IN THE CONSTITUTIONAL COURT OF THE REPUBLIC OF KOREA

Application Number 2016Heonma388

THIRD-PARTY INTERVENTION SUBMISSIONS BY ARTICLE 19

ARTICLE 19
Free Word Centre
60 Farringdon Road
London EC1R 3GA
United Kingdom
Tel: +44 207 324 2500
Fax: +44 207 490 0566
Web: www.article19.org

15 December 2016

I. INTRODUCTION

This amicus brief is submitted by ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) to assist the Constitutional Court of the Republic of Korea (Korea) in its consideration of the freedom of expression and privacy aspects in the above referenced case.

ARTICLE 19 believes that this case raises critical issues which fundamentally affect the extent to which the Korean legislation provides meaningful protection to individuals in the exercise of their freedom of expression and privacy rights. We are aware of the reports that communication surveillance is taking place in Korea at an alarming rate. It has been reported that in 2011 alone, communication metadata were seized for 37.3 million communication facilities – phone numbers, e-mail addresses or other accounts – and subscriber-identifying information was seized for 5.84 million facilities.[1] It is our understanding that the current legal framework allows for law enforcement to obtain much of these data without a warrant. Moreover, linking "anonymous" metadata with individual user identities can easily be done under the Telecommunications Business Act.[2]

According to the UN High Commissioner for Human Rights "even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy."[3]

To assist the Court in the case, this brief addresses three key areas:

a) Surveillance and the rights to freedom of expression and privacy under international human rights law;
b) Compliance of Articles 83(3) and 83(4) of the Telecommunications Business Act with the international standards on the right to freedom of expression; and
c) Compliance of Articles 83(3) and 83(4) of the Telecommunications Business Act with the international standards on the right to privacy.

II. INTEREST OF ARTICLE 19

ARTICLE 19 is an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends, and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally. ARTICLE 19 is a registered UK charity (No. 32741), with the international office in London and with regional offices in Bangladesh, Myanmar, Kenya, Senegal, Tunisia, Mexico, USA and Brazil.

---

[1] Park, Kyung Sin, Communication Surveillance in Korea (December 1, 2014). Korea University Law Review, Vol. 16-17, May 2015, pp. 53-72. Available at SSRN: https://ssrn.com/abstract=2748318.

[2] Telecommunications Business Act, Act. No. 3686, Dec. 30, 1983; see Communication Surveillance in Korea, *op.cit.,* at p. 60-61.

[3] The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, A/HRC/27/37, para 20, available at http://bit.ly/1yqH5yH.

III. MASS SURVEILLANCE, FREEDOM OF EXPRESSION AND PRIVACY

The right to freedom of expression

Freedom of expression is one of the bedrock principles of democracy and human rights. It has consistently been described as "one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfillment".[4] The UN Human Rights Committee further stated that freedom of expression is "a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights."[5]

The right to freedom of expression is strongly protected under Article 19 of the International Covenant on Civil and Political Rights[6] ("ICCPR"), which Korea ratified in 1990.[7] The right is further recognized worldwide by the Universal Declaration of Human Rights[8] ("UDHR", Article 19) and protected under regional human rights instruments such as the European Covenant on Human Rights[9] (Article 10), American Convention on Human Rights[10] (Article 13), African Charter on Human and Peoples' Rights[11] (Article 9), and the ASEAN Human Rights Declaration[12] (Article 23).

The right to freedom of expression may only be restricted under limited circumstances

The right to freedom of expression may only be restricted if specific conditions are met, set out in Article 19(3) of the ICCPR:[13]

- The restrictions must be "provided by law";
- Restrictions may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3 of Article 19: respect for the rights or reputations of others, and the protection of national security, public order (*ordre public*), public health or morals; and
- The restrictions must conform to the strict tests of necessity and proportionality.

These conditions are cumulative: all parts of this three-part test must be met in order for a restriction to the right to freedom of expression to be permissible under international law.

---

[4] European Court of Human Rights, *Lingens v. Austria*, Application no. 9815/82, 8 July 1986, available at http://bit.ly/2gBmi7B.
[5] UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression ("General Comment 34"), 12 September 2011, CCPR/C/GC/34, para 2-3, available at http://bit.ly/1xmySgV.
[6] ICCPR, 16 December 1966, UN Doc. A/6316 (1966), available at http://bit.ly/1bNeudO.
[7] See http://indicators.ohchr.org/.
[8] UDHR, 10 December 1948, GA res. 217A (III), UN Doc A/810 at 71 (1948), available at http://bit.ly/1kYiZcO.
[9] European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5, available at http://bit.ly/2hxcWvH.
[10] American Convention on Human Rights, 12 November 1969, OAS Treaty Series No. 36, available at http://bit.ly/2hFPYoV.
[11] African (Banjul) Charter on Human and Peoples' Rights, 27 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, available at www.achpr.org/instruments/achpr/.
[12] ASEAN Human Rights Declaration, 18 November 2012, available at http://bit.ly/2hFOmM9.
[13] General Comment 34, *supra* note 5, para 22.

For a norm to be characterised as "law" it needs to be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public.[14] It needs to provide sufficient guidance to those charged with its execution to enable them to determine what type of expression is restricted and what is not. Importantly, the UN Human Rights Committee states: "A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[15]

On the requirement of a legitimate aim for the restriction, the Necessary & Proportionate Principles,[16] developed by civil society, privacy and technology experts to apply existing human rights law to the modern-day reality of technology and surveillance, state that:

> Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

To meet the requirement of necessity and proportionality, the restriction must be necessary for a legitimate purpose and not be overbroad. The UN Human Rights Committee specified this as follows:

> [R]estrictive 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 their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law.[17]

The Necessary & Proportionate Principles apply the requirement of necessity and proportionality to surveillance in the following manner:

> Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.[18]

The right to privacy

The right to privacy is well-established under international law. It is internationally recognised by Article 12 of the Universal Declaration of Human Rights and Article 17 of the ICCPR. It is further protected under the following regional human rights instruments: the European

[14] General Comment 34, *op.cit.*, para 24.
[15] *Ibid*.
[16] Necessary and Proportionate Coalition, Necessary & Proportionate ("Necessary & Proportionate"), May 2014, available at http://bit.ly/2hOmbqi.
[17] UN Human Rights Committee, General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9, par. 14, available at http://bit.ly/1KcMQDE. See also General Comment 34, *op.cit.*, para 34.
[18] Necessary & Proportionate, *op.cit*.

Convention on Human Rights (Article 8), the American Convention on Human Rights (Article 11), and the ASEAN Declaration (Article 21).

The right to privacy may only be restricted under limited circumstances

The wording of Article 17 ICCPR prohibits "arbitrary and unlawful" interferences with the right to privacy. Under international human rights law, restrictions to the right to privacy can only be permissible if the same test as that which is applicable to Article 19 of the ICCPR, is met. The UN Special Rapporteur on promotion and protection of human rights while countering terrorism stated this as follows:

> Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17. Consequently, limitations to the right to privacy or other dimensions of article 17 are subject to a permissible limitations test, as set forth by the Human Rights Committee in its general comment No. 27.[19]

This has also been clearly set out by the UN Human Rights Committee[20] and UN Commission on Human Rights.[21]

The Necessary & Proportionate Principles set out in a detailed manner what the requirement of proportionality entails in the surveillance context, given the grave interference with the right to privacy that it constitutes:

> Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.
>
> This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:
>
> - there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;
> - there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;

[19] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 28 December 1999, A/HRC/13/37, available at http://bit.ly/23NMPpo.
[20] UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available at http://bit.ly/1JWQHZZ.
[21] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4, available at http://bit.ly/1SNYFo9.

- other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and;
- information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
- any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
- information is will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
- that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.[22]

The right to freedom of expression and the right to privacy are intertwined

Without adequate protection of the right to privacy, the right to freedom of expression is also harmed. The UN Special Rapporteur on the right to freedom of opinion and expression put it as follows:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.
>
> In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks.[23]

ARTICLE 19 submits that Article 84(3) and 83(4) of the Telecommunications Business Act must be reviewed for their compliance with these standards. We do this in the following sections.

IV. ARTICLES 83(3) AND 83(4) OF THE TELECOMMUNICATIONS BUSINESS ACT VIOLATE THE RIGHT TO FREEDOM OF EXPRESSION

As set out in the previous section, the right to freedom of expression may only be restricted if the conditions of legality, necessity and proportionality are met, and if the restriction pursues a legitimate aim. Articles 83(3) and 83(4) of the Telecommunications Business Act fail to meet these international standards as follows.

[22] Necessary & Proportionate, *op.cit.*
[23] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, A/HRC/23/40, para 79-80, available at http://bit.ly/1ot3aYJ.

Legality

In order for legislation to meet the "provided by law" criterion, the law must be "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly."[24] It may not "confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[25]

Under the Telecommunications Business Act, telecommunications business operators may be asked by a court, prosecutor, head of an investigative agency or the head of an intelligence and investigation agency to provide the personal data of its users if the person making the request "intends to collect information or intelligence in order to prevent any threat to a trial, an investigation (including the investigation of a violation committed by means of a telephone, the Internet, etc. among the offences prescribed in Article 10 (1), (3) and (4) of the Punishment of Tax Evaders Act), the execution of a sentence or the guarantee of the national security."[26]

ARTICLE 19 finds that this wording is overly broad and gives unfettered discretion to the authorities in question to request a wide range of user data. According to Article 83(3), the authority making the request only needs to "intend" to collect the information for the objectives listed in the law – there is no need for them to demonstrate that the collected data will actually be used for this stated purpose, nor is there a requirement to demonstrate afterwards that the data have indeed been used for this intended purpose.

Moreover, the data can be requested in the context of "any threat" to a trial, investigation, execution of a sentence or the guarantee of national security. The wording "any threat" creates a limitless category of instances in which personal data can be requested, giving the authorities unfettered discretion as to when they can use their powers under the law. There is no requirement for a threat to be credible, for a threat to be able to cause any concrete harm, nor for the authorities to show any proof for the actual existence of the threat.

Due to its overly broad wording, which gives unfettered discretion to the authorities to request personal data, we respectfully submit that Article 83(3) fails to meet the "prescribed by law" criterion of Article 19(3) ICCPR.

Legitimate aim

Article 83(3) allows authorities to request user data from a telecommunications business operator on the grounds of "any threat to... the guarantee of the national security." While national security is indeed one of the legitimate aims for the restriction of the right to freedom of expression listed in Article 19(3) of the ICCPR, there is still a requirement for the scope of the law to be defined with sufficient precision. The UN Human Rights Committee stated that:

> Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security ... are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of

[24] General Comment No 34, *op.cit.*
[25] *Ibid*.
[26] Telecommunications Business Act, *op.cit,* Article 83(3).

> legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. Nor is it generally appropriate to include in the remit of such laws such categories of information as those relating to the commercial sector, banking and scientific progress.[27]

The UN Special Rapporteur on freedom of opinion and expression has stated that, while the use of communications surveillance technologies may exceptionally be justified by the protection of national security, such measures must still be necessary, legitimate and proportionate.[28]

In a joint declaration, the UN Special Rapporteur on the right to freedom of opinion and expression and the Special Rapporteur for freedom of expression of the Inter-American Commission on Human Rights stated the following on the need for national security to be clearly defined:

> When national security is invoked as a reason for the surveillance of correspondence and personal information, the law must clearly specify the criteria to be used for determining the cases in which such surveillance is legitimate. Its application shall be authorized only in the event of a clear risk to protected interests and when the damage that may result would be greater than society's general interest in maintaining the right to privacy and the free circulation of ideas and information.[29]

Again, ARTICLE 19 finds that allowing authorities to request personal data on the grounds of "any threat" to national security, instead of a specific and narrowly defined one, does not meet the relevant standards under international human rights law.

Necessity and proportionality

Article 83(3) allows for the request of a wide range of personal data: user names, resident registration numbers, addresses, phone numbers, passwords and subscription information.[30] While Article 83(4) requires motivation of the request and an explanation of the scope of "necessary data" in writing, that same provision allows to forego this requirement due to "an urgent reason".[31] Without further defining what qualifies as an "urgent reason" (the overly broad wording of which also violates the legality requirement, set out above), the law leaves open the possibility for a maximum scope of data to be requested without the need for any motivation, written or unwritten, to first be provided.

As stated by the UN Human Rights Committee:

> When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat,

[27] General Comment 34, *op.cit.*, para 30. See also Article 19, The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1 October 1995, available at http://bit.ly/1Oi176F.
[28] Report of the Special Rapporteur on freedom of expression, 17 April 2013, *op.cit.,* para 3 and 58-60.
[29] UN Special Rapporteur on Freedom of Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Joint Declaration on surveillance programs and their impact on freedom of expression, 21 June 2013, available at http://bit.ly/2h16k7M.
[30] Telecommunications Business Act, *op.cit.*, Article 83(3).
[31] *Ibid*.

> and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.[32]

The requirement in Article 83(4) to file a written request once the "urgent reason" has disappeared provides no solace; since there is a complete lack of clarity as to which reasons qualify for this exemption, no need to motivate their invocation, and no supervisory mechanism exists, the authorities can easily argue that such reasons remain in existence for an indefinite period of time, exempting them from ever having to submit a motivation for the data request. Moreover, once the data have been obtained, the violation of the data subject's rights has already taken place – the harm has already been done.

By not requiring the authorities to demonstrate that their data requests comply with the principles of proportionality and necessity, ARTICLE 19 submits that Articles 83(3) and 83(4) violate the necessity and proportionality requirements of Article 19(3) ICCPR. In addition, the overly broad wording of Article 83(4) violates the legality requirement.

Surveillance has a chilling effect on freedom of expression

In addition to Article 83(3) and 83(4) not meeting the criteria by which expression can lawfully be restricted under international human rights law, the existence of surveillance practices in and of itself has a chilling effect on the right to freedom of expression.[33] In the words of the UN Special Rapporteur on freedom of opinion and expression:

> Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.[34] … States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy.[35]

We would also like to draw the attention of the Court to the 2014 report of PEN International and Human Rights Watch on the impact of surveillance on journalists and lawyers in the United States. The report found that the revelations of mass surveillance taking place in the country had a significant impact on individuals, journalists and lawyers:

> [E]arly research indicates that the revelations in 2013 and continuing to date have begun to have a chilling effect on private individuals' electronic communications practices and activities. And, as this report documents, surveillance can have a profound impact on the practice of journalism and law.[36]

With surveillance in Korea taking place on a scale that is multi-fold that of the US,[37] ARTICLE 19 believes that this will inevitably have a considerable negative impact on the exercise of the right to freedom of expression in the country. In this context, it is important to recall the

[32] General Comment 34, *op.cit.*, para 35. See also Necessary & Proportionate, *op.cit.*.
[33] The right to privacy in the digital age, *op.cit.*
[34] Report of the Special Rapporteur on freedom of expression, 17 April 2013, *op.cit.,* para 52.
[35] *Ibid.*, para 79.
[36] Human Rights Watch and PEN International, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy, July 2014, p. 18, available at http://bit.ly/UBzQ8b.
[37] Park, Kyung Sin, Communication Surveillance in Korea, *op.cit.*, at p. 53-55.

obligations of States Parties under the ICCPR:

> The obligations of the Covenant in general and article 2 in particular are binding on every State Party as a whole. All branches of government (executive, legislative and judicial), and other public or governmental authorities, at whatever level - national, regional or local - are in a position to engage the responsibility of the State Party.[38]

Korea therefore has an obligation not only to ensure that its laws facilitate the enjoyment of the right to freedom of expression, but also to ensure that all public authorities, including those currently authorized to request the personal data of telecommunications users, act in accordance with Korea's obligations under Article 19 and 17 of the ICCPR.

V. ARTICLES 83(3) AND 83(4) OF THE TELECOMMUNICATIONS BUSINESS ACT VIOLATE THE RIGHT TO PRIVACY

As set out above, the right to privacy can only be lawfully restricted under international human rights law when those restrictions meet the criteria of legality, necessity and proportionality, and the restrictions take place in the pursuit of a legitimate aim. The foregoing section on freedom of expression therefore applies similarly to the right to privacy, and the conclusion must be drawn that Articles 83(3) and 83(4) of the Telecommunications Business Act constitute an unlawful and arbitrary interference with the right to privacy as protected by Article 17 of the ICCPR.

Two additional points relevant to the right to privacy need to be highlighted in this context: the absence in Articles 83(3) and 83(4) of the Telecommunications Business Act of a requirement for a warrant to obtain user data, and the absence of a notification requirement to users of telecommunication services whose data have been provided to the authorities.

Obtaining user data should require a warrant

International law requires that the use of surveillance powers by public officials must not only be necessary and proportionate, but also be subject to independently oversight to safeguard against abuse. The Necessary & Proportionate Principles state that "Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent."[39] This is related to the principle of due process, meaning that surveillance decisions must not only be made in accordance with the law, but also in a manner that is compatible with the fundamental rights of the data subject:

> Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a

[38] UN Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, par. 4, available at http://bit.ly/1pCTdpl.
[39] Necessary & Proportionate, *op.cit.*

> reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.[40]

The UN Human Rights Committee has stated clearly that Article 83(3) of the Telecommunications Business Act, which allows the authorities to obtain personal data without a warrant, runs counter to these fundamental principles of international human rights law:

> The Committee notes with concern that, under article 83 (3) of the Telecommunications Business Act, subscriber information may be requested without a warrant by any telecommunications operator for investigatory purposes. It is also concerned about the use and insufficient regulation in practice of base station investigations of mobile telephone signals picked up near the site of demonstrations in order to identify participants, and about the extensive use and insufficient regulation in practice of wiretapping, in particular by the National Intelligence Service (arts. 17 and 21).
>
> The State party should introduce the legal amendments necessary to ensure that any surveillance, including for the purposes of State security, is compatible with the Covenant. It should, inter alia, ensure that subscriber information may be issued with a warrant only, introduce a mechanism to monitor the communication investigations of the National Intelligence Service, and increase the safeguards to prevent the arbitrary operation of base station investigations.[41]

Notification of data transfer should be required

The principle of user notification not only relates to the right to privacy, but is also part of the right to a fair trial and the right to an effective remedy. The right to a fair trial is guaranteed under Article 14 of the ICCPR and Article 10 of the UDHR. It is also guaranteed in the regional human rights instruments: the European Convention on Human Rights (Article 6), the American Convention on Human Rights (Article 8), the African Charter on Human and Peoples' Rights (Article 7), and the ASEAN Declaration (Article 20).

The Necessary & Proportionate Principles summarise the respective requirements as follows:

> Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:
>
> - Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and
> - Authorisation to delay notification is granted by a Competent Judicial Authority; and
> - The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority. The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.[42]

[40] *Ibid*.
[41] UN Human Rights Committee, Fourth periodic report submitted by the Republic of Korea, 3 December 2015, CCPR/C/KOR/4, par 42-43, available at http://bit.ly/2gBv712.
[42] Necessary & Proportionate, *op.cit.*

The principle of user notification requires that the authorities notify the data subject in time for them to challenge the surveillance decision. A delay (note: not absence) of notification is only possible under narrow circumstances, when authorised by a competent judicial authority. The Telecommunications Business Act currently does not require any notification of the data subject at all, resulting in a significant infringement of their right to a fair trial and their right to privacy. In addition, the lack of a notification requirement violates the general principle of transparency, as a complete absence of notification deprives the general public of the opportunity to assess if Korea's surveillance practices are being performed in compliance with its obligations under international human rights law.

VI. CONCLUSION

In light of the foregoing, ARTICLE 19 respectfully submits that Articles 83(3) and 83(4) of the Telecommunications Business Act do not comply with Korea's obligations under international human rights law, in particular the right to freedom of expression and the right to privacy. ARTICLE 19 suggests that the Constitutional Court of Korea take the relevant standards into account when considering the Constitutional challenge currently brought before it.

JUDr Barbora Bukovska

Senior Director for Law and Policy
ARTICLE 19