CONSTITUTIONAL COURT OF THE REPUBLIC OF KOREA

Application Number 2016Heonma388

THIRD-PARTY INTERVENTION SUBMISSION BY DAVID KAYE, UNITED NATIONS SPECIAL RAPPORTEUR ON THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION

DAVID KAYE
United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression
Clinical Professor of Law and Director,
International Justice Clinic,
University of California Irvine School of Law
(949) 824-2427
401 East Peltason Dr. Ste. 3800-C
Irvine, CA 92697-8000
https://freedex.org/

9 May 2017

TABLE OF CONTENTS

I. INTRODUCTION

1. The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, submits this brief as *amicus curiae* to the Constitutional Court of the Republic of Korea.[1] The case before this Court concerns Article 83(3) and Article 83(4) of the Telecommunications Business Act ("TBA").

2. It is customary to note in the context of amicus filings that any submission by the Special Rapporteur is provided on a voluntary basis without prejudice to, and should not be considered as a waiver, express or implied, of the privileges and immunities of the United Nations, its officials and experts on missions, pursuant to the 1946 Convention on the Privileges and Immunities of the United Nations. Authorization for the positions and views expressed by the Special Rapporteur, in full accordance with his independence, was neither sought nor given by the United Nations, the Human Rights Council, the Office of the High Commissioner for Human Rights, or any of the officials associated with those bodies.

II. THE INTEREST OF THE SPECIAL RAPPORTEUR IN THE RESOLUTION OF THIS MATTER

3. The International Covenant on Civil and Political Rights ("the Covenant"), which the Republic of Korea ratified on April 10, 1990, establishes the obligations of State parties to respect and ensure the right to freedom of opinion (Article 19(1)) and the right to freedom of expression (Article 19(2)). The Human Rights Council, the central human rights institution of the United Nations ("U.N."), has affirmed that freedom of opinion and expression is "essential for the enjoyment of other human rights and freedoms and constitutes a fundamental pillar for building a democratic society and strengthening democracy."[2] As a State party, the Republic of Korea is bound to uphold these obligations "in good faith" and may not invoke "the provisions of its internal law as justification for its failure to perform a treaty."[3]

4. U.N. Human Rights Council resolution 7/36, Section 3(c), mandates me to "make recommendations and provide suggestions on ways and means to better promote and protect

---

[1] The Special Rapporteur would like to thank Mr. Calvin Bryne, Ms. Sarah Choi, and Mr. Adam Lhedmat, student advocates with the University of California Irvine School of Law International Justice Clinic, and Mr. Amos Toh, legal advisor to the mandate and Ford Foundation Fellow, for their assistance with the preparation of the brief.

[2] Human Rights Council Res. 23/L.5, at ¶2, U.N. Doc. A/HRC/23/L.5 (April 9, 2014).

[3] Vienna Convention on the Law of Treaties arts. 26-27, May 23, 1969 1155 U.N.T.S. 331.

the right to freedom of opinion and expression in all its manifestations."[4] Under the mandate, these recommendations are based on an analysis of international human rights law, including relevant jurisprudence, standards, and international practice, as well as relevant regional and national laws, standards, and practices. The laws at issue in this case raise critical issues concerning their compatibility with international human rights law and the degree to which they infringe upon fundamental rights to freedom of opinion and expression.

5. Since assuming the mandate, I have observed a marked increase in threats to freedom of expression online. Among other threats, my predecessor and I have documented the spread of unaccountable and intrusive electronic surveillance activities and attempts to weaken encryption and undermine online anonymity.[5] The present case raises similar concerns.

III. THE REPUBLIC OF KOREA HAS A DUTY TO ENSURE THAT GOVERNMENT ACCESS TO CUSTOMER IDENTITY DATA DOES NOT INTERFERE WITH THE RIGHT TO FREEDOM OF OPINION GUARANTEED UNDER ARTICLE 19(1) OF THE COVENANT.

6. Article 19(1) provides that "everyone shall have the right to hold opinions without interference." While freedom of *expression* may be "restricted by law or other power" according to narrow and specific criteria established under Article 19(3), the right to freedom of opinion "was held to be absolute."[6] This ability to hold opinions "was seen to be a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction."[7]

7. Multiple international and regional institutions, including the Human Rights Council, the U.N. General Assembly, and the Council of Europe, have concluded that the right freedom of opinion and expression applies equally offline as well as online.[8] Examples of offline interferences that challenge one's right to hold opinions include physical harassment,

[4] Human Rights Council Res. 7/36 at ¶3(c), U.N. Doc. A/HRC/7/36 (Mar. 28, 2008).

[5] See e.g. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) ("2013 Report"); Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, (May 22, 2015) ("2015 Report"); Human Rights Council Res. 34/7 (Mar. 22, 2017).

[6] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary*, at 441 (Feb., 1993).

[7] 2015 Report at ¶19 (May 22, 2015).

[8] See, e.g. G.A. Res. 68/167 (Jan. 21, 2014); Human Rights Council Res. 26/13 (July 14, 2014); and Council of Europe CM/Rec(2014)6 (Apr. 16, 2014).

detention, or other subtler efforts of punishment.[9] In the digital age, individuals hold opinions online by "saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in email archives".[10] These digital platforms in turn enable individuals to "*form* an opinion and to develop this by way of reasoning."[11] To the extent that the Republic of Korea seeks access to such information under Articles 83(3) and 83(4) of the TBA, it must not do so in a manner that interferes with the individual's right to form and hold opinions.

IV. UNDER ARTICLES 19(2) AND 19(3) OF THE COVENANT, THE REPUBLIC OF KOREA HAS A DUTY TO ENSURE THAT GOVERNMENT ACCESS TO CUSTOMER IDENTITY DATA DOES NOT UNDULY INTERFERE WITH THE RIGHT TO ANONYMOUS EXPRESSION AND COMMUNICATION.

A. Anonymous expression is an exercise of freedom of expression protected under Article 19(2).

8. Article 19(2) states that:

> "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

9. The Covenant does not expressly refer to anonymity. In fact, the *travaux preparatoires* concerning the text of Article 19 reveal that the negotiators understood anonymity to be a critical element of freedom of expression. During negotiations, participating States rejected a proposal to add the phrase "anonymity is not permitted" to Article 19(1), recognizing that "anonymity might at times be necessary protect the author" and "that such a clause might prevent the use of pen names."[12]

10. The States' concerns reflect that anonymity is often essential to public participation in civil and political discourse. The protection afforded by "pen names" - pseudonyms that individuals rely on instead of their 'real' names in their communications or works - liberate

---

[9] *See Yong-Joo Kang v. Republic of Korea*, Communication No. 878/1999, U.N. Doc. CCPR/C/78//D/878/1999, at ¶¶ 2.5, 7.2, and 7.3 (July 15, 2003).

[10] 2015 Report, at ¶20 (May 22, 2015).

[11] Nowak, *supra* at 441 (emphasis added).

[12] Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights*, at 379-80 (Feb. 17, 1987).

them to "explore and impart ideas and opinions more than [they] would using [their] actual identity." [13] In particular, individuals may be more willing to express and discuss unconventional, unpopular, or minority opinions and views, which they might otherwise withhold for fear of stigma, abuse, or threats to their physical safety.

11. The digital equivalents of "pen names" are equally protected under Article 19(2). Whether on blogs, social media platforms, online discussion forums, or in their private correspondence, many Internet users rely on online pseudonyms to achieve some measure of anonymity. Those who wish to conceal their identity more effectively may rely on a combination of encryption and anonymity tools, such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks.[14]

12. Article 19(2) was broadly drafted to accommodate these advances in technology. Its criteria for protection apply regardless of where or how the individual chooses to express herself: States parties chose to adopt the general phrase "through any other media of his choice," as opposed to an enumeration of then-existing media.[15] This interpretation is consistent with widespread international consensus that the right applies both online and offline. [16] Accordingly, anonymous expression is also protected "through any … media," whether online or offline.

13. Anonymous communication may also be, in and of itself, expressive activity that is protected under Article 19(2). In modern culture, symbols such as the Guy Fawkes mask donned at protests serve both to hide the wearer's identity and to make a political statement.[17] The act of concealing one's identity may therefore itself be a form of expression.

B. The ability to communicate anonymously creates a zone of privacy necessary for the realization of freedom of expression protected under Article 19(2).

14. Under Article 17 of the Covenant, everyone shall have the "right to the protection of the law" against "arbitrary or unlawful interference with his privacy, family, home or correspondence." Various international and regional bodies, including the U.N. General Assembly and Human Rights Council, the Council of Europe, and the Inter-American Commission on Human

[13] 2015 Report, at ¶9 (May 22, 2015).

[14] *Id*.

[15] 2015 Report, at ¶26 (May 22, 2015).

[16] *Supra* note 8.

[17] *See, e.g.,* Glenda Kwek, *V for vague: Occupy Sydney's faceless leaders*, The Sydney Morning Herald, (Oct. 14, 2011), available at: http://www.smh.com.au/nsw/v-for-vague-occupy-sydneys-faceless-leaders-20111014-1loy6.html.

Rights, have affirmed that protection of the right to privacy is critical to the exercise of freedom of expression.[18] As a result, undue interference with the right to privacy "can both directly and indirectly limit the free development and exchange of ideas."[19]

15. Online anonymity exemplifies the close connection between these rights, establishing a "zone of privacy ... to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[20] In particular, the combination of encryption and anonymity tools may secure the privacy of online correspondence, such as e-mail, text messaging, chat applications, and other online interactions, which have become popular media for the development and sharing of opinions.[21] Conversely, restrictions on anonymity may incentivize self-censorship. For example, my predecessor found that restrictions of anonymity in communication "have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization."[22]

16. When users disclose their identity data to telecommunications operators, this does not relieve the State of its obligation to respect and ensure the individual's right to anonymous expression and communication. Anonymity is not secrecy; instead, it is contingent on the individual's capacity to determine the circumstances under which their identity may be disclosed, including to whom and for what purposes. In this vein, the European Court of Human Rights has distinguished "metering" conducted by telephone operators (i.e. the collection of communications metadata) from the interception of communications, which the Court observed is "undesirable and illegitimate in a democratic society unless justified."[23] Likewise, users may disclose identity data to operators (or permit their collection) in order to facilitate the provision of Internet and telecommunications services; however, this does not grant the government or any other third party unfettered access to such data. With

[18] 2013 Report, at ¶24 (Apr. 17, 2013); *see also* G.A. Res. 68/167 (Jan. 21, 2014); Human Rights Council Res. 34/7 (Mar. 22, 2017); 2015 Report, at ¶16 (May 22, 2015); The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶19 (Apr. 17, 2013); Freedom of Expression and the Internet, Inter-American Commission for H.R., Office of the Special Rapporteur for Freedom of Expression, at ¶¶ 130, 150 (Dec. 31, 2013); The Rule of Law on the Internet and in the Wider Digital World, Council of Europe, Commissioner for Human Rights, at ¶88 (Dec. 8, 2014); Declaration on freedom of Communication on the Internet, Council of Europe, at principle 7 (May 28, 2003).

[19] 2013 Report, at ¶24 (Apr. 17, 2013).

[20] 2015 Report, at ¶16 (May 22, 2015).

[21] *Id.* at ¶17.

[22] 2013 Report, at ¶24 (Apr. 17, 2013).

[23] Malone v. United Kingdom, App. No. 8691/79, Judgment, 82 Eur. Ct. H.R. 10, ¶84.

appropriate legal and procedural safeguards, subscribers may remain anonymous to law enforcement and other government authorities.

C. Government access to customer identity data transmitted or held by a telecommunications business operator under Articles 83(3) and 83(4) of the TBA interferes with anonymous expression and communication protected under Article 19(2).

17. Article 83(3) states that:

> "A telecommunications business operator may comply with a request for the perusal or provision of any of the following data … from a court, a prosecutor, the head of an investigative agency ... or the head of an intelligence and investigation agency, who intends to collect information or intelligence in order to prevent any threat to a trial, an investigation … the execution of a sentence or the guarantee of the national security:
>
> (1) Names of users;
> (2) Resident registration numbers of users;
> (3) Addresses of users;
> (4) Phone numbers of users;
> (5) User ID (referring to the identification codes of users used to identify the rightful users of computer systems or communications networks); and
> (6) Dates on which users subscribe or terminate their subscriptions."

18. Article 83(4) states that:

> "Requests for provision of communications data under paragraph (3) shall be made in writing … which states a reason for such request, relation with the relevant user and the scope of necessary data: Provided, That where it is impossible to make a request in writing due to an urgent reason, such request may be made without resorting to writing, and when such reason disappears, a written request for provision of data shall be promptly filed with the telecommunications business operator."

19. Government access to customer data under Articles 83(3) and 83(4) potentially restrict both anonymous expression and communication. The scope of accessible data under Article 83(3) provides law enforcement, intelligence agencies, and other government authorities with comprehensive insight into an individual's online and offline identities, including their legal name, where they live and work, and the phone numbers, email addresses, and usernames they use. Such information can be combined and analyzed with other Internet and telecommunications metadata - such as Internet Protocol (IP) addresses, cell site location

information, the numbers dialed, and the time and date of phone calls and e-mails - to create an even more detailed picture of "an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication."[24]

20. Given the potential scope of government access, common forms of online anonymity may be "superficial and easily disturbed."[25] For example, reliance on pseudonyms or even widely available encryption tools (such as HTTPS websites that encrypt web traffic by default) may be insufficient. Users that have an urgent need to avoid discovery - particularly those who wish to express minority views or disclose sensitive information in the public interest - may be compelled to turn to sophisticated anonymizing software and tools, which can be technically complicated or cumbersome to use. Given the burden and risks involved, many may choose not to speak at all.

21. The mere prospect of government access to customer identity data may also deter individuals from expressing themselves freely in their private communications. As a result, the mere existence of a legal regime that facilitates government access to such data "creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."[26] This chilling effect may have a disproportionate impact on attorney-client relationships, journalists and their sources, whistleblowers, human rights defenders, and minorities and vulnerable groups.

D. Article 19(3) requires government access to customer identity data to be provided by law, and a necessary and proportionate means of accomplishing a legitimate government objective.

22. Article 19(3) states that:

> "The exercise of the rights provided for in [Article 19(2)] carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are *provided by law* and are *necessary*:
>
> (a) For respect of the rights or reputations of others;

[24] The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶19 (Apr. 17, 2013).

[25] 2015 Report, at ¶9 (May 22, 2015)

[26] The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶20 (Apr. 17, 2013).

(b) For the protection of national security or of public order (ordre public), or of public health or morals."[27]

23. For a restriction on freedom of expression to be "provided by law," the Human Rights Committee—a body of experts charged with monitoring implementation of the Covenant—concluded that it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation.[28] Accordingly, the laws and regulations defining the circumstances under which government authorities are permitted to access customer identity data must meet "a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application."[29] In the context of communications surveillance, the government must also demonstrate that access to user data does not grant the authorities unfettered discretion to restrict freedom of expression.

24. The scope of the government's authority to access user data must also be "necessary" to accomplish an objective specified under Article 19(3), be it law enforcement, national security, or public safety. Necessity, by definition, means that the restriction must be more than simply reasonable, useful, or desirable.[30] Instead, a State must demonstrate "in specific and individualized fashion the precise nature of the threat," and a "direct and immediate connection" between the threat on one hand, and the scope of data accessed and the manner in which it is accessed on the other.[31] In the context of national security, my predecessor has observed that broad definitions of this objective are "vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists."[32]

25. Necessity also implies an assessment of the proportionality of the government's authority to access user data.[33] According to the Human Rights Committee, a proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve [the intended] protective function."[34] In other words, access to user data

[27] International Covenant on Civil and Political Rights art. 19(3), Dec. 16, 1966, 999 U.N.T.S. 171 (emphasis added).

[28] U.N Doc. CCPR/C/GC/34, at ¶39 (Sep. 12, 2011); 2015 Report, at ¶32 (May 22, 2015).

[29] 2013 Report, at ¶83 (Apr. 17, 2013).

[30] 2015 report, at ¶34 (May 22, 2015)

[31] U.N Doc. CCPR/C/GC/34, at ¶35.

[32] 2013 Report, at ¶60 (Apr. 17, 2013).

[33] U.N Doc. CCPR/C/GC/34, at ¶34 (Sep. 12, 2011); *See also* Lohe Issa Konate v. Burkina Faso, No. 004/2013, Afr. Ct. H.P.R., at ¶¶ 148, 149 (Dec 5, 2014); The Sunday Times v. The United Kingdom, No. 6538/74, Eur. Ct. H.R. at ¶¶ 59, 62 (Apr. 26, 1979).

[34] *Id*.

should only be sought when less intrusive means of surveillance or investigation have been exhausted. In any case, "a detailed and evidence-based public justification" for such access is critical to enable transparent and robust public debate.[35]

V. WARRANTLESS ACCESS TO CUSTOMER IDENTITY DATA VIOLATES THE REPUBLIC OF KOREA'S OBLIGATION TO REFRAIN FROM UNDUE INTERFERENCE WITH THE RIGHT TO ANONYMOUS EXPRESSION AND COMMUNICATION.

26. Warrantless government access to customer identity data violates the legality, necessity, and proportionality criteria set out above. Instead, such access should only be granted pursuant to legal criteria defined with sufficient precision, and an order by a competent and impartial judicial body certifying necessity and proportionality to achieve a legitimate objective. My analysis of relevant international jurisprudence and practice indicates that this view is shared by respected international and regional bodies and a growing number of States.

A. The authority to request for customer identity data without a warrant is inconsistent with emerging global consensus that government access to identity data must be authorized by judicial order.

27. U.N. mechanisms have concluded that government access to personal data, including customer identity data and communications metadata, should be regulated through a competent, independent, and impartial judicial process. In 2014, the General Assembly called upon member States to "establish or maintain existing *independent, effective domestic oversight mechanisms* capable of ensuring transparency, as appropriate, and accountability" for both "State surveillance of communications" and "the collection of personal data."[36] The U.N. High Commissioner for Human Rights, which the General Assembly commissioned to propose recommendations addressing the human rights impact of communications surveillance, elaborated that "*judicial involvement* that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires."[37] In 2016, the General Assembly adopted a similar recommendation, calling on States to "establish or maintain existing *independent, effective, adequately resourced and impartial judicial*, administrative, and/or parliamentary domestic oversight mechanisms

[35] *See* G.A. Res. 69/397, ¶12 (Sep. 23, 2014).

[36] G.A. Res. 69/166 (Feb. 10, 2015) at ¶4(d) (emphasis added).

[37] The Right to Privacy in the Digital Age, Office of the United Nations High Commissioner for Human Rights, U.N. Doc. A/HRC/27/37, at ¶38 (Apr. 17, 2013) (emphasis added).

capable of ensuring transparency, as appropriate, and accountability for … the collection of personal data."[38]

28. International and regional experts on freedom of expression have also reaffirmed the need for judicial process. In its 2013 study of freedom of expression and the Internet, the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights concluded that "[t]he laws that authorize the interception of communications must establish clearly and precisely the reasons the State can invoke to request that interception, which *can only be authorized by a judge*."[39] Similarly, my predecessor has found that, under human rights law, "[t]he provision of communications data to the State should be monitored by an independent authority, *such as a court* or oversight mechanism."[40] Both Special Rapporteurs reiterated these recommendations in their 2013 Joint Declaration on surveillance programs and their impact on freedom of expression, urging States to ensure that "[t]he collection of [personal] information [is] monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight."[41]

29. A survey of relevant regional and domestic jurisprudence also indicates that judicial pre-authorization establishes a critical safeguard against unlawful, unnecessary, and disproportionate government access to user data. In *R v. Spencer*, a case concerning provisions materially similar to Arts. 83(3) and 83(4) of the TBA, the Supreme Court of Canada held that it was unconstitutional for law enforcement to submit requests for subscriber information held by third party operators without a judicial warrant, even when these requests are non-binding and the operator voluntarily discloses such information.[42] The Court reasoned that 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 these activities would be anonymous."[43] Accordingly, a "request by a

---

[38] G.A. Res. 71/39, at ¶5(d) (Nov. 16, 2016) (emphasis added).

[39] *Freedom of Expression and the Internet*, Office of the Special Rapporteur for Freedom of Expression, Inter-American Commission for Human Rights, at 156 (Dec 31, 2013), available at: https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf, (emphasis added).

[40] 2013 Report, at ¶86 (Apr. 17, 2013) (emphasis added).

[41] *Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression*, United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression; Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, available at: https://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

[42] *See R v. Spencer,* 2 S.C.R. 212 (June 13, 2014).

[43] *Id.* at ¶66.

police officer that an ISP voluntarily disclose such information amounts to a search" that must comply with established legal and procedural safeguards, including the warrant requirement.[44]

30. The lack of pre-judicial authorization also led the European Court of Justice to invalidate the European Union (EU) Data Retention Directive, in its 2014 decision in *Digital Rights Ireland and Seitlinger*. In particular, the Court of Justice found that government access to personal data retained by telecommunications business operators under the Directive was "not made dependent on a prior review carried out by a court or by an independent administrative body" that limits access to "what is strictly necessary for the purpose of attaining the objective pursued."[45] Similarly, the Supreme Court of Mexico has concluded that law enforcement access to cell phone metadata without a warrant violates the communicants' right to privacy.[46]

31. Additionally, an examination of relevant domestic legislative frameworks reveals that more than a dozen countries require a warrant or some other form of judicial process to grant law enforcement access to customer identity data.[47] Varying levels of judicial pre-authorization have been established in Azerbaijan, the Czech Republic, Denmark, Mauritius, Romania, the Ukraine, and the United States, among others.[48] In Spain, France, and Japan, judicial pre-authorization is required when the information requested affects the secrecy of the communication.[49]

32. Finally, it bears emphasis that this Court has recognized the importance of limiting restrictions on online anonymity. In the 2010 decision *Hun-Ma*, this Court found that:

> Anonymous speech in the Internet, rapidly spreading and reciprocal, allows people to overcome the economic or political hierarchy offline and therefore to form public opinions free from class, social status, age, and gender distinctions, which make governance more reflective of the opinions of people from diverse classes and thereby further promotes democracy. Therefore, anonymous speech in the Internet, though

---

[44] *Id.*

[45] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine, and Natural Resources*, E.C.J. 238 at ¶62 (Apr. 8, 2014)

[46] *See Contradicción de Tesis*, 2012 Mex. S.C. 194, (Oct. 10, 2012).

[47] *Rules on obtaining subscriber information*, Cybercrime Convention Committee, T-CY(2014), at 17 (Dec. 3, 2014).

[48] *Id.*

[49] *Id.*

fraught with harmful side-effects, should be strongly protected in view of its constitutional values.[50]

33. A decision endorsing the warrant requirement for law enforcement access to personal data would meaningfully address these concerns and, in so doing, align this Court with emerging international consensus.

B. The warrant requirement will meaningfully address the Republic of Korea's urgent need to curb unnecessary and disproportionate requests for customer identity data.

34. To be sure, several states continue to permit warrantless access to customer identity data, potentially in violation of their human rights obligations.[51] For example, in Australia and Bulgaria, senior law enforcement officials may access user identity information pursuant to a "formal police request."[52] In my view, however, these frameworks should not serve as a model for the Republic of Korea, where the risk to users' freedom of expression is exacerbated by the sheer volume of government requests for customer identity data.

35. A survey of similar practices worldwide indicates that the Republic of Korea has among the highest number of government requests for customer identity data per capita. In 2011, the country, which has a population of slightly under 50 million, recorded 5.84 million seizures of customer identity data —a startlingly high rate of one request for every nine individuals. In 2015, the number of requests ballooned to roughly 1 billion.[53]

36. These figures are significantly higher than those recorded in comparable democratic nations. In the United Kingdom, with a population of roughly 65 million, 761,702 items of communications data were approved in 2015, half of which were customer identity data —an average rate of one item of communications data for every 85 individuals, and one item of

[50] Const. Ct., 2010 Hun-Ma 47, 252 (Aug. 28, 2012) (S. Kor.).

[51] *Rules on obtaining subscriber information*, Cybercrime Convention Committee, T-CY(2014), at 16 (Dec. 3, 2014).

[52] *Id.*

[53] *See 2016 First Semi-Annual Numbers of Communication Data Disclosures and Communication Metadata Acquisitions*, Ministry of Science, ICT and Future Planning (November 1, 2016), available at: http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1316113&snsMId=NzM%3D&getServerPort=80&sn.sLinkUrl=%2Fweb%2FmsipContents%2FsnsView.do&getServerName=www.msip.go.kr.

customer identity data for every 170 individuals.[54] In France, evidence suggests that, between October 2015 and October 2016, there were 48,208 requests for stored metadata - a much wider category of communications data, of which customer identity data is only a subset.[55] With a population of roughly 66 million, this translates to one metadata request per 1,375 individuals. In the United States, with a population of roughly 314 million, it is estimated that there were between 500,000 and 600,000 requests for customer identity data in 2012 – an average rate of roughly one request for every 600 individuals.[56]

37. In fact, the number of customer identity data requests per capita in Korea is at least 3.5 times higher than Canada, the country with the next highest figure. In 2011, Canada recorded 1.2 million requests for user data (including but not limited to customer identity data). With a population of roughly 34 million, this translates to an average rate of one request per 28 Canadians.[57] Furthermore, Canada has explicitly rejected warrantless access to user identity data.[58] Under the Criminal Code, government access to user data must be authorized by judicial order certifying "reasonable grounds to believe" that the data will provide evidence

---

[54] Each item of data is "a request for data on a single identifier or other descriptor, for example, 30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data." Sir Stanley Burton, *Report of the Interception Communications Commissioner, Annual Report for 2015*, Interception of Communications Commissioner's Office, at ¶¶ 7.23-7.24 (Sep. 8, 2016), available at: http://iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf.

[55] *1er Rapport d'activité 2015/2016*, Commission Nationale de Contrôle des Techniques de Renseignment, at 65 (Nov., 2016) available at: https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf.

[56] Kyung Sin Park, Communications Surveillance in Korea, Korea University Law Review, Vol. 16-17, May 2015, at 61 - 62 (May, 2015), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2748318. These estimates are based on VERIZON, *Verizon's Transparency Report*, http://transparency.verizon.com/us-data, and calculated with reference to numbers that major U.S. telecommunications providers provided to Senator Edward J. Markey in 2012 and 2013. Ed Markey, *For Second Year in a Row, Markey Investigation Reveals More Than One Million Requests By Law Enforcement for Americans Mobile Phone Data*, ED MARKEY (Dec. 9, 2013), http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data; Ed Markey, *Markey: Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers*, ED MARKEY (July. 9, 2012), http://www.markey.senate.gov/news/press-releases/markey-law-enforcement-collecting-information-on-millions-of-americans-from-mobile-phone-carriers.

[57] *Response to Request for General Information from Canadian Wireless Telecommunications Association*, Office of the Privacy Commissioner of Canada, at 3 (Dec. 14, 2011), available at: *https://www.priv.gc.ca/media/1103/let_gowling_e.pdf*.

[58] *See R v. Spencer,* 2 S.C.R. 212 at 249 (June 13, 2014).

of a crime.[59] Data minimization requirements also preclude telecommunications operators from collecting social insurance numbers—Canada's equivalent of the national identification number — when other less invasive means of identification are available.[60]

38. Given the rate at which the Republic of Korea requests for and acquires customer identity data, the lack of a warrant requirement for access to such data creates an even greater risk of unnecessary and disproportionate restrictions on freedom of expression.

VI. CONCLUSION

39. For the reasons identified above, I submit that Articles 83(3) and 83(4) of the TBA pose a grave risk to the freedom of expression of Internet and telecommunications users in the Republic of Korea. Articles 83(3) and 83(4) permit telecommunications operators to disclose customer identity data to select government authorities without a judicial warrant. Both the mere prospect of disclosure and the actual disclosures themselves interfere with anonymous expression and communication protected under Article 19(2) of the Covenant. An analysis of international law and practice indicates that the lack of judicial pre-authorization for government requests for customer identity data constitutes an unnecessary and disproportionate restriction under Article 19(3). The risk to freedom of expression is exacerbated by the reality that the Republic of Korea has among the highest number of user data requests per capita.

40. I respectfully urge the Court to take these concerns into careful consideration when they assess the legal and constitutional validity of Articles 83(3) and 83(4) of the TBA.

---

[59] Canada Criminal Code § 487.018, RSC 1985, c C-46

[60] *See e.g.* Personal Identification Protection and Electronic Documents Act, Case Summary #2001-22, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/pipeda-2001-022/; Personal Identification Protection and Electronic Documents Act, Case Summary #2003-184, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-184/; Personal Identification Protection and Electronic Documents Act, Case Summary #2003-204, available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-204/.

Respectfully Submitted,

DAVID KAYE

UN Special Rapporteur on the Right to Freedom of Opinion and Expression
Clinical Professor of Law and Director, International Justice Clinic, University of California Irvine School of Law
401 East Peltason Dr. Ste. 3800-C
Irvine, CA 92697-8000
(949) 824-2427
dkaye@law.uci.edu