law grants RGC authorities vast powers to surveil electronic communications, but often does not require judicial approval prior to commencing surveillance and does not provide a time frame for that surveillance. As a consequence, electronic surveillance can be initiated for arbitrary reasons and potentially persist for years, which would violate the right to privacy and freedom of expression.
- **Administrative penalties and transitional fines may be used to target civil society organizations.** The Ministry of Interior (MOI) is empowered to issue

[1] This English Translation is marked as an official translation from the Anti-Cybercrime Department.
[2] See, ICNL, Legal Analysis: Draft Law on Cybercrimes (December 2020).

administrative penalties, which include "suspension or revocation of licenses." The MOI is similarly empowered to fine violators of the Law, but the amount of the fine is not defined, and the Law contains no criteria stating when it is appropriate for the MOI to impose either administrative penalties or transitional fines.

International Law

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) requires State parties to guarantee the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers.[3] The UN Human Rights Committee has stated that, "any restrictions on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination systems" must comply with Article 19.[4]

Restrictions to the freedom of expression guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test.[5] According to the test:

(1) the restriction must be provided by law, which is clear and accessible to everyone (i.e., adheres to principles of predictability and transparency);

(2) the restriction must pursue one of the purposes set out in article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and

(3) the restriction must be necessary and the least restrictive means required to achieve the purported aim (i.e., adheres to principles of necessity and proportionality).

Similarly, the right to privacy is enshrined in Article 17 of the ICCPR, "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from State intervention.[6] "In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous."[7]

Although Article 17 envisages necessary, legitimate and proportionate restrictions to the right to privacy, the United Nations Special Rapporteur on the promotion and protection of the

[3] The Kingdom of Cambodia became a party to the ICCPR on 26 August 1992.
[4] Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 43, UN Doc # CCPR/C/GC/34 (2011).
[5] *See, e.g.* United Nations Human Rights Council, A/HRC/17/27, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" May 16, 2011, para. 69.
[6] *See*, Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, para. 4. 82 (Butterworth, 2004).
[7] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 23.

right to freedom of opinion and expression (Special Rapporteur) states that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, elucidated in the Human Rights Committee General Comment 27, paragraph 15:

(a) Any restrictions must be provided by the law;
(b) The essence of a human right is not subject to restrictions;
(c) Restrictions must be necessary in a democratic society;
(d) Any discretion exercised when implementing the restrictions must not be unfettered;
(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim; and
(f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected.[8]

The freedom of expression and the right to privacy are interrelated: "the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression."[9] Limitations or restrictions to one of these rights impact the enjoyment of the other. Just as a restriction to the freedom of expression must pass the three-part cumulative test derived from ICCPR Article 19 to be lawful, a restriction to the right to privacy is only lawful if it passes the test articulated in General Comment 27.15.[10]

Analysis

VAGUE LANGUAGE UNDERMINES THE FREEDOM OF EXPRESSION

ISSUE: Chapter 7 of the Law defines several acts as cybercrimes. While it is essential that authorities have the ability to prevent, investigate and prosecute legitimate cybercrimes, several of the crimes listed in Chapter 7 are vague and overly broad, which could lead to impermissible restrictions to the freedom of expression.

ANALYSIS: Restrictions to the speech and expressions guaranteed in Article 19 of the ICCPR are lawful only when such restrictions pass Article 19's three-part, cumulative test.[11]

[8] Human Rights Committee, General Comment No. 27: Freedom of Movement (Article 12), para. 15, UN Doc # CCPR/C/21/Rev.1/Add.9 (1999); United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 29.
[9] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 24.
[10] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 29.
[11] *See, e.g.* United Nations Human Rights Council, A/HRC/17/27, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" May 16, 2011, para. 69.

Article 45

Article 45 criminalizes "disinformation" and "false statements" made on computers or telecommunications equipment:

> 1. Any person who disseminates or distributes false information through information technology that intentionally harms relations with other countries, social security and order, society, economy, or causes racism, or affects traditional culture shall be punishable by imprisonment from 1 (one) month to 3 (three) years and a fine from 2,000,000 (two million) to 10,000,000 (ten million) Riels.
> 2. Any person who disseminates or distributes false information through information technology that intentionally harms national defense or national security shall be punishable by imprisonment from 2 (two) years to 5 (five) years and a fine from 10,000,000 (ten million) to 50,000,000 (fifty million) Riels.[12]

These provisions essentially amount to an "anti-fake news" law, which is incompatible with the freedom of expression.[13] Rather than prevent the spread of misinformation or disinformation,[14] such laws chill legitimate and important expression from civil society and the public. Allowing governments to be the arbiters of truth tends to erode existing democratic norms, while failing to actually prevent false content.[15]

International experts on the freedom of expression have definitively stated that "anti-fake news" laws violate the freedom of expression. The international special rapporteurs on the freedom of expression and/or the media adopted a joint declaration in March 2017 that specifically noted, "General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression…and should be

[12] Law, Article 45.
[13] *See*, The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on "Fake News", Disinformation and Propaganda, para. 2(a) (March 3, 2017).
[14] According to UNESCO, 'misinformation' is defined as "[i]nformation that is false but not created with the intention of causing harm," while 'disinformation' is "[i]nformation that is false and deliberately created to harm a person, social group, organisation or country." (Mal-information is "[i]nformation that is based on reality, used to inflict harm on a person, social group, organisation or country.") *Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training*, UNESCO, https://en.unesco.org/fightfakenews.
[15] Education and media literacy campaigns have been much more effective at combating false information in the public sphere. For more, *see, e.g.*, Darrell M. West, *How to combat fake news and disinformation, Report*, Brookings, Dec 18, 2017, available at: https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.

abolished."[16] Joint declarations by these mandate holders are considered as very persuasive interpretations of existing international human rights law on the topics addressed.[17]

From a policy perspective, criminalizing "false" news or "false" content, like in Article 45, will: (a) stifle independent media, especially those outlets and reports that are critical of government policies; (b) create a chilling effect on public debate; (c) undermine government and public accountability because the presentation of critical views is criminalized; (d) result in less information on community needs being available to government decision-makers, thereby impeding government ability to solve problems; and (e) weaken democracy. Ironically, laws seeking to prohibit false news may actually result in the suppression of "true news," including the presentation of non-partisan, objective analysis, especially where such analysis challenges a government policy or position.

OVERLY BROAD AND VAGUE RESTRICTIONS OF CONTENT

The categories of speech prohibited in Article 45 are too broad and too vague to satisfy the principles of predictability and transparency. These principles, which make up the "provided by law" requirement of Article 19's three-part test, are not met merely because a law or regulation is officially enacted. To satisfy this requirement, restrictions to the freedom of expression must be both predicable and transparent; the law in question must be formulated with sufficient precision to enable both the individual and those charged with its execution to conform their conduct to the law.[18] The categories of prohibited content in Article 45 are too vague to meet the principles of predictability and transparency because they are too broad for people to know what content is or is not permissible.

- *Harms relations with other countries, social security and order, society, economy*
  This category of speech is simply too broad for individuals to know what can and cannot be said, and thus fails the first prong of Article 19's three-part test. Nearly any criticism of Cambodia's foreign relations, immigration policy or customs enforcement could be seen as harming Cambodia's relations with other countries.
  Similarly, the prohibition against making "false" statements that would "harm social security" or "harm society" are wide-ranging and undefined, making it impossible for the public to know in advance what conduct or speech is permissible and what speech is illegal. For example, news coverage related to demonstrations or protests, or allegations of human rights abuses could be deemed to harm order or society.

[16] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration on ''Fake News'', Disinformation and Propaganda, para. 2(a) (March 3, 2017).
[17] *See*, Toby Mendel, *The UN Special Rapporteur on Freedom of Opinion and Expression: Progressive Development of International Standards Relating to Freedom of Expression*, in T. McGonagle and Y. Donders (eds), The United Nations and Freedom of Expression and Information: Critical Perspectives, Cambridge University Press, p. 251-257 (2015).
[18] United Nations Human Rights Council, A/71/373, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" September 6, 2016, para. 12 ("The first prong of the three-part test requires restrictions to the freedom of expression to be both predicable and transparent; a restriction "must be formulated with sufficient precision to enable both the individual and those charged with its execution to regulate conduct accordingly…").

Finally, speech that "harms the economy" could include news coverage related to corruption, taxes or development projects. Would a report from the World Bank that forecasts lower GDP growth than the Ministry of Finance run afoul of this prohibition?

- *Causes racism*
  This provision amounts to a prohibition against "hate speech." While States are required to prohibit hate speech under Article 20(2) of the ICCPR and Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), any restriction to speech made under ICCPR, Article 20(2) or ICERD, Article 4 must comply with Article 19's three-part test.[19] Laws prohibiting hate speech need to be carefully drafted to ensure that they do not inadvertently restrict legitimate expression. "Article 20 of the [ICCPR] requires a high threshold because, as a matter of fundamental principle, limitation of speech must remain an exception."[20] "Advocacy of hatred on the basis of national, racial or religious grounds is not an offence in itself. Such advocacy becomes an offence only when it also constitutes incitement to discrimination, hostility or violence, or when the speaker seeks to provoke reactions on the part of the audience."[21]

  Therefore, to meet this high threshold and ensure compliance with freedom of expression protections, a legal provision prohibiting hate speech must contain three elements: (1) conduct that constitutes advocacy of hatred on the basis of national, racial or religious grounds; (2) the advocacy of hatred involves incitement to discrimination, hostility or violence; and (3) such incitement leads to discrimination, hostility or violence.[22] A hate speech restriction will comply with Article 19 of the ICCPR if it includes the proper intent, actual incitement and proscribed results. Simply put, prohibiting any speech that "causes racism" does not meet any of the three elements required to properly prohibit hate speech.

  This provision would significantly restrict expression and does not comply with Article 19 of the ICCPR.

- *Affects traditional culture*
  This category of speech is too vague to be compatible with international law. The term "traditional culture" is undefined, which is likely to lead to arbitrary enforcement. Indeed, several artists have been arrested in recent years for artwork or songs that RGC authorities deemed were offensive to Cambodia's traditions and culture. The right to freedom of expression includes the right to offend, shock and disturb.

[19] *See, e.g.* United Nations Human Rights Council, A/67/357, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" September 7, 2012, para. 41.
[20] Rabat Plan of Action, *Annual report of the United Nations High Commissioner for Human Rights Addendum Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred*, A/HRC/22/17/Add.4, Appendix, para. 18 (January 2013).
[21] United Nations Human Rights Council, A/67/357, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" September 7, 2012, para. 43.
[22] United Nations Human Rights Council, A/67/357, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" September 7, 2012, para. 43.

- *Harms national defense or national security*
  Legal provisions that prohibit statements or online content that "harms national defense or national security" are used to unlawfully restrict and penalize criticism of governments in contravention of Article 19 of the ICCPR.[23] These vague terms are open to interpretation and therefore give the government broad discretion to pursue criminal actions against individuals on arbitrary and subjective grounds.

The categories of prohibited speech in Article 45 do not sufficiently allow internet users or even government authorities to know what content is or is not permitted online. When officials are given unlimited discretion to determine whether speech is allowable, a grave threat to free speech exists, especially when such speech is critical of government authorities. These imprecise categories of prohibited content in Article 45 do not pass the first part of Article 19's three-part test due to their imprecision, and if enacted will likely lead to the censorship of legitimate speech.

DISPROPORTIONATE PENALTIES

The penalties outlined in Article 45 are disproportionate to any harm that may be caused, and therefore Article 45 fails the third-prong of Article 19's three-part test. The principles of necessity and proportionality require that punishments be the least restrictive means necessary to remedy the alleged harm. In other words, any penalty must be the least restrictive means to achieve the purported aim.

Article 45 provides for criminal penalties, including extensive fines (up to 50 million riel) and prison time of up to five years. These are exceedingly harsh punishments for sharing news, ideas and opinions, and are disproportionate to any harm caused by speech that is deemed to be false.

RECOMMENDATION: As currently written, Article 45 would allow the RGC to effectively silence and prohibit any speech it does not like. Laws that criminalize "fake news" or that prohibit "false information" violate international law. To comply with international human rights norms, Article 45 and the categories of prohibited speech in it should be revoked. To the extent that prohibiting certain types of content is necessary to protect the rights or reputations of others, national security or public order, or public health or morals, the categories of prohibited content should be redefined to comply with the principles of predictability and transparency.

Article 40

Article 40 prohibits anyone from "caus[ing] harassment, alarm, threat, abuse, persecution, or insult to another person by a computer-related means."[24]

[23] United Nations Human Rights Council, A/71/373, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" September 6, 2016, paras. 13, 29-32.
[24] Law, Article 40: Computer Abuse: "Any person who intentionally causes harassment, alarm, threat, abuse, persecution, or insult to another person by a computer-related means shall be punishable by a fine from 1,000,000 (one million) to 5,000,000 (five million) Riels. In case of causing grievous harm, the offender shall be punishable by

These categories of prohibited content are too vague and broad to pass the "provided by law" principle of Article 19's three-part test since no individual can reasonably predict which statements or content will be considered to "cause alarm" to someone. Similarly, terms like "abuse" and "persecution" are subjective and open to interpretation, which therefore gives the government broad discretion to pursue criminal actions against individuals on arbitrary and subjective grounds. A whole range of legitimate speech could be interpreted as violating Article 40. This is especially true for speech that is critical of government actors or government policy. The right to freedom of expression includes the right to scrutinize, debate openly, make statements that offend, shock and disturb, and criticize.

RECOMMENDATION: To comply with international human rights norms, Article 40 should be removed.

SUSPENSION OR REVOCATION OF LICENSES AND UNDEFINED "TRANSITIONAL FINE" THREATENS CIVIL SOCIETY AND BUSINESSES

ISSUE: Article 6 gives the MOI the power to impose warnings and "transitional fines." The MOI is also empowered to seek a court order to temporarily suspend activities of organizations and businesses in case of "recidivism."[25] However, Article 6 does not state what the fine amounts can be or how the MOI determines "recidivism."

It is also notable that Article 22 states that some cybercrimes will be punishable by a transitional fine via a sub-decree, and that payment of such fine will extinguish criminal actions.[26]

Article 7 permits the institution or ministry that provides a business license, certificate or permit to suspend or revoke that license if an offense is committed.[27]

ANALYSIS: Articles 6, 7 and 22 give vast, unchecked power to the MOI and other ministries, which could be used to target civil society and other businesses.

First, the MOI and relevant ministries are empowered to suspend or shut down organizations and businesses. Closing businesses or organizations is likely a disproportionate penalty under international law, especially if the "crime" relates to speech made online.[28]

---

imprisonment from 1 (one) month to 6 (six) months and a fine from 5,000,000 (five million) to 10,000,000 (ten million). Riels."

[25] Law, Article 6: Competence to warn or impose transitional fine: "Judicial police officers of the General Commissariat of National Police of Ministry of Interior who are in charge of combating cybercrime shall have competence to issue warning and impose transitional fine. In case of recidivism, the competent judicial police officers may seek the court order for temporary suspension of activities or business."

[26] Law, Article 22: Transitional Penalty: "Cybercrime punishable by transitional penalty shall be determined by sub-decree. - The payment of a transitional fine shall extinguish criminal actions."

[27] Law, Article 7: Competence to revoke business rights/business license: "The competent institution that issues a business license, a certificate, or a permit may suspend or revoke that license, certificate or permit if the online business operator commits an offense as prescribed by this law."

[28] United Nations Human Rights Council, A/HRC/17/27, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" May 16, 2011, para. 36: ""Imprisoning individuals for seeking, receiving and imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims under article 19, paragraph 3, of the [ICCPR]."; see also, United Nations Human Rights Council, A/71/373, "Report of the Special Rapporteur on the promotion and protection of

Similarly, the closure of an entity is incompatible with the freedom of association. Involuntary dissolution is a remedy of last resort that should be utilized only for the most serious abuses and generally after notice and an opportunity to rectify the deficiency has been given:

> The suspension and the involuntarily dissolution of an association are the severest types of restrictions on freedom of association. As a result, it should only be possible when there is a clear and imminent danger resulting in a flagrant violation of national law, in compliance with international human rights law. It should be strictly proportional to the legitimate aim pursued and used only when softer measures would be insufficient.[29]

Every media organization, civil society organization and private entity would be in danger of being shut down if one of its employees makes or publishes a statement that violates any of the overly broad and vague restrictions of content. Depending on how the Law is interpreted, organizations will be liable even if an employee was acting outside of his or her official duties while making an alleged illegal statement. Actions by governments against associations must be proportionate.[30] The dissolution or closing of a business, organization or other legal entity is not a proportionate penalty to many of the criminal acts contained in the Law.

Second, because the amount of fines will be determined in a subsequent sub-decree, no one knows the full extent of violating the Law.[31] The sub-decree could set massive fines, which many civil society organizations and businesses could not pay. This would presumably lead to those entities losing their licenses or permits.

Third, there is no threshold or criteria for when the MOI is to issue a warning or impose a transitional fine. This may lead to the MOI arbitrarily choosing when to issue a warning or impose a fine based on subjective, non-transparent reasons.

Punishments for crimes should not occur until after a determination of guilt by a court of law. And that court should determine any and all criminal sanctions. Allowing the MOI and various ministries to solely determine if and when a cybercrime has been committed and what the appropriate penalty should be likely violates international law.

RECOMMENDATION: To comply with international human rights norms, Articles 6 and 7 should be removed from the Law. Fines are already part of several criminal provisions in the Law. If the RGC believes that institutions should be suspended or closed for violations of the Law,

---

the right to freedom of opinion and expression, David Kaye" September 6, 2016, para. 33; United Nations Human Rights Council, A/HRC/7/14, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Ambeyi Ligabo" February 28, 2008, paras. 39-43.

[29] United Nations Human Rights Council, A/HRC/20/27, "Report of UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai" May 21, 2012, para. 75.

[30] See, United Nations General Assembly, A/59/401, "Report of the Special Representative of the Secretary-General on human rights defenders, Hina Jilani, in accordance with General Assembly resolution 58/178" October 1, 2004, page 23; see also: United Nations Human Rights Council, A/HRC/23/39, "Report of UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai" April 24, 2013, para. 38.

[31] See, Law, Article 22: Transitional Fine: "Punishable cybercrime subject to transitional fine shall be determined by sub-decree."

these punishments should be stipulated in the relevant criminal provisions and only courts should be allowed to issue penalties for committing crimes under the Law.

BETTER JUDICIAL OVERSIGHT NEEDED

ISSUE 1: Articles 12-16 outline the procedures required for authorities to search, seize, and intercept data, and order the preservation and production of data. The Law grants the Judicial Police Officers of the General Commissariat of National Police of Ministry of Interior (MOI) the powers to investigate cybercrimes.[32] The Law lacks adequate judicial oversight and safeguards, which jeopardizes the right to privacy and freedom of expression.

DISCUSSION: When Articles 12-16 are reviewed in their entirety, it is clear that the MOI will have vast surveillance powers without meaningful judicial oversight. This is likely to greatly affect the freedom of expression and right to privacy of Cambodians and those living in Cambodia.

Articles 12-16 confer broad, sweeping investigatory powers to the MOI. Even though the MOI can only exercise most these powers after an order from a prosecutor or investigating judge, these entities are not independent judicial authorities, as required under international law.

These powers amount to creating a system of communications surveillance.[33] International human rights law makes clear that the collection and retention of communications data amounts to an interference with the right to privacy.[34] Therefore, pursuant to Article 17 of the ICCPR, the RGC has the onus of showing that the communications surveillance established by Articles 12-16 of the Law passes the test articulated in General Comment 27.15. These articles likely fail because they lack the safeguards required to pass the proportionality prong of this test.

Under international human rights law, any restriction on the rights to privacy and freedom of expression must be shown to be the least restrictive means required to achieve the purported aim. "States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks."[35]

In order to meet a State's international legal obligations, national legislation must "stipulate that State surveillance of communications must only occur under the most exceptional

[32] Law, Article 5: Competent authority to investigate cybercrime: "The judicial police officers of the Ministry of Interior's National Police Commissariat are authorized to investigate offenses under this law. Where necessary, judicial police officers in charge of anti-cybercrime may collaborate with national or international technical experts to investigate said offenses."
[33] The former Special Rapporteur for the freedom of expression, Frank La Rue, defined "communications surveillance" as "the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks." *See*, United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 67.
[34] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, paras. 19-23.
[35] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 80.

circumstances and exclusively under the supervision of an independent judicial authority."[36] Prior judicial authorization of surveillance powers is not merely desirable but essential to respecting the freedom of expression and right to privacy.

Requiring warrants or a judicial order from an independent judicial authority prior to accessing or searching computers and other electronic communications reflects best practices. However, warrants must contain safeguards so that individuals' rights are not infringed upon.

First, warrants for the production, collection or interception of computer data should be narrow in scope and only for a certain, defined duration. International human rights law requires that periods of interception should be limited, not extended indefinitely, and proceed with a continued showing of the interception's necessity.

Second, the scope of data to be collected must be clearly defined and related to the commission of an alleged criminal act. Without this requirement, the likelihood of violations to the right to privacy is increased because authorities are able to collect any and all information of an individual, even if the information is not directly associated with any suspected criminal activity.

Third, the judicial threshold upon which to grant a warrant or order for surveillance or collection of data must be sufficiently high so as not to amount to *de facto* approval. A low threshold like "reasonable grounds to believe" or "reasonable grounds that evidence of a crime exists" amounts to a *de facto* approval of law enforcement requests, which could lead or contribute to an impermissible restriction on the freedom of expression.[37]

In addition, under international law, a set of safeguards needs to be in place to ensure that the system of communications surveillance complies with the ICCPR. "Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law."[38] These safeguards include:

- The offenses and activities in relation to which surveillance may be ordered must be spelled out in a clear and precise manner;
- The law must clearly indicate which categories of people may be subjected to surveillance;
- There must be strict time limits on surveillance operations;
- Strict procedures must be in place for ordering the examination, use, and storage of the data obtained through surveillance;
- There must be strict rules on the destruction or erasure of surveillance data to prevent surveillance from remaining hidden after the fact;

[36] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 81.
[37] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 56.
[38] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 81.

- The bodies responsible for supervising the use of surveillance powers must be independent and responsible to, and be appointed by, Parliament rather than the Executive.[39]

Finally, best practices require legal mechanisms by which these investigatory measures may be challenged by affected individuals and/or service providers.[40]

ARTICLE 12

Article 12(1) requires service providers to immediately preserve any computer data, traffic data or user information upon request from the MOI in cases where "there are reasonable grounds that evidence of a crime exists on a service provider's computer system or otherwise under the control of the service provider."[41] Under Article 12(2), service providers are then required to preserve this data for 180 days, but the MOI can request one additional extension of another 180 days. Under Article 12(3), a prosecutor or an investigating judge can also order the preservation of data; there is no time limit for such preservation. Notably, no warrant or any other judicial oversight is required.

RECOMMENDATION: To comply with international human rights norms, Article 12 should be revised to require meaningful judicial oversight before the preservation of data. In addition, the scope of data that must be preserved should be limited to data directly related to the commission of an alleged criminal act. Finally, safeguards surrounding the use, safety and deletion of such data should be added.

[39] *See*, *Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (May 2014)*, available at: *http://necessaryandproportionate.org/global-legal-analysis*; *citing*, *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, para. 37; *Liberty and Others v. the United Kingdom*, no. 58243/00,1 July 2008 and *Rotaru v. Romania*, no. 28341/95, [GC], 4 May 2000 concerning surveillance carried out by the intelligence agencies.

[40] *See, eg.*, Joint Declaration on surveillance programs and their impact on freedom of expression, issued by the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013, paras. 8 and 9, available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

[41] Law, Article 12: Preservation of computer data and traffic data: "At the request of the competent authority for the collection of the evidence, if there are reasonable grounds that evidence of a crime exists on a service provider's computer system or otherwise under the control of the service provider, the service provider shall preserve any and all relevant computer data, traffic data or subscriber information. 2. The service providers who are obliged to preserve computer data and/or traffic data as outlined in Paragraph 1 above shall preserve computer data or traffic data for 180 (one hundred and eighty) days. In case of necessity, the competent authority may request an extension of the data preservation period for one time only for an additional 180 (one hundred and eighty) days. 3. A prosecutor or an investigating judge may issue an order to preserve data relevant to a criminal investigation at any point during judicial proceedings. 4. The service providers or the persons who own the data as outlined in Paragraph 1 are obliged to effectively preserve such information in a confidential manner and not disclose or take any action which may disclose the preservation of such data to the subscriber or the suspect. 5. If the traffic data is in the possession of multiple providers, the service providers referred to in Paragraph 4 above shall be obliged to provide the necessary information to identify the service providers and the path through which the communication was transmitted. 6. The investigation of criminal offenses outlined in this law shall be in accordance with the Code of Criminal Procedure of the Kingdom of Cambodia."

ARTICLE 13

Article 13 provides the power to access records, data and other user information from service providers upon an order from a prosecutor or an investigating judge.[42] The records, data and other user information must be "necessary for a criminal investigation."

RECOMMENDATION: To conform with international human rights norms, Article 13 should be amended to include safeguards surrounding the use, safety and deletion of such data should be added.

ARTICLE 14

Article 14 authorizes the MOI to search and seize computer systems and computer data upon an order from a prosecutor on an investigating judge. Notably, under Article 14(3), the MOI is also empowered, while searching or seizing computer systems or data, to "render inaccessible or remove those computer data in the accessed computer system."[43]

Article 14 also lacks limits to the duration of the searching and seizing of computer data. Article 14 permits the MOI to remove or render inaccessible any data from a computer system. While it is likely permissible under international law to allow authorities to make data that is part of a criminal investigation inaccessible,[44] giving unfettered power to remove computer data without any oversight likely violates the right to privacy. The MOI, under Article 14, is able to permanently remove any data it wants. There are no criteria upon which such a determination is based and no requirement that the owner of such data actually committed any crime. In order to comply with international law, a better approach is for the Law to provide an avenue for such data to be returned or made accessible after the judicial process is completed.

---

[42] Law, Article 13: Order to provide data: "1. Upon a written request made by a judicial police officer which demonstrates that there exist reasonable grounds to believe that specified subscriber information, or specified data stored in a computer system or a computer data storage medium in the possession or control of a service provider, that is necessary for a criminal investigation, a prosecutor or an investigating judge may order such service provider to submit, produce or make available the specified stored data or such subscriber information to the judicial police officer. 2. The prosecutor or the investigating judge may also require that the recipient of the order and any person in control of the computer system shall keep confidential the existence of the production order."

[43] Law, Article 14: Search and seizure of computer data: "In order to search or gather the evidence necessary to investigate a crime in which a computer system or a computer data storage medium may contain evidence of that crime, the judicial police officers shall request an order from a prosecutor or an investigating judge to: - search or access a computer system or part of it and computer data stored therein; and - search or access a computer-data storage medium in which computer data may be stored - with such assistance as may be necessary using existing technical capability. 2. If during the search process as stated in Paragraph 1 above, the judicial police officers have reasonable grounds to believe that the data sought is stored in another computer system or part of it, and such data is connected to the initial system, the judicial police officers shall obtain an order from a prosecutor or an investigating judge authorizing a search of the other system prior to continuing to search or access the other system. 3. During the search process as stated in Paragraph 1 and Paragraph 2 above, the judicial police officers shall have the right to: - seize or secure a computer system or part of it or a computer-data storage medium identified in the prosecutor or investigating judge order; - make and retain a copy of those computer data; - maintain the integrity of the relevant stored computer data; - render inaccessible or remove those computer data in the accessed computer system 4. In case where the seizure of the equipment, devise or tool could adversely affect the operational capability of the owners of such items, the judicial police officers may make and retain a copy of the computer data without seizing said equipment, device or tool."

[44] *See, e.g.*, Budapest Convention, Article 19(3)(d): "render inaccessible or remove those computer data in the accessed computer system."

RECOMMENDATION: Article 14 should be revised to include adequate safeguards regarding the scope of data to be preserved, searched or seized, i.e., that data that is directly related to the commission of a criminal act. Article 14 should also be revised to: (a) limit the duration of the search or seizure of computer data; (b) limit when computer data can be removed or rendered inaccessible by the MOI; and (c) clarify when such data should be returned to its owner.

ARTICLE 15

Article 15 allows for the MOI to collect traffic data for an initial period of 14 days upon an order from a prosecutor or an investigating judge. However, under Article 15(2) the prosecutor or investigating judge can extend the time period "for a specific period of time."[45] This allows for data collection in perpetuity. Such collection is only available when the MOI is investigating "serious offenses."[46]

RECOMMENDATION: Article 15 should be revised to require meaningful judicial oversight before the collection of data, i.e., a higher judicial threshold. Article 15 should include a limited duration for the collection of data. Article 15 should include a definition of which criminal offenses allow for the MOI to undertake real-time collection of data, and limit such data to that which directly relates to the commission of an alleged criminal activity. Finally, Article 15 should be revised to include adequate safeguards regarding the use, preservation and deletion/destruction of collected data.

ARTICLE 16

Article 16 empowers the MOI to intercept "data content" upon an order from a prosecutor on an investigating judge for up to fourteen days. However, under Article 16(2) the prosecutor or investigating judge can extend the time period "for a specific period of time,"[47] which

[45] Law, Article 15: Collection of traffic data in a specific period: "1. After receiving a written application by a judicial police officer indicating that there are reasonable grounds to believe that traffic data associated with specified communications and related to or connected with the person under investigation is required for a criminal investigation, a prosecutor or an investigating judge may order the service provider to collect or record traffic data in real-time by technical means and provide only the specified traffic data to the judicial police officer. Such collection or recording of real-time traffic data shall not be ordered for a period beyond what is absolutely necessary and, in any event, not for more than 14 (fourteen) days. 2. Upon receiving a written application for an extension by a judicial police officer, a prosecutor or an investigating judge may authorize an extension for a further specified period. 3. This Article shall apply only to investigations related to serious offense. 4. A prosecutor or an investigating judge may also require the service provider to keep confidential the order to collect real-time traffic data"

[46] The term "serious offenses" is undefined.

[47] Law, Article 16: Interception of data content: "1. After receiving a written application by a judicial police officer indicating that there are reasonable grounds to believe that content data related to or connected with the person under investigation is required for a criminal investigation, a prosecutor or an investigating judge may order: a. the judicial police officer to collect or record through the application of technical means, content data, in real-time, of specified communications by means of a computer system; or b. a service provider, within its existing technical capability to collect, record, or cooperate and assist the judicial police officer in the collection or recording of content data, in real-time, of specified communications transmitted by means of a computer system. Such real-time collection or recording of real-time content data shall not be ordered for a period beyond what is absolutely necessary and, in any event, not for more than 14 (fourteen) days. 2. Upon receiving a written application for an extension by a judicial police officer, a prosecutor or an investigating judge may authorize an extension for a further specified period. 3.This Article shall apply only to investigations related to serious offenses or crimes related to national security. 4. A prosecutor or an investigating judge may also require the service provider to keep confidential the order to intercept content data."

allows for such interception to continue indefinitely. In addition, such interception is only available when the MOI is investigating "serious offenses or crimes related to national security."[48]

RECOMMENDATION: Article 16 should be revised to require meaningful judicial oversight before the collection of data, i.e. a higher judicial threshold. Article 16 should include a limited duration for the collection of data and a definition of which criminal offenses allow for the MOI to intercept data, and limit such data to that which directly relates to the commission of an alleged criminal activity. Finally, Article 16 should be revised to include adequate safeguards regarding the use, preservation and deletion/destruction of collected data.

UNREASONABLE OBLIGATIONS FOR SERVICE PROVIDERS

ISSUE: Articles 8 and 9 of the Law impose unreasonable obligations on service providers, which are likely to undermine the right to privacy.

DISCUSSION: Article 8 requires service providers to: (a) "accurately maintain and manage" registration and application form(s) from its users and (b) retain all "traffic data" for a period of at least 180 days and to have "sufficient technical expertise" to provide authorities with "subscriber information."[49] Failure of the service provider to retain all traffic data for 180 days is subject to a fine between 2,000,000 (two million) riels to 10,000,000 (ten million) riels.[50]

There are two main issues with Article 8. First, depending on how this article is interpreted, it could constitute an arbitrary interference with the right to privacy protected by the ICCPR.[51] It is unclear what exactly it means to "accurately maintain and manage the registration and application" of one's users.[52] If service providers are required to gather and store all sorts of personal identifying information, including one's real name, government identification number, date of birth, etc., then this would likely amount to a violation of the right to privacy protected by the ICCPR.

Anonymity has been recognized as an important component of safeguarding free expression, privacy, political accountability and public participation.[53] Every person has the right to

[48] The term "serious offenses" and "crimes related to national security" are undefined.
[49] Law, Article 8: Management of Subscriber Registration and Application: "Service providers shall: 1. Have an obligation to accurately maintain and manage the registration and applications of its subscribers. 2. Store traffic data for 180 (one hundred eighty) days. 3. Have sufficient technical expertise to research and provide subscriber information as requested by any authority authorized by law to request such information."
[50] Law, Article 25: Negligence of management of registration and subscriber applications: "Service providers who, by negligence, fail to manage the registration, applications, or data of users of their service as stated in Article 8 of this law shall be fined from 2,000,000 (two million) to 10,000,000 (ten million) Riels."
[51] ICCPR, Article 17, "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."
[52] Article 2(12) defines "Subscriber Information" as: "any information contained in any form which establishes the subscriber's identity such as name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address (including internet protocol address), and means and source of payment for such service (including any credit card or bank account number)." However it is not clear from the Law if service providers are required to obtain all of the data contained in the definition of "Subscriber Information."
[53] United Nations Human Rights Council, A/HRC/29/32, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" May 22, 2015, paras. 47.

communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies. To ensure compliance with the ICCPR, governments have an obligation to show that any interference with the right to privacy is neither arbitrary nor unlawful. Requiring all service providers to maintain undefined personal information of users constitutes an arbitrary interference with the right to privacy. The Special Rapporteur specifically noted that similar legislation in Iran and Russia, which require internet café users to register with their real names, constitutes a prohibition of anonymity online and, as a result is an impermissible interference with the freedom of expression and right to privacy.[54]

The second issue is that requiring the retention of all user data for 180 days establishes an environment for the bulk collection of private communications data, which could have a significant, negative impact on the freedom of expression and right to privacy. Bulk compulsory data retention increases the scope of State surveillance, increases business expenses, which lowers profits, and increases the likelihood that the data will be stolen, accidentally disclosed or used to commit fraud.[55] "States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption."[56]

RECOMMENDATION: To comply with international human rights norms:

- Article 8, paragraph 1 should be revised to make clear what types of information service providers are required to obtain from user applications and registration documents for internet service. The information required should be minimal and should allow for anonymous use of the internet.
- Article 8, paragraph 2 ("preserve traffic data for at least 180 (one hundred eighty) days") should be deleted as this creates an avenue for bulk collection of data and mass surveillance. (Articles 15 and 16 of the Law provide authorities with the ability to collect and intercept computer data during the course of law enforcement and judicial investigations). Alternatively, Article 8, paragraph 2 should be revised to require service providers to retain traffic data for a short period of time, such as 10 days. This amount of time would then enable authorities to investigate on-going crimes while complying with privacy rights.

OTHER ISSUES

- *Article 2* creates universal jurisdiction. The Law's scope is outlined in Article 2 as being "applicable to any cybercrime committed within or outside the territory of the Kingdom of Cambodia, which in any way infringes the security, public order or

[54] United Nations Human Rights Council, A/HRC/29/32, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" May 22, 2015, paras. 49-50.
[55] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 67.
[56] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 96.

interests of the Kingdom of Cambodia ."[57] This creates universal jurisdiction over every internet user, which is problematic for two main reasons. First, many internet users, especially those outside of Cambodia, will not be aware of this Law or its applicability. Second, the categories of offenses listed, those that "infringe the security, public order, or interests of the Kingdom of Cambodia," are so broad that nearly any discussion of Cambodia that includes negative attributes or any criticism could be categorized as an offense.

- *Article 30* prohibits the "Advertisement and mobilizing funds for purchase, sale, exchange or payment transactions of cryptocurrency via information technology without authorization or license from the competent authority…"[58] Cryptocurrency is a well-recognized method for payment used by businesses, governments, civil society organizations and individuals. Rather than issuing criminal sanctions for offering payment in cryptocurrencies, the RGC should create a regulatory framework that enables such payments to be conducted in a clear, transparent manner.

- *Article 32* prohibits unauthorized access to a computer or computer and doing so is a criminal offence.[59] The criminal penalties are increased if the "unauthorized access" occurs when done with an "intention of downloading, copying, using and/or transferring computer data (Article 32(2)); in violation of security measures (Article 32(3)) or on a computer system that is "classified as confidential or under special protection or related to national security or military confidential information, by means of secret linking or direct transferring or electromagnetic or other forms which are invisible…" (Article 32(4)).

  Article 32 is a reasonable restriction targeted at preventing hacking, installing malware, etc., and properly contains the *mens rea* of intention. However, the additional penalties for committing the actions noted in paragraphs 2, 3 and 4 seem to target journalists, whistleblowers and other watchdogs seeking to expose human rights violations, corruption or other abuses. Journalists and whistleblowers will often

[57] Law, Article 2.

[58] Law, Article 30: Cryptocurrency: "Advertisement and mobilizing funds for purchase, sale, exchange or payment transactions of cryptocurrency via information technology without authorization or license from the competent authority shall be punishable by a term of imprisonment from 6 (six) months to 5 (five) years and a fine from 10,000,000 (ten million) to 50,000 000 (fifty million) Riels."

[59] Law, Article 32: Unauthorized Access: "1. Any person who intentionally accesses the whole or any part of a computer system or without proper grounds or legal reasoning or authorization, shall be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine of 1,000,000 (one million) riels to 6,000,000 (six million) riels. 2. Any person who commits the act as provided for in Paragraph 1 above with the intention of downloading, copying, using and/or transferring computer data or information of owners without authorization, shall be punishable by an imprisonment from 1 (one) month to 3 (three) years and a fine of 2,000,000 (two millions) riels to 10,000,000 (ten million)s riels. 3. Any person who commits the act provided for in Paragraph 1 and/or Paragraph 2 above in violation of security measures, shall be punishable by an imprisonment from 6 (six) months to 5 (five) years and a fine from 8,000,000 (eight millions) riels to 24,000,000 (twenty-four millions) riels. 4. Any person who commits the acts as provided for in Paragraph 1 and/or Paragraph 2 above which are related to computer system, computer data, or security measures, classified as confidential or under special protection or related to national security or military confidential information, by means of secret linking or direct transferring or electromagnetic or other forms which are invisible, shall be punishable by an imprisonment from 2 (two) years to 10 (ten) years and a fine from 24,000,000 (twenty-four millions) riels to 100,000,000 (one hundred millions) riels."

need to access computer systems without express permission or use a program on computer to obtain relevant documents without authorization, and these actions will almost always be done in the performance of one's employment or work. Although States should curtail and criminalize illegal surveillance, laws should not target whistleblowers or others seeking to expose human rights violations or provide legitimate oversight of government actions. An exception should be made for whistleblowers.[60] Therefore, it is recommended that these articles be amended to excuse such actions if they are undertaken in "good faith" and do not harm the underlying computer systems.[61]

Conclusion

The Law is an improvement over earlier versions. However, it still contains several articles that are likely to restrict the freedom of expression or violate the right to privacy in contravention of international law and best practices. Many of the provisions that currently violate international law can be resolved relatively easily. If the Law is revised to include the outlined recommendations, it would not only comply with international law, but it would also provide the RGC with a solid legal framework to prevent, investigate and prosecute criminal activity in the cyber realm, while protecting the freedom of expression and right to privacy of all Cambodians.

ICNL remains available to provide technical assistance, as appropriate.
Respectfully submitted
September 14, 2022

[60] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 84.
[61] See e.g., The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, Joint Declaration December 6, 2004, p. 4 (2004).