NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

TÉLÉCOPIE • FACSIMILE TRANSMISSION

DATE: 3 June 2019

A/TO: The Registrar
European Court of Human Rights
Council of Europe
F-6005 Strasbourg CEDEX
France

FAX: + 33(03) 388 41 27 30, 0033388412730

E-MAIL:

DE/FROM: Beatriz Balbin
Chief
Special Procedures Branch

FAX: +41 22 917 90 06

TEL: +41 22 917 98 67

E-MAIL: freedex@ohchr.org

REF:

PAGES: 11

COPIES:

OBJET/SUBJECT: Please find attached the intervention by Mr. David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in the case of Big Brother Watch and Others v. United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15 before the Grand Chamber of the European Court of Human Rights.

IN THE EUROPEAN COURT OF HUMAN RIGHTS
GRAND CHAMBER

Applications nos. 58170/13, 62322/14 and 24960/15
Case of Big Brother Watch and Others v. the United Kingdom
Referred to the Grand Chamber on 4 February 2019

INTERVENTION

Pursuant to Article 36(2) of the European Convention on Human Rights and Rule 44(3) of the Rules of Court

By the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Professor David Kaye

A. Introduction

1. In accordance with the conditions set by the Court, this submission is filed in connection with Applications nos. 58170/13, 62322/14 and 24960/15. It shall address general principles applicable in the case, as interpreted from the perspective of the mandate of Special Rapporteur established by the United Nations Human Rights Council. Leave to intervene was granted on 9 May 2019.

B. Background

The Special Rapporteur

2. Special Rapporteurs are independent experts appointed by the Human Rights Council of the United Nations ("UN"). The Special Procedures system, of which special rapporteurs are a part, is a central element of the UN human rights machinery and covers all human rights: civil, cultural, economic, political, and social. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression ("the Special Rapporteur") is mandated by Human Rights Council resolution 7/36 to, *inter alia*, gather all relevant information, wherever it may occur, relating to violations of the right to freedom of opinion and expression, discrimination against, threats or use of violence, harassment, persecution or intimidation directed at persons seeking to exercise or to promote the exercise of the right to freedom of opinion and expression.

3. The Special Rapporteur's mandate rests primarily upon Article 19 of the International Covenant on Civil and Political Rights ("the Covenant").[1] In discharging his mandate, the Special Rapporteur has collected and continues to collect evidence and to report on the nature, extent and severity of the violations of the rights to freedom of opinion and

[1] International Covenant on Civil and Political Rights, adopted 16 December 1966, 999 UNTS 1057.

freedom of expression globally, as well as the means by which these violations are effected by State and non-State actors.

4. This intervention is submitted to the European Court of Human Rights by the Special Rapporteur 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, including the individuals listed above, pursuant to the 1946 Convention on the Privileges and Immunities of the United Nations. Authorization for the positions and views expressed by the Special Rapporteurs, in full accordance with their 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.

C. SURVEILLANCE INTERFERES WITH SEVERAL RIGHTS UNDER THE COVENANT, ESPECIALLY RIGHTS TO PRIVACY AND FREEDOM OF OPINION AND EXPRESSION

5. Surveillance casts a shadow over communications – online and offline – such that individuals may refrain from engaging in activities protected under international human rights law.[2] In particular, surveillance may cause an interference with privacy that has significant implications for the exercise of the rights to freedom of opinion and expression. Moreover, mass and targeted surveillance programs operate in such ways that they are often unknown to those whose communications, locations, and other activities have been collected and observed, creating a perverse sense of violation – with the attendant consequences of chilling fully legitimate expression – even when the specific acts of surveillance are difficult, if not impossible, to determine. This is not to say that all surveillance operations constitute a violation of human rights law; some restrictions may be tolerable when they meet conditions of legality, necessity and legitimacy. However, because of the risks they involve to fundamental rights, all types of surveillance practices call for a rigorous evaluation of whether they are consistent with norms of international human rights law.

6. The human rights mechanisms of the United Nations, in particular within Special Procedures, have conducted several studies into the implications of surveillance for the rights to privacy and freedom of opinion and expression. This intervention draws upon several of those reports in order to provide the Court with information about the approach taken in light of the rights individuals enjoy under international human rights law, in particular under the Covenant. For instance, in a seminal study in 2013 the previous Special Rapporteur concluded that, "[w]ithout 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."[3] The UN High Commissioner for Human Rights concluded, in her study in 2014, "International human rights law provides a clear and universal framework for the promotion and protection of the right

[2] OHCHR, 'Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age' (30 June 2014) UN doc. A/HRC/27/37, para. 47 (hereinafter "High Commissioner Report"); HRC, '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) UN doc. A/HRC/23/40, para 79 (hereinafter "La Rue Report").

[3] La Rue Report (n 2), para. 79.

to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data."[4] The current Special Rapporteur has built upon these foundational reports by exploring surveillance and human rights in a number of contexts. Among them, two are most relevant: In his 2015 report to the Human Rights Council, the Special Rapporteur examined how privacy and freedom of expression interlink so as to provide individuals with the right to tools such as encryption and anonymity as protection in the face of mass and targeted surveillance conducted by State and non-State actors.[5] In his 2015 report to the UN General Assembly, the Special Rapporteur examined how the individual's right to information, so essential to democratic society, counseled in favor of strong protections of the confidentiality of communications of journalists, their sources and whistleblowers.[6] The Special Rapporteur has expanded beyond State obligations to evaluate the roles and responsibilities of private actors that facilitate surveillance.[7]

7. Rights to privacy and freedom of expression are inextricably linked, and surveillance highlights why this is true. Article 17 of the Covenant protects against "arbitrary or unlawful interference with [one's] privacy, family, home or correspondence". The High Commissioner for Human Rights noted that "any capture of communications data is potentially an interference with privacy".[8] The UN General Assembly, the High Commissioner for Human Rights, and special procedures mandate-holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression.[9] The right to privacy must be protected not only on its own terms, as a fundamental right independent of other rights, but also in order to protect other rights that depend upon a zone of privacy for their enjoyment. Under Article 17, an interference with the right to private life may not be arbitrary or unlawful. In addition to covering acts that are unlawful or contrary to international law, the notion of arbitrariness has been interpreted in a separate contexts "to include elements of inappropriateness, injustice, lack of predictability, and due process of law as well as elements of reasonableness, necessity, and proportionality".[10] The State has

[4] High Commissioner Report (n 2), para. 47.
[5] HRC, 'Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye', (22 May 2015) UN Doc. A/HRC/29/32 (Hereinafter: Report on encryption and anonymity).
[6] UNGA, 'Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye', (8 September 2015) UN doc. A/70/361 (Hereinafter: Report on the protection of sources and whistleblowers).
[7] See, e.g., HRC, 'Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye', (30 March 2017) UN doc. A/HRC/35/22.
[8] High Commissioner Report (n 2), para. 20. In its General Comment no 16, the Human Rights Committee holds that surveillance measures should be prohibited, and the gathering or holding of personal information must be regulated by law, see Human Rights Committee, 'CCPR 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), paras. 8 and 10.
[9] See UNGA, 'Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age' (21 January 2014) UN doc. A/Res/68/167; HRC, 'Resolution adopted by the Human Rights Council: The promotion, protection and enjoyment of human rights on the Internet' (16 July 2012) UN doc. A/HRC/RES/20/8.
[10] Human Rights Committee, 'General Comment No. 35: Article 9 (Liberty and security of person)' (16 December 2014) UN docs. CCPR/C/GC/35, para. 12; Human Rights Committee, 'General Comment no. 36: Article 6 of the International Covenant on Civil and Political Rights, on the right to life' (30 October 2018) UN

the burden of proof to demonstrate the compatibility of any restrictions or interferences with the requirements of the ICCPR.[11]

8. The right to freedom of opinion and expression is enshrined in the Covenant's Article 19, but finds parallel in global and regional human rights instruments.[12] Article 19(1) safeguards everyone's right to hold opinions without interference, while Article 19(2) protects everyone's right to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media.

9. In the decades since the adoption of the Universal Declaration of Human Rights (1948) and then the Covenant, human rights mechanisms, including treaty bodies, courts and special procedures, have paid less attention to the right to freedom of opinion than freedom of expression. This is notwithstanding the fact that human rights instruments provide an absolute right to freedom of opinion, allowing for no restriction or interference in the holding of opinions.[13] The drafters of the Covenant saw the right to hold an opinion as "a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction".[14] It may very well be that the drafters of the Covenant saw the holding of an opinion as something that someone would retain internally, and thus an interference with opinion would have involved such draconian measures as re-education camps, punishment for membership in illicit organizations, and similar kinds of penalties.

10. The digital age provides reasons for moving away from an approach to opinion that is so limiting, one that resulted in limited jurisprudence. The mechanics of forming and holding opinions have undergone remarkable change over the recent past, requiring a reconsideration of how human rights law protects opinion particularly in the face of surveillance. As indicated by the Special Rapporteur in the 2015 report on encryption:

> "Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one's mind. […] Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as

---

docs. CCPR/C/GC/36), para. 12. See also Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN docs. CCPR/C/21/Rev.1/Add. 13, para. 6.

[11] Human Rights Committee, 'General Comment No. 34: Article 19: Freedoms of opinion and expression' (12 September 2011) UN docs. CCPR/C/GC/34, paras. 27 and 35.

[12] See e.g. the Convention on the Rights of the Child, adopted 20 November 1989, 1577 UNTS 3, Art. 13; the American Convention on Human Rights, adopted 22 November 1969, OAS TS 36, Art. 13; the African Charter on Human and Peoples' Rights, adopted 27 June 1981, OAU doc. CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982), Art. 9.

[13] General Comment no. 34 (n 11), paras. 9 – 10.

[14] Report on encryption and anonymity (n 5), para. 19.

search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes."[15]

In other words, surveillance systems that interfere with opinion should be analysed as such, with a rigorous approach to ensure that the protections available under Article 19(1) remain robust as governments gain ever stronger and increasingly intrusive tools to interfere with this fundamental right.

11. Whereas the freedom of opinion is absolute, the right to freedom of expression is both broad and subject to narrow limitations under restrictive conditions. As the Human Rights Council put it, echoing the principles that have been at the root of European jurisprudence for several decades, the freedom of 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".[16] (Human Rights Council resolution 25/2). As confirmed by the Human Rights Committee, the monitoring body of the Covenant, Article 19(2) applies to all forms of expression and the means of their dissemination, including expressions made through communications technologies.[17] To constitute a restriction on the freedom of expression, a measure does not need to directly censor or restrict speech; it can be considered an interference based on its chilling effects on the exercise if the freedom of expression, the journalistic privilege being a notable example.[18] Surveillance measures, including bulk interception and communications interference, that entail a possibility of interference contrary to the principle of journalistic privilege will, in addition to Article 17, constitute an interference with Article 19 (2).[19] The Human Rights Committee has not, however, restricted its analysis of chilling effects to journalistic freedom. Surveillance regimes with the effect of discouraging individuals from legitimate exercise of the right to freedom of expression and opinion can similarly constitute an interference with Article 19 (2).[20]

12. Consequently, surveillance measures constitute an interference with the right to freedom of expression and must therefore comply with the requirements of Art. 19 (3). Under Article 19(3), restrictions on expression "shall only be such as are provided by law and are necessary" for specifically enumerated purposes, namely "(a) For respect of the rights or reputations of others; [and] (b) For the protection of national security or of public order (*ordre public*), or of public health or morals". In other words, any restriction on the right to freedom of expression must meet the tests of legality, necessity and proportionality, and legitimacy.

13. *Legality:* Mass surveillance programmes, including bulk interference and interception of communication, provide significant challenges to the requirement of accessible legislation. Beyond the complexity of how surveillance technologies function,[21] vague

[15] Report on encryption and anonymity (n 5), paras. 20 and 21.
[16] HRC, 'Resolution adopted by the Human Rights Council: Freedom of opinion and expression: mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (9 April 2014) UN doc. A/HRC/RES/25/2.
[17] General Comment no. 34 (n 11), para 12.
[18] *Id*., para 45.
[19] Report on the protection of sources and whistleblowers (n 6), para. 5; La Rue Report (n 2), paras. 24 and 26.
[20] See e.g. General Comment no 34 (n 11), para 47.
[21] Report on encryption and anonymity (n 5), para. 25.

legal standards for intercepting communications, and complicated and often classified administrative frameworks fall short of enabling "those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur".[22] In order to be compatible with the Covenant, any restriction "must be made accessible to the public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly."[23] Moreover, it "must not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution".[24] In its case law under the European Convention, and consistent with the law of the Covenant, the Court has developed minimum requirements on the quality of the law for interception of communication in criminal investigations.[25] Any requirements on the accessibility of the law should be understood in light of the significant impact that mass surveillance has on the rights concerned. Consequently, the Special Rapporteur has recommended that States should provide "individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance."[26]

14. *Necessity:* The requirement of necessity entails that restrictions "must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated".[27] Beyond prohibiting overbroad restrictions, measures must be "appropriate to achieve their protective function; they must be the least intrusive instrument […]; they must be proportionate to the interest to be protected".[28] Under no circumstance can the restriction be so comprehensive as to reverse the role between the norm and the exception, see the Covenant Article 5.[29]

15. As indicated in the report by the former Special Rapporteur on the promotion and protection of human rights while countering terrorism, mass surveillance measures entail the interference of rights of "a potentially unlimited number of innocent people in any part of the world".[30] Beyond preventing individualised assessments of proportionality on the part of the State for each interference, it risks running contrary to the requirements of Article 5 of the Covenant. Thus, in assessing the proportionality of the measure, the collateral damage to collective rights to privacy, the freedom of expression and opinion must be taken into account.[31]

16. The UN High Commissioner's Report counseled against distinguishing metadata from content interferences when examining the severity of the interference with rights protected under the Covenant. Her 2014 report noted that the aggregation of "metadata" by way of Government surveillance may reveal more private detail about an individual than perhaps even a private communication would.[32] The European Court of Justice has

---

[22] UNGA, 'Report of the Special Rapporteur on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson' (23 September 2014) UN doc. A/69/397, para. 36 (Hereinafter: Emmerson Report); High Commissioner Report (n 2), para. 29.
[23] General Comment No. 34 (n 11), para. 25.
[24] *Id*.
[25] *Weber and Saravia v. Germany* App no 54934/00 (ECtHR (dec), 29 June 2006), para. 95.
[26] La Rue Report (n 2), para. 92.
[27] General Comment No. 34 (n 11), para. 22.
[28] *Id* para. 34.
[29] *Id.*, para. 21.
[30] Emmerson Report (n 22), para. 52.
[31] *Id.*
[32] High Commissioner Report (n 2), para. 19.

recognized that such aggregation of data "may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."[33]

17. A serious concern of disproportionality relates to interference with the work of journalists and the protection of their sources. The Covenant protects all exercising rights to freedom of expression and does not make fine distinctions among the categories of people sharing information, such as those, like journalists, sharing information in the public interest. As indicated by the Human Rights Committee, journalism "is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the internet or elsewhere".[34] Thus, attempts to filter communication that would be covered by the journalistic privilege would be arbitrary and thus unlawful.

18. In the 2015 report to the UN General Assembly, the Special Rapporteur highlighted the importance of source protection as a mechanism for ensuring State accountability, and for individuals to make informed decisions about matters that may most affect them and their communities.[35] Restrictions on source protection and confidentiality create "disincentives for disclosure, dries up further sources to report a story accurately and damages an important tool of accountability".[36] Under international human rights law, sources and whistle-blowers enjoy the right to impart information, but their legal protection when publicly disclosing information rests especially on the public's right to receive it.[37] The protection of the confidentiality of sources is, in turn, a crucial to ensure society's access to information in the public interest. These elements have been recognized by global and regional human rights mechanisms, as well as in domestic legal systems.[38] The scope of the special protection of confidentiality under Article 19 must take into account the broad understanding of journalist under the Covenant. Consequently, as human rights law affords source confidentiality a high standard of protection, the 2015 report concluded that any "restrictions on confidentiality must be genuinely exceptional and subject to the highest standards, and implemented by judicial authorities only. Circumventions, such as secret surveillance or metadata analysis not authorized by judicial authorities according to clear and narrow legal rules, should not be used to undermine source confidentiality".[39]

19. Another concern of disproportionality relates more generally to other criteria established by domestic authorities on subjects of surveillance. The Human Rights Committee, in its 2015 Concluding Observations on the United Kingdom, expressed its

---

[33] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* (CJEU, 8 April 2014), paras. 26-27, and 37. See also Executive Office of the President, *Big Data and Privacy: A Technological Perspective* (May 2014) (available here: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf), 19.

[34] General Comment no. 34 (n 11), para. 44; Report on the protection of sources and whistleblowers (n 6), paras. 17 – 18.

[35] Report on the protection of sources and whistleblowers (n 6), para 1.

[36] *Id.* para. 21.

[37] *Id.* para 5.

[38] *Id.* paras. 14 – 16.

[39] *Id.* para. 62.

concern "that the Regulation of Investigatory Powers Act 2000 (RIPA), that makes a distinction between 'internal' and 'external' communications, provides for untargeted warrants for the interception of external private communication and communication data which are sent or received outside the United Kingdom without affording the same safeguards as in the case of interception of internal communications".[40] Under the Covenant, the State is under a duty to respect and ensure all Covenant rights to all within its jurisdiction. In its interpretative practice, the Human Rights Committee has considered the protection to cover everyone within the power of the State.[41] In its latest General Comment, the Committee interpreted the standard as including State activities that directly impact rights outside its own territory.[42] Thus, limiting the protection to those within the State's own territory may run contrary to the scope of applicability of the Covenant. More generally, maintaining this distinction as permissive for a lower threshold of protection risks allowing "a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory".[43]

20. *Legitimacy:* Within the ambit of Art. 19, restrictions are limited to those specified under article 19(3), which include limitations to protect the rights and reputations of others, national security or public order (*ordre public*), or public health or morals. As indicated by mandate holders under UN Special procedures, States regularly invoke national security to legitimise surveillance measures that entail over-broad restrictions on human rights.[44] The invocation of national security does not in and of itself provide an adequate human rights law justification.[45] Rather, the State must provide an "articulable and evidence-based justification for the interference".[46] The State must, at a minimum, give a meaningful public account of the tangible benefits.[47]

21. The need for certain safeguards to prevent abuse of surveillance regimes has long been acknowledged in the jurisprudence of the Court.[48] Similar requirements for safeguards exist under the Covenant.[49] The Special Rapporteur has particularly emphasized the need for a court, tribunal or other independent adjudicatory body to supervise the application of an interference measure.[50] The previous Special Rapporteur recommended that individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. If it would jeopardize the State's interest to notify beforehand, the State must notify the individual once surveillance has been completed

[40] Human Rights Committee, 'Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland' (17 August 2015) UN docs. CCPR/C/GBR/CO/7, para. 24.
[41] General Comment no. 31 (n 10), para. 10.
[42] General Comment no. 36 (n 10), para 63.
[43] *Issa and Others* v. Turkey App no 31821/96 (ECtHR, 16 November 2004), para. 71.
[44] La Rue Report (n 2), paras. 59 – 60.
[45] Emmerson Report (n 22), para. 11.
[46] *Id.*, para. 12.
[47] *Id*., para. 14.
[48] See in particular *Weber and Saravia v. Germany*, para. 106.
[49] See also Human Rights Committee, Concluding Observations (n 40), para. 24; Emmerson Report (n 22), paras. 45 – 50.
[50] Report on encryption and anonymity (n 5), para. 32.

and individuals should have the possibility to seek redress.[51] The State should also publish information, at least in aggregate, of the scope of communications surveillance techniques and powers.[52] Lastly, and as generally acknowledged under the Covenant, the State must ensure the right to effective remedies in case of abuse.[53]

22. The basic starting point is that the same standards must apply for the acquisition of data from foreign intelligence services, as are applicable for the domestic authorities to acquire information. This is based on the principle of effectiveness in the interpretation of the Covenant,[54] as a contrary position could lead State authorities to *de facto* outsource surveillance operations circumventing the protections afforded by the Covenant. Along these lines, the Human Rights Committee in its 2015 Concluding observations on the United Kingdom voiced concern over the "lack of sufficient safeguards in regard to the obtaining of private communications from foreign security agencies and the sharing of personal communications data with such agencies."[55] In sum, for the acquisition of intelligence from foreign authorities to be compatible with the requirements of the Covenant, the data acquired must be subject to the same requirements as the acquisition of data by domestic authorities provided that these, in turn, are compatible with the Covenant.

D. CONLCUSIONS

23. In light of the above analysis, the following conclusions can be derived:

a) Mass surveillance, intelligence sharing and the acquisition of communication involve significant interferences with human rights that must be subjected to the most rigorous scrutiny.

b) In the present case, the Grand Chamber has a unique opportunity to clarify the relationship between mass surveillance, communication interception and intelligence sharing regimes, and the freedom of opinion. The instant case presents fundamental questions such as the extent to which mass surveillance regimes affect the right to freedom of opinion and may therefore require remedial action. It may also provide an opportunity to clarify the significance of the freedom of opinion to the assessment of the compatibility of the United Kingdom surveillance regime with Articles 8 (2) and 10 (2) of the European Convention.

c) Based on the inherent risks that mass surveillance entails, the requirement of legality means that those affected may be given opportunities to understand fully the scope, nature, and application of the laws permitting communications surveillance.

d) The instant case provide ample reason to explore whether the rights interferences are wider than strictly necessary to protect the legitimate aims invoked for them.

---

[51] La Rue Report (n 2), para. 82.
[52] *Id*., para. 91.
[53] Cf. ICCPR Art. 2; General Comment no 31 (n 10), paras 15 - 19.
[54] Human Rights Committee, *Barbarín Mojica v. Dominican Republic* (Communication No. 449/1991) Views adopted on 15 July 1994, at para. 5.4.
[55] Human Rights Committee, Concluding Observations (n 40), para. 24.

Particularly, the proportionality assessment must take into account the collateral damage to collective rights to privacy, and the freedom of opinion and expression.

e) When assessing any restrictive measures, including safeguards against abuse, a high level of protection should be afforded for the confidentiality of sources. The threat posed to the protection of the confidentiality of sources should be part of the broader assessment of the proportionality of surveillance measures.

f) Intelligence sharing regimes should be subject to the same standards as rights interferences by the domestic authorities themselves, providing that the standards are fully compatible with human rights law.

Yours faithfully,

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression