NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

TÉLÉCOPIE · FACSIMILE TRANSMISSION

DATE: 16 September 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

E-MAIL:

DE/FROM: Karim Ghezraoui
Officer in Charge
Special Procedures Branch

FAX: +41 22 917 90 06
TEL: +41 22 917 91 47
E-MAIL: freedex@ohchr.org

REF:

PAGES: 10

COPIES:

OBJET/SUBJECT: **Intervention by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**

Please find attached the intervention of 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 Privacy International and Others v. the United Kingdom, Application no. 46259/16, before the European Court of Human Rights.

UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9000 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

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

IN THE EUROPEAN COURT OF HUMAN RIGHTS
First Section

Application no. 46259/16
Case of Privacy International and Others v. the United Kingdom
Referred to the First Section on 24 June 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 Application No. 46259/16. It shall address general principles applicable in the case, as interpreted from the perspective of the mandate of the Special Rapporteur established by the United Nations ("UN") Human Rights Council. The Special Rapporteur's mandate rests primarily upon Article 19 of the International Covenant on Civil and Political Rights ("the Covenant").[1] Leave to intervene was granted on 29 March 2019.

B. Background

The Special Rapporteur

2. Special Rapporteurs are independent experts appointed by the Human Rights Council. 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

[1] International Covenant on Civil and Political Rights, 999 UNTS 1057 (hereinafter: Covenant).

("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. 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, 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 UN, including the Human Rights Council or the Office of the High Commissioner for Human Rights, or any of the officials associated with those bodies.

C. Government surveillance and hacking risk serious interference with the international human rights to privacy and freedom of opinion and expression

4. Government hacking – or "the manipulation of software, data, a computer system, network, or other electronic device" without authorization from the organization or person responsible, and without the knowledge or permission of users[2] – and surveillance have long been concerns of civil society and inter-governmental organizations. The explosion of digital communications has given governments and corporations the ability to obtain information from individuals without their consent or even knowledge, and to monitor their use, examination, and dissemination of data and private information.[3] In recent years, State surveillance programs have expanded massively under the justification of counter-terrorism efforts.[4] The widespread deployment of unaccountable and secret State surveillance and hacking tools is not limited to any one nation, but rather is a growing global phenomenon.

5. The human rights mechanisms of the UN have expressed growing concern about the risks that State surveillance practices pose to universal human rights, particularly the rights to privacy and freedom of opinion and expression. As the UN High Commissioner for Human Rights emphasized in a recent report, the mere collection of data via State surveillance can interfere with these rights, regardless of whether the collected data is ever analyzed by a State actor.[5] In 2013, the UN General Assembly expressed grave concern that government surveillance interfered with the right to privacy in the digital age.[6] The General Assembly affirmed that the same rights that people enjoy offline are protected online. The resolution emphasizes that unlawful or arbitrary surveillance is "highly intrusive" and "violate[s] the rights to privacy and to freedom of expression and may contradict the tenets of a

---

[2] Access Now, A Human Rights Response to Government Hacking (available here: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf).
[3] United Nations Human Rights Council, '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, para. 1, (hereinafter: Report on encryption and anonymity).
[4] OHCHR, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin' (28 December 2009), UN doc. A/HRC/13/37, para. 20.
[5] "Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy." 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. 20 (hereinafter: High Commissioner Report).
[6] 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 (hereinafter: Resolution on privacy in the digital age).

democratic society."[7] It further calls upon all States "[t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection" to ensure that they are implementing their obligations under international human rights law.[8] It bears noting the context of this particular resolution: it was adopted just months after the revelations by American security analyst Edward Snowden of the United States' National Security Agency (NSA) and the United Kingdom's General Communications Headquarters (GCHQ) programs of surveillance allowing them access to "global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content."[9]

The right to privacy under the Covenant

6. Article 17 of the Covenant protects individuals against "arbitrary or unlawful interference with [one's] privacy, family, home, or correspondence". The previous Special Rapporteur on Freedom of Expression found that privacy rights involve protection of an area of autonomous development, interaction and liberty, free from State intervention.[10] The right includes an individual's ability "to determine who holds information about them and how that information [is] used."[11] "In order for individuals to exercise their right to privacy in communications," the Special Rapporteur continued, they must have the power to maintain communications that are "private, secure, and...anonymous," should they so choose.[12]

7. Under Article 17, surveillance measures must not engage in "and Governments are obligated to take specific measures to guarantee protection of the law against any such interference.[13] Moreover, the State has the burden of showing that any such interference is neither arbitrary nor unlawful.[14] Government hacking technologies "not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein," threatening the right to privacy.[15]

8. In a contemporary era in which digital communications are so fundamental to an extraordinary range of human activity, online privacy helps to secure the exercise of the freedom of opinion and expression.[16] Article 17 of the Covenant carves out permissible interferences with the right to privacy only in circumstances that are "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant," are in pursuit of "a legitimate aim," and that satisfy the requirements of "necessity and proportionality."[17] This test for permissible interference in the context of surveillance works in tandem with the one required for restrictions on freedom of expression under Article 19(3) of the Covenant, outlined below.

---

[7] *Id.*
[8] Resolution on privacy in the digital age, *supra* n. 6.
[9] High Commissioner Report, *supra* n. 5 at para. 4.
[10] 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. 22 (hereinafter: La Rue report).
[11] *Id*.
[12] *Id.*, para. 23.
[13] Covenant, *supra* n. 1 at Art. 17; High Commissioner Report, *supra* n. 5 at para. 34.
[14] Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (29 March 2004) UN doc. HRI/GEN/1/Rev.9, para. 6 (hereinafter: General Comment 31).
[15] La Rue report, *supra* n. 10 at para. 62.
[16] Report on encryption and anonymity, *supra* n. 3 at para. 16; La Rue report, *supra*, para. 24.
[17] General Comment 31, *supra* n. 16 at para. 6.

The right to freedom of opinion under the Covenant

9. Freedom of opinion and expression are closely connected rights that are vital for the full development of the person and a functioning society.[18] Restrictions on the ability to receive information and express ideas may interfere with one's ability to form and hold opinions.[19] Conversely, interference with one's holding of opinions inevitably restricts the ability for expression.[20] While interlinked, freedom of opinion and freedom of expression are separate rights with distinct legal implications under international human rights law.[21]

10. Article 19(1) of the Covenant protects the right to freedom of opinion. The right includes the freedom to form an opinion, to develop an opinion by way of reasoning, and to hold an opinion without interference.[22] Because opinions are of an utmost personal nature, reflecting the workings of one's mind and cumulations of their private thoughts, freedom of opinion requires freedom from any influence exerted by threat, coercion or the use of force, whether from private or State actors.[23] The right to hold an opinion without interference is a "fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction,"[24] and accordingly is an absolute right.[25] Even in a state of emergency, the Human Rights Committee has noted, a State may not derogate from its obligation not to interfere with the freedom of opinion.[26]

The right to freedom of expression under the Covenant

11. Article 19(2) of the Covenant provides a robust right to freedom of expression, emphasizing that "everyone shall have the right … 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."[27] The ability to seek, receive, and impart information include "the expression and receipt of communications of every form of idea and opinion capable of transmission to others," and is subject only to the narrow restrictions in Article 19(3).[28] "Regardless of frontiers" acknowledges the transboundary scope of this right, as information is often and sometimes inadvertently transmitted across state boundaries.[29] Additionally, "through any other media" encompasses electronic and Internet-based modes of expression, as technological development allows people around the world to receive and impart information through new technologies.[30]

12. While the right to freedom of expression may be restricted in exceptional circumstances, restrictions are only permissible if a State's action meets Article 19(3)'s three-part test, namely its requirements of legality, necessity, and legitimacy of objective.

    - First, any restriction on freedom of expression must be provided for by law. Any restriction must be formulated with sufficient precision to enable an individual to regulate his or her

[18] Human Rights Committee, 'General Comment No. 34: Article 19: Freedoms of opinion and expression' (12 September 2011) UN doc. CCPR/C/GC/34, para. 1 (hereinafter: General Comment 34).
[19] Report on encryption and anonymity, *supra* n. 3 at para. 19.
[20] *Id.*
[21] *Id.*
[22] Economic and Social Council, 'Report of the Special Rapporteur pursuant to Commision on Human Rights resolution 1993/45' (14 December 1994) UN doc. E/CN.4/1995/32, para. 19.
[23] *Id.*, para. 27.
[24] Report on encryption and anonymity, *supra n. 3*, para 19.
[25] General Comment 34, supra n. 18 at para. 9.
[26] General Comment 34, *supra* n. 18 at para. 5.
[27] Covenant, *supra* n. 1 at Art. 19(2).
[28] General Comment 34, *supra* n. 18 at para. 11
[29] Report on encryption and anonymity, *supra* n. 3 at para. 25.
[30] General Comment 34, *supra* n. 18 at para. 11; see also Resolution on privacy in the digital age, *supra* n. 6.

conduct accordingly and it must be made accessible to the public.[31] Any restriction may not be unduly vague or overbroad such that it could confer unfettered discretion on officials.[32]

- Second, the purpose must be for a legitimate objective. Article 19(3) highlights a set of objectives. Specifically, restrictions involve the respect of the rights or reputations or others, or for the protection of national security or of public order (*ordre public*), or of public health or morals.[33] These reasons may not be used by a State as sweeping justifications for mass surveillance. Restrictions "must be applied for the purposes for which they were prescribed and must be directly related to the specific need on which they are predicated."[34] Mere assertions of national security do not satisfy this requirement.[35] It is critical that independent courts provide oversight to ensure that interferences with freedom of expression actually serve the objectives for which they are claimed.

- Finally, restrictions on freedom of expression must be necessary to achieve a legitimate State objective. This means that the restrictions are appropriately tailored and use "the least intrusive instrument" to achieve the objective, and are "proportionate to the interest to be protected."[36] To satisfy the proportionality requirement, the State must identify "in specific and individualized fashion the precise nature of the threat," establish "a direct and immediate connection between the expression and the threat," and show the necessity and proportionality of the specific action taken in reaction to the threat.[37] Mass surveillance and hacking, including the use of interception technology like Trojans and malware that allows States to access devices, cannot generally satisfy the specificity and narrow application requirements of the necessity and proportionality standard.[38]

Access to a remedy for unlawful surveillance

13. In applying these standards to surveillance, national law is expected to provide certain safeguards and avenues to ensure a remedy.[39] First, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.[40] The judicial authority must be competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights involved, as well as have adequate resources in exercising their functions.[41] Second, 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."[42] If it would jeopardize the State's interest to notify beforehand, the State must notify the individual once surveillance has been completed and individuals should have the possibility to seek redress.[43] Third, the State should publish information, at least in aggregate, of the scope of communications surveillance techniques and powers, to provide "individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance."[44] State legislation must

[31] General Comment 32, *supra* no. 18. at para. 25.
[32] *Id.*
[33] Article 19(3).
[34] General Comment 34, *supra* n. 18 at para. 22.; European Convention on Human Rights, Article 18.
[35] 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, para. 18.
[36] General Comment 34, *supra* n. 18 at paras. 33-34.
[37] *Id.*, para. 35.
[38] 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.
[39] La Rue report, *supra* n. 10 at para. 81.
[40] Report on encryption and anonymity, *supra* n. 3 at para 32.
[41] Electronic Frontier Foundation, 'International Principles on the Application of Human Rights to Communications Surveillance' (available here: https://www.eff.org/files/necessaryandproportionatefinal.pdf).
[42] La Rue report, *supra* n. 10 at para. 82.
[43] *Id.*, para. 81.
[44] *Id.*, para. 92.

stipulate that communication surveillance "must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority."[45]

14. The Human Rights Committee addressed legislation permitting surveillance, interception and hacking in its 2017 concluding observations on Italy. The Committee recommended the State to implement independent and vigorous oversight systems to ensure compatibility of these measures with the Covenant.[46] In addition to obligations to provide a comprehensive legal framework to protect privacy, States have an obligation not to intrude on privacy themselves and also a resulting obligation to protect the privacy of individuals from third-party hackers.[47] Article 17(2) provides that "[e]veryone has the right to the protection of the law against such interference or attacks" and Article 2 imposes duties on States to uphold that specific right. Article 2(3)(a) provides that in order to redress for violations of the right to privacy, States must provide access to effective remedies. Victims of surveillance are often not even recognized as having suffered harm, much less given access to remedies.[48] Governments often reject requests from civil society organizations to investigate instances of surveillance, despite recognition from the European Court of Human Rights and the High Commissioner for Human Rights that the mere threat of surveillance, even when secret, coupled with the lack of remedy, can constitute an interference with the right to privacy.[49]

15. Additionally, the Guiding Principles on Business and Human Rights, adopted by the Human Rights Council in 2011, reaffirm the duty under Article 2 of the Covenant that States have an obligation to take appropriate steps to "prevent, investigate, punish, and redress human rights abuses by third parties."[50] In addition to the risks posed by State surveillance itself, against which the State must establish safeguards, such surveillance also puts the surveilled at risk for third-party interference. For example, encryption software allows individuals to protect data from digital surveillance by scrambling data to ensure that only intended recipients can actually access it.[51] In response, States often make concerted efforts to prevent encryption, effectively eliminating the most operational safeguard of digital security.[52] Releasing encrypted information can expose vulnerabilities in encryption, allowing third-party hackers access to the encrypted information.[53] States should consider this security risk in implementing safeguards and access to remedy.

D. The mandate has Seen a marked increase in concerns about the lack of legal control over surveillance

16. Despite the UN's repeated condemnation of State collection and analysis of private data,[54] many States continue to employ and advance their surveillance programs, often in conjunction with private actors.[55]

---

[45] *Id.,* para. 81.
[46] ICCPR, 'Concluding observations on the sixth periodic report of Italy' (1 May 2017) UN doc. CCPR/C/ITA/CO/6, para. 37.
[47] *Id.*, para. 27.
[48] *Id.*, para. 39.
[49] European Court of Human Rights, Roman Zakharov v. Russia (application No. 47143/06), judgment of 4 December 2015, para. 171; High Commissioner Report, *supra* n. 5 at para. 20.
[50] HRC, 'Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie' (21 March 2011) UN doc. A/HRC/17/31, para. 10.
[51] See SANS Institute, 'History of encryption' (2001).
[52] *Id.*
[53] Report on encryption and anonymity, *supra* n. 3; Abelson, Harold, et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications*, MIT-CSAIL-TR-2015-026 (accessed at http://hdl.handle.net/1721.1/97690).
[54] La Rue report, *supra* n. 10 at para. 15.
[55] Private companies often play a significant role in facilitating State surveillance programs. In 2012, the International Federation on Human Rights and the French Human Rights League called for the prosecution of French companies for providing surveillance to Syria, possibly through German and Italian

Other United Nations special rapporteurs and I are frequently called upon to respond to concerns about State surveillance measures and legislation, and to relevant allegations of human rights abuses. We do so by communicating our concerns directly to governments in an effort to understand more fully the nature of their interferences with freedom of expression, if such interference exists, and the reasons for such interferences. In this section, I will share some recent and current instances of concerning State surveillance practices around the world that I, and others, have addressed.

17. As a general matter, I most recently raised concerns about the widespread use of private surveillance tools – principally hacking and other spyware – to interfere with individual privacy and freedom of expression.[56] In a 2019 report to the Human Rights Council, I recognized that States frequently purchase a wide range of intrusive surveillance programs from private actors that allow surreptitious access to the data, communications, location history, and activities of targeted individuals.[57] I underscored that, although the Guiding Principles direct all companies to respect human rights and apply due diligence when qualifying human rights impacts, private surveillance companies have failed to meet these guidelines.[58] To address the problem, I called for a moratorium on the export and sale of targeted surveillance technologies.[59] I further urged States to reinforce domestic laws limiting surveillance in accordance with international standards, to establish oversight for surveillance mechanisms, and provide victims with tools for legal redress against violations.[60]

18. My mandate and others have also addressed these kinds of concerns with respect to specific State allegations. For instance, it has been alleged that, since 2012, the Lebanese General Security Directorate, based in Beirut, has been conducting large-scale surveillance and cyber espionage via a spyware program called Dark Caracal.[61] The program allegedly conducted "spear phishing" attacks, tricking users into downloading fake versions of popular applications and in some cases, obtaining personal communications and data. The Special Rapporteur on the Right to Privacy and I raised concerns that the program was violating domestic and international law, especially as the program lacked legal basis and used invasive hacking techniques without public criteria and judicial safeguards, seemingly operating beyond the bounds of international standards for due process and accountability.

19. A 2015 draft of the United Kingdom's Investigatory Powers Bill drew attention from several mandates as the law permitted bulk warrants, data decryption, and warrants for communications between journalists and sources.[62] Along with the Special Rapporteur on Peaceful Assembly and of Association and the Special Rapporteur on the Situation of Human Rights Defenders, I underscored that communication surveillance must occur under exceptional circumstances, under the supervision of a judicial authority, and that the surveillance of communications data must be pursuant to oversight by an independent authority. I also noted that the vague bases for warrants – including national security, preventing or detecting serious crime, or the interest of State economic well-being – were not tied to specific offenses and presented potential for abuse. I also expressed concern about the impact that State ability to remove encryption on data and communications would have on the protection and security of communications.

---

intermediaries. I have previously called for a moratorium on the international sale and transfer of the tools of the private surveillance industry. See HRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (28 May 2019) UN doc. A/HRC/41/35, para. 24(a) (hereinafter: Private surveillance report). para. 2; see also Amnesty International submission to the Special Rapporteur, 'The Surveillance Industry and Human Rights', pg. 2 (available here: https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf) ; International Federation of Human Rights, 'The Surveillance Industry and Human Rights', pg. 2 (available here: https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/FIDH.pdf).

[56] Private surveillance report, *supra* n. 56.

[57] *Id.*, para. 7.

[58] *Id.*, paras. 30-31.

[59] *Id.*, para. 49.

[60] *Id.*, paras. 50-54.

[61] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=23831

[62] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=15850

20. In 2015, I commented on China's proposed Cybersecurity Law, expressing concern about limitations on Internet activity, restrictions on the right to anonymity, and broad surveillance authority.[63] I emphasized that the Law's grant of broad authority to the State for national security and public order purposes had tremendous potential to restrict the freedom of opinion. The Law's stringent requirement that users provide real identity information to network providers conflicted with the rights to freedom of opinion, expression, and privacy. The Law's provision that "citizens' personal data and other important data" would be stored on the Chinese mainland lacked sufficient clarity and may have caused a chilling effect that curbed free expression.

21. In 2015, alongside four other special rapporteurs, I expressed concerns about French legislation authorizing government officials to obtain communications, data in transit, and metadata.[64] We specifically raised concerns about the program's oversight by a government official as opposed to an independent judiciary, the legislation's lack of explanation regarding how data would be stored or shared with French or foreign agencies, and the lack of judicial oversight for such practices. Also problematic was the legislation's grant of authority to the French government to use communication surveillance techniques, particularly for international communications, without sufficient prior judicial oversight.

22. I further raised concerns regarding Pakistan's "Prevention of Electronic Crimes Act," finding that the law granted government authorities exceedingly broad powers to inspect information systems, demand information, code, or use technology to unencrypt data.[65] The law also allowed authorities to demand that telecommunications providers turn over traffic data. I noted that the legislation used overbroad, vague language and permitted a restriction on Internet access without judicial control, which in turn could have institutionalized violations of essential rights within Pakistani law. The law also threatened vulnerable groups, such as media workers and journalists, for whom expansive State surveillance could result in censorship or self-censorship.

23. Together with the Special Rapporteur on the Situation of Human Rights Defenders and the Special Rapporteur on the Independence of Judges and Lawyers, I responded in 2016 to a draft of a German law pertaining to surveillance of communications by non-German citizens.[66] The law, as then written, authorized the bulk surveillance of non-German citizens and institutions, and established surveillance procedures to target those groups. The bases for bulk data collection – including threats to internal and external security, protection of Germany's capability to act, and findings concerning significant policy issues – were insufficiently clear that we feared the legislation was neither necessary nor provided for by law. The agencies performing the surveillance appeared to be granted unfettered discretion in determining the scope, nature, and viability of security threats, creating the potential for German intelligence agencies to conduct surveillance on non-German citizens and institutions not suspected of having engaged in any illicit activity.

24. The above-mentioned responses are just some examples reflecting growing human rights concerns posed by the use of various surveillance techniques by States. They demonstrate ongoing concern about State surveillance efforts and their widespread potential for abuse. Other mandate holders and I continue to recommend clear, publicly accessible laws that are both necessary and proportionate to achieve explicitly stated State aims, as well as judicial and independent oversight for intelligence agencies implementing surveillance programs.

[63] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=14423
[64] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=15049
[65] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=22604.
[66] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=3316

E. Conclusion

25. The present case offers an opportunity for the Court to provide global guidance for the practice of government surveillance. As a leading court on the application of human rights, this Court represents the highest standard to which other courts, agencies, and non-government organizations turn for human rights decisions. Special note should be made that the United Kingdom is a member of the Five Eyes intelligence agencies, and a recognized leader in the area of State surveillance. By guiding the United Kingdom on its surveillance and privacy policies, this Court would provide both concrete guidelines to the leading intelligence agency pact, as well as offer precedent for other nations. This Court's decision will prove essential to building surveillance jurisprudence and to furthering the abilities of other courts, human rights institutions, and non-governmental organizations to advance the rights to privacy, opinion, and expression in the context of surveillance and hacking. As technology grows, surveillance practices will continue to grow with it. Any decision by the European Court of Human Rights in this case will have a lasting and cognizable impact on the protection and expression of human rights globally.

Yours faithfully,

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