IN THE CONSTITUTIONAL COURT OF THE REPUBLIC OF KOREA

Application Number 2016Heonma388

THIRD-PARTY INTERVENTION SUBMISSIONS BY PRIVACY INTERNATIONAL

PRIVACY INTERNATIONAL
62 Britton Street
London EC1M 5UY
United Kingdom
Tel: +44 20 3422 4321
www.privacyinternational.org

10 April 2017

I. INTRODUCTION

1. Privacy International submits this intervention to assist the Constitutional Court of the Republic of Korea ("Korea") in its consideration of the rights to privacy and freedom of expression as they relate to Articles 83(3) and 83(4) of the Telecommunications Business Act. In particular, Privacy International highlights the importance of anonymity to the exercise of both rights and how the Act interferes with the anonymity and anonymous speech of millions of Koreans.

II. INTEREST OF PRIVACY INTERNATIONAL

2. Privacy International is a non-profit, non-governmental organization based in London, the United Kingdom ("UK"), which defends the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened as *amicus curiae* in cases implicating the right to privacy in courts around the world, including in the United States, the UK and Europe. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect this right. It also strengthens the capacity of privacy organizations in developing countries to identify and defend against threats to privacy.

III. ARGUMENT

A. THE IMPORTANCE OF ANONYMITY AND ANONYMOUS SPEECH

3. Anonymity and anonymous speech has played a foundational role in human history.[1] Anonymity is one of the essential tools available to individuals to mitigate or avert unlawful interferences with their rights to privacy and free expression, and it has long been a means by which individuals could enjoy their right to impart and receive information free from state control. As such, anonymity, which has traditionally been linked to the right to privacy,[2] is also an important safeguard for the exercise of the right to freedom of expression.[3]

4. "At its simplest, anonymity is *the fact* of not being identified and, in this sense, it is part of the ordinary experience of most people on a daily basis, e.g. walking as part of a crowd or

[1] See generally *Anonymity as a Legal Right: Where and Why It Matters*, 16 N.C. J.L. & Tech. 311, 317-331 (2015) (discussing the historical importance of anonymity to freedom of expression).
[2] See *Rotaru v. Romania*, Application no. 28341/95 (4 May 2000), para. 42, where the European Court of Human Rights stated that anonymity is inherent to an individual's private life as protected by Article 8 of the European Convention on Human Rights.
[3] Article 19, Right to Online Anonymity (18 June 2015), p. 1, available at https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.

standing in a queue of strangers."[4] As such, "an activity can be anonymous even though it is also public."[5] That one can be both public and maintain her identity as secret is the very benefit of anonymity—it is what allows individuals to freely engage in works that critique governments or powerful actors, or expose wrongdoings.[6]

5. It is in this context that the European Court of Human Rights has emphasised the importance of anonymity as "a means of avoiding reprisals or unwanted attention" and thereby "capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet."[7] The Supreme Court of the United States has also characterised anonymous speech "as an honorable tradition of advocacy and of dissent" and observed that it acts as "a shield from the tyranny of the majority."[8] It has further identified anonymity's historical significance:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies, was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers.[9]

6. Anonymity has given individuals throughout history a necessary cloak with which to shield themselves from reprisal – reprisal from the state, their fellow countrymen and women, or would-be oppressors located anywhere in the world.[10] These individuals may be whistleblowers, who seek to expose the latest abuse of power by a government agency or private company. They may be dissidents, who seek to expand the channels of governance to include the dispossessed. They may be sources for journalists, who provide the necessary informational inputs to facilitate transparency and scrutiny of public and private institutions. Or they may be everyday people who are not comfortable discussing their trials and

---

[4] *Id*. at p. 10.
[5] *Id*.
[6] Privacy International, Securing Safe Spaces Online, p. 8 (June 2015), available at: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf.
[7] *Delfi AS v. Estonia*, Application no. 64569/09 (16 June 2015), para. 147.
[8] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), p. 357.
[9] *Talley v. California*, 362 U.S. 60 (1960), pp. 64-65.
[10] See Privacy International, Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications (February 2015), p. 2, available at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/PrivacyInternational.pdf. See also Electronic Frontier Foundation, Anonymity, https://www.eff.org/issues/anonymity.

tribulations without the layer of protection that anonymity provides.[11] For all of these speakers, anonymity "protects the freedom of individuals to live their lives without unnecessary and undue scrutiny."[12] It is perhaps unsurprising, then, that "[a]nonymity is a deeply held value for many internet users and has contributed to a robust internet public sphere."[13]

7. Anonymity and anonymous speech are particularly threatened in the modern world, where the advent of the internet and advancements in modern technologies have revolutionized the way we communicate.[14] People around the world, but also Koreans in particular, live major portions of their lives online.[15] They use the internet to impart ideas, conduct research, communicate with loved ones and express political and personal views. They also use it to conduct many of their daily activities, such as keeping records, arranging travel and conducting financial transactions. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into personal and professional lives. These devices have replaced and consolidated fixed-line telephones, filing cabinets, photo albums and address books.

8. The internet has not only dramatically changed the way people communicate but also increased the frequency of communications and enabled the creation of greater quantities of personal data about communications, known as "communications data" or "metadata." Communications data is information about a communication, which may include the sender and recipient, the date and location from where it was sent, and the type of device used to send it. In the digital realm, communications data can also record much more, for example, your web browsing activities, which might reveal medical conditions, religious viewpoints or political affiliations. Items purchased, news sites visited, forums joined, books read, movies watched and games played – each of these pieces of communications data gives us insight into a person.

---

[11] See Gabriela Coleman, Anonymity Online Serves Us All, N.Y. Times (20 Aug. 2014), available at: http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls/anonymity-online-serves-us-all. The op-ed discusses equally significant but more common forms of anonymous speech, such as "medical patients and mothers [who] discuss sensitive issues (be they clinical or related to parenting) in pseudonymous forums, . . . [a]nd . . . victims of hate crimes [who] use anonymity to speak out as well: anonymity can empower those who seek consolation and justice to speak out against assailants enabled by the same processes."

[12] Article 19, Right to Online Anonymity, *supra* note 3, at p. 10.

[13] Privacy International, Securing Safe Spaces Online, *supra* note 6, at p. 8.

[14] See United Nations, Human Rights Council (2014), 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. 1 (discussing the omnipresence of modern digital communications technology), available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.

[15] See FRONTLINE/World, South Korea: The Most Wired Place on Earth, PBS, Apr. 14, 2009, available at http://www.pbs.org/frontlineworld/stories/south_korea802/.

9. Pieced together, communications data allows an intrusive and comprehensive view into a person's life, revealing his or her relationships, interests, location and activity. But importantly, subscriber data, by linking identifying information with communications data (and other sources of data), makes it easier to identify exactly who this person is. Once obtained, subscriber data can be used, for example, to tie specific individuals to particular conversations, locations and times – all the government needs to do is correlate an individual's name with a phone number and other communications data that has already been collected by its authorities. Thus, a detailed portrait of unknown person "x" becomes a detailed portrait of a specific person known to the government.

10. Because of anonymity's importance to the ability to live a full private life and to the free exchange of ideas, courts and human rights experts have started evaluating interferences with anonymity under relevant human rights standards – e.g., legality, necessity, and proportionality – and have required strict procedural safeguards to protect people if the interference is to be permitted.[16]

B. INTERNATIONAL LEGAL AUTHORITIES HAVE MOVED TOWARDS RECOGNISING ANONYMITY AS A RIGHT UNDER THE RIGHTS TO PRIVACY AND FREEDOM OF EXPRESSION

11. International law experts have long argued that interferences with anonymity should be analysed under relevant human rights standards.

12. Both the current and prior Special Rapporteurs to the United Nations on the promotion and protection of the right to freedom of opinion and expression have been steadfast proponents of anonymity as part of the right to freedom of expression. As early as 2011, Special Rapporteur Frank La Rue identified the interplay between the right to privacy and the right to freedom of expression online[17] and emphasised that any interference with anonymity should be subject to the same three part test of legality, necessity, and proportionality as any other interference with freedom of expression.[18]

[16] Article 19, Right to Online Anonymity, *supra* note 3, at p. 22-23.
[17] United Nations, Human Rights Council (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para. 53 ("The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."), available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[18] *Id*. at paras. 24, 59.

13. In 2013, Special Rapporteur La Rue elaborated on his 2011 report. He reemphasised the interconnected nature of the rights to privacy and freedom of expression and noted the need "to ensure the privacy, security and *anonymity* of communications."[19]

14. Special Rapporteur La Rue rightly noted that "[o]ne of the most important advances facilitated by the advent of the Internet was the ability to anonymously access and impart information, and to communicate securely without having to be identified," but that "in the name of security and law enforcement, gradually States have been eradicating the opportunities for anonymous communication."[20] He specifically identified how increasingly "identification and registration are . . . required when buying a SIM card or mobile telephone device, for visiting certain major websites, or for making comments on media sites or blogs."[21] The Special Rapporteur concluded that "restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas," which "can also result in individuals' de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities."[22]

15. The current Special Rapporteur, David Kaye, has built upon his predecessor's recommendations. He has emphasised the same interconnectedness between anonymity and the rights to privacy and freedom of expression.[23] He has also reinforced that interferences with anonymity are subject to a human rights analysis,[24] and emphasised that "[c]orporate actors should . . . consider their own policies that restrict encryption and anonymity."[25] Finally, Special Rapporteur Kaye stressed that there must be a remedy available to individuals affected by such measures and that "[i]n order for the right to a remedy to be meaningful, individuals must be given notice of any compromise of their privacy."[26]

16. Like the U.N.'s Special Rapporteurs, Catalina Botero Marina, the Special Rapporteur for Freedom of Expression to the Inter-American Commission on Human Rights, published a report in 2013 making many of the same observations about the importance of anonymity to

---

[19] United Nations, Human Rights Council (2013), 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, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (emphasis added).
[20] *Id*. at para. 47.
[21] *Id*.
[22] *Id*. at para. 49.
[23] United Nations, Human Rights Council (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 22 May 2015, A/HRC/29/32, para. 16, available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.
[24] *Id*. at para. 31 ("Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.").
[25] *Id*. at para. 60.
[26] *Id*. at para. 18.

privacy and freedom of expression. She noted that "online spaces where people's activities and identities are not observed or documented should be promoted" and that this interest "is closely linked to the State's obligation to create a safe environment for the exercise of freedom of expression, as violation of communication privacy has a chilling effect and hampers the full exercise of the right to communicate."[27] She also recognised that in certain circumstances "judicial authorities would be authorised to take reasonable measures to determine the identity of the sender engaged in prohibited acts, in order to take proportionate action in response, as provided by law."[28]

17. In 2003, the Committee of Ministers of the Council of Europe adopted a Declaration on freedom of communication on the Internet.[29] One of the seven principles concerned anonymity:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

18. In the commentary supporting the principles, the Committee noted that the "aim of this principle is first and foremost to underline that the will of users to remain anonymous should be respected."[30] The Committee recognised that "users may have a valid reason not to reveal their identity when they have statements published on the Internet" and that "[o]bliging them to do so could restrict excessively their freedom of expression."[31] The Committee also observed that "users need protection against unwarranted on-line surveillance by public or private entities."[32]

19. Since then, in Europe, the law's treatment of anonymity and anonymous speech has expanded and been refined. The European Court of Human Rights had reason to consider the Committee of Ministers' 2003 Declaration and the issue of anonymity in *Delfi AS v. Estonia*. The Court reaffirmed the importance of anonymity to online speech and described various types of anonymity available to users of the internet. It also highlighted certain procedural

---

[27] Inter-American Commission on Human Rights (2013), Freedom of expression and the Internet, Catalina Botero Marina, 31 December 2013, OEA/Ser.L/V/II, para. 23, available at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.
[28] *Id*. at para 135.
[29] Council of Europe, Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies), available at: http://portal.unesco.org/ci/en/files/25147/11861368651Declaration-Inf(2003)007.pdf/Declaration-Inf(2003)007.pdf.
[30] *Id*. at p. 12.
[31] *Id*.
[32] *Id*.

safeguards that protect the release of identifying information – for example, "[t]he release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions."[33]

20. In light of the breadth of international authorities that recognise anonymity and its role in ensuring the rights to privacy and freedom of expression, Privacy International submits that this Court should evaluate any law that restricts anonymity, like Articles 83(3) and 83(4) of the Telecommunications Business Act, under the international human rights framework for assessing interferences with these rights.

C. THE INTERPLAY BETWEEN ARTICLES 83(3) AND 83(4) OF THE TELECOMMUNICATIONS BUSINESS ACT AND ANONYMITY

21. Pursuant to Article 83(3), a telecommunications business operator may comply with a request for "communications data" from a court, prosecutor, head of an investigative agency (including the Commissioners of the National Tax Service and Regional Tax Office), or head of an intelligence agency where the data is for the purpose of preventing a threat to a trial, investigation, execution of a sentence or national security.

22. The Telecommunications Business Act defines "communications data" as:[34]

1. Names of users;
2. Resident registration numbers of users;
3. Addresses of users;

[33] *Delfi AS v. Estonia*, Application no. 64569/09 (16 June 2015), para. 148.

[34] What the Telecommunications Business Act describes as "communications data" is commonly referred to as "subscriber data" or "subscriber information." See, for example, Article 18.3 of the Budapest Convention, which defines "subscriber information" as:

> any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
>
> a. the type of communciation service used, the technical provisions taken thereto and the period of service;
>
> b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
>
> c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Privacy International uses the term "subscriber data" – rather than "communications data" – to refer to the information that can be requested from telecommunications business operators under Articles 83(3) and 83(4) of the Telecommunications Business Act.

4. Phone numbers of users;
5. User identification codes;
6. Subscription and termination dates of service

23. Article 83(4) provides that requests for "communications data" are to be made in writing, stating a reason for the request, relationship with the relevant user, and the scope of the data requested, unless rendered impossible due to urgent circumstances.

24. Articles 83(3) and 83(4) of the Telecommunications Business Act amount to a general measure that undermines the anonymity and anonymous speech of Koreans and thereby their rights to privacy and freedom of expression. On its face, it gives telecommunications operators virtual carte blanche to turn over the subscriber data of their users upon a simple written request from a variety of government bodies. As discussed above, by turning over subscriber data to the government, companies permit the government to tie identifying information to other sources of personal data, facilitating serious interferences with the rights to privacy and freedom of expression.[35]

25. In Korea, those interferences occur at a mass scale. According to a 2016 report by the Korean Ministry of Science, ICT and Future Planning, in 2015, government authorities seized the subscriber-identifying information for 10,577,079 communication devices and the metadata records for 5,484,945 instances of communication.[36] By linking these sources of data together, the Korean government could easily and reasonably build detailed profiles of millions of its citizens.

D. ARTICLES 83(3) AND 83(4) OF THE TELECOMMUNICATIONS BUSINESS ACT VIOLATE THE RIGHTS TO PRIVACY AND FREEDOM OF EXPRESSION

26. It is a well-established principle that interferences with the rights to privacy and freedom of expression in some form may be necessary to combat criminal offences and genuine threats to national security. But because surveillance interferes with these rights, it must therefore also be subject to the principles of legality, necessity and proportionality. For the reasons set

[35] International data protection standards recognize that subscriber data itself amounts to "personal data." For example, Article 4 of the the European Union's General Data Protection Regulation ("GDPR") defines personal data as "any information relating to an identified or identifiable natural person" and "identifiable natural person" as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Article 4(1), EU GDPR. As such, the processing – which includes collection and disclosure – of subscriber data can and should be subject to certain safeguards. See generally EU GDPR.

[36] The report is available on the website of the Ministry of Science, ICT and Future Planning at this link: http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1316113&snsMId=NzM%3D&getServerPort=80&snsLinkUrl=%2Fweb%2FmsipContents%2FsnsView.do&getServerName=www.msip.go.kr.

forth in Article 19's submission to the Constitutional Court, Articles 83(3) and 83(4) of the Telecommunications Business Act fail to meet these requirements.[37]

27. Articles 83(3) and 83(4) of the Telecommunications Business Act also lack certain additional safeguards to render these provisions compliant with international human rights law. Article 19's submission highlights two such safeguards – (1) a requirement that the government obtain a warrant prior to requesting subscriber data from telecommunications operators and (2) notification to users whose subscriber data has been provided to the government.

28. Privacy International reiterates the need for effective safeguards to govern government access to the subscriber data of Koreans and highlights several additional authorities to buttress Article 19's analysis.

1. Prior Independent Authorization

29. Privacy International notes two recent cases of the Court of Justice of the European Union ("CJEU"), which discuss the importance of independent authorization prior to government access to communications data held by telecommunications operators. Privacy International recognizes that the present case involves access to subscriber data, rather than communications data. However, the significant implications for anonymity (and therefore the rights to privacy and freedom of expression) raised by government access to subscriber data – particularly when paired with communications data – suggest the need for similar safeguards.

30. In *Digital Rights Ireland*, the Grand Chamber of the CJEU concluded that the 2006 Data Retention Directive of the EU, which required communications service providers to retain customer communications data in bulk for up to two years for the sake of preventing and detecting serious crime, breached the rights to privacy and data protection under Articles 7 and 8 respectively of the EU Charter of Fundamental Rights.[38] The CJEU noted that the Directive did not contain sufficient substantive and procedural safeguards governing the access and use of retained data. In particular, it highlighted that "the access by the competent national authorities is not made dependent on a prior review carried out by a court or by an independent administrative body."[39]

---

[37] Third-Party Intervention Submissions by Article 19, Application Number 2016Heonma388, Constitutional Court of the Republic of Korea, 15 Dec. 2016, pp. 6-10, available at https://www.article19.org/data/files/medialibrary/38672/Korea-amicus-Brief-ARTICLE-19.pdf.

[38] Judgment of the Court (Grand Chamber), Digital Rights Ireland Ltd v Minister for Communications et al (C-293/12 and C-594/12), CJEU, 8 Apr. 2014, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=40531.

[39] *Id*. at para. 62.

31. In *Tele2 Sverige AB* and *Tom Watson & Others*, which considered Swedish and UK laws mandating communications service providers retain customer communications data in bulk (six months for Sweden, one year for the UK) for the sake of preventing and detecting serious crime, the Grand Chamber of the CJEU held:

> it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.[40]

32. These findings are also in line with the way a number of countries treat access to subscriber data. A 2014 study by the Council of Europe Cybercrime Convention Committee found that, in over half of responding member states, "obtaining subscriber information requires judicial authorisation."[41]

33. In 2014, the Canadian Supreme Court outlined the importance of anonymity as "the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure" in the case of *R. v. Spencer*.[42] It determined that the police's request for identifying information "engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognised by the Court in other circumstances as engaging significant privacy interests."[43] It concluded that the subscriber had a reasonable expectation of privacy in his subscriber (identifying) information,[44] effectively requiring that the police secure a court order in similar situations in the future:

> In my view, in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that

[40] Judgment of the Court (Grand Chamber), Tele2 Sverige AB and Tom Watson & Others (C-698/15), CJEU, 21 Dec. 2016, para. 120, available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=40531.
[41] Cybercrime Convention Committee, Council of Europe, Rules on obtaining subscriber information, 3 Dec. 2014, p. 28, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1.
[42] R. v. Spencer, 2014 SCC 43, para. 48, available at: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.
[43] *Id*. at para. 50.
[44] *Id*. at para. 62.

these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.[45]

34. Privacy International also draws the Court's attention to U.N. Special Rapporteur Kaye's 2015 report, which focused on the importance of anonymity to the exercise of the right to freedom of expression. In that report, the Special Rapporteur specifically recommended:

> States should revise or establish . . . national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective [and] *require court orders for any specific limitation* . . . .[46]

35. Thus, the U.N. Human Rights Committee has "note[d] 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."[47] The Committee went on to recommend that the government "ensure that subscriber information . . . be issued with a warrant only."[48]

2. Notification to Users

36. The Telecommunications Business Act also lacks a requirement that the government notify users when it accesses their subscriber data.

37. In *Tele2 Sverige AB* and *Tom Watson & Others*, the CJEU held that:

> Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy . . . where their rights have been infringed.[49]

---

[45] *Id*. at para. 66.
[46] United Nations, Human Rights Council (2015), Report of the Special Rapporteur Kaye, *supra* note 23, at para. 57 (emphasis added).
[47] Human Rights Committee, Concluding observations on the fourth periodic report of the Republic of Korea, UN doc. CCPR/C/KOR/CO/4, 3 December 2015, para. 42.
[48] *Id*. at para. 43.
[49] Judgment, Tele2 Sverige AB and Tom Watson & Others, *supra* note 40, at para. 121.

38. The CJEU's approach reflects the recommendations contained in the 2013 report of the former U.N. Special Rapporteur La Rue, which stated:

> Individuals should have a legal right to be notified that they have been subject to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath. [50]

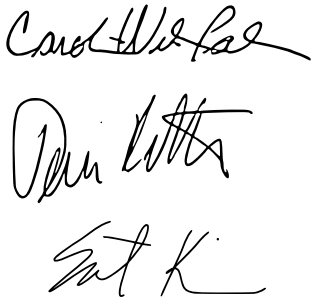
39. Similarly, in his 2015 report, current U.N. Special Rapporteur Kaye stated:

> Individuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection. In article 17(2) of the International Covenant on Civil and Political Rights, States are obliged to protect privacy against unlawful and arbitrary interference and attacks. Under such an affirmative obligation, States should ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors. Such protection must include the right to a remedy for a violation. In order for the right to a remedy to be meaningful, *individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data*. [51]

[50] United Nations, Human Rights Council (2013), Report of the Special Rapporteur La Rue, *supra* note 19, at para. 82.
[51] United Nations, Human Rights Council (2015), Report of the Special Rapporteur Kaye, *supra* note 23, at para. 18 (emphasis added).

IV. CONCLUSIONS

40. In light of the above considerations, Privacy International 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. Privacy International urges the Constitutional Court of Korea to take these standards into account when assessing the challenge currently before it.



Caroline Wilson Palow
General Counsel

Tomaso Falchetta
Legal Officer

Scarlet Kim
Legal Officer

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

Tel: +44 (0) 20 3422 4321
caroline@privacyinternational.org