European Court of Human Rights

***Mikolaj PIETRZAK v. Poland*, Application No. 72038/17**
***Dominika BYCHAWSKA-SINIARSKA ao v. Poland*, Application No. 25237/18**

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL, ARTICLE 19 AND THE ELECTRONIC FRONTIER FOUNDATION

Introduction and summary of intervention

1. This intervention is submitted by Privacy International (PI), ARTICLE 19 and the Electronic Frontier Foundation (EFF) pursuant to leave granted by the President of the Section in accordance with Rule 44(3) of the Rules of the Court. PI is a human rights organization that works globally at the intersection of modern technologies and rights, and is dedicated to promoting the right to privacy globally. ARTICLE 19 is an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. EFF is a non-profit legal and policy organization that safeguards freedom of expression, privacy and innovation in the digital world.

2. This submission aims to contribute to the development of this Court's jurisprudence under Article 8 of the European Convention on Human Rights (the "Convention"), with particular reference to surveillance, data collection and analysis in the context of advancements in technology. The regulation of secret surveillance measures, in accordance with Article 8(2) of the Convention, today requires taking into account the unprecedented level of intrusions to privacy that new technologies increasingly enable, including access to communications metadata and subscriber data (collectively, "communications data"). These secret surveillance measures do not only significantly interfere with the right to privacy. They also have a chilling effect on the freedom of expression of journalists, NGOs, activists and lawyers, among others.

3. The interveners will confine this intervention to addressing the following:
    1. Access to communications data can be as intrusive as content;
    2. Direct and unrestricted access to communications data constitutes a serious interference with the right to privacy;
    3. Minimum and additional safeguards necessary to ensure compliance with the requirements of Article 8, including judicial authorisation and notification;
    4. The impact of secret surveillance on the activities of civil society organisations; and
    5. Victim status.

1. Access to communications data (including metadata and subscriber data) can be as intrusive as content

4. Communications data, including metadata and subscriber data, describe any data apart from the content of a communication.[1] This data makes it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication originated. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

5. When collected in aggregate about one or a number of individuals, it is no less – and can be even more – sensitive than the actual content of a communication. For example, a person visits an IP address, hosting a medical self-diagnosis website, followed by a visit to their doctor's website, followed by a telephone call to an oncologist, followed by an appointment with a private client solicitor and then a hospice may reveal that the person in question has terminal cancer.[2]

6. The understanding that metadata can be as intrusive as content has been long recognised by Courts and expert bodies. This Court has recognised that the collection of communications "metadata" is no less intrusive than collecting content.[3] It explained that "the patterns that will emerge" through metadata are "capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with".[4]

7. Similarly, the Court of Justice of the European Union (CJEU), in *Tele2/Watson*, regarding communications data retention, concluded that the distinction between content and communications data or traffic data is, in fact, no longer fit for purpose.[5] This premise has been also recognised by international intergovernmental bodies, including the UN General Assembly and UN Human Rights Council[6], as well as, independent experts, such as the UN High Commissioner for Human Rights and the Council of Europe Commissioner for Human rights[7].

8. In the US, the US Court of Appeals for the Second Circuit found that:

---

[1] This data includes, but is not limited to: the who, what, when, and where of our communications, map searches, visited websites, as well as information, including technical identifiers, about every device connected to every network.

[2] PI, "Video explaining Metadata", https://www.youtube.com/watch?v=xP_e56DsymA; EFF, "Why metadata matters", 7 June 2013, https://www.eff.org/deeplinks/2013/06/why-metadata-matters; PI, "How intrusive is communications data?", 21 August 2019, https://privacyinternational.org/long-read/3176/how-intrusive-communications-data.

[3] ECtHR, *Big Brother Watch and Others v. UK*, Appl. Nos. 58170/13, 62322/14 and 24960/15, Judgment, 13 September 2018, para. 356. Earlier see also, ECtHR, *Uzun v. Germany*, Appl. No. 35623/05, Judgment, 2 September 2010, paras. 44-69.

[4] *Big Brother Watch* ao, note 3, para. 356 (see also para. 301).

[5] CJEU, Joined cases *Tele2 Sverige AB v Post-och telestyrelse*n and *Secretary of State for the Home Department v Tom Watson*, Cases Nos. C–203/15 and C–698/15, Judgment, 21 December 2016, paras. 99-101; CJEU, Joined cases *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others*, Cases Nos. C-293/12 and C-594-12, Judgment, 8 April 2014, para. 27.

[6] UN General Assembly, Resolution on the Right to Privacy in the Digital Age, UN Doc. A/RES/73/179, 17 December 2018; UN Human Rights Council, Resolution on the right to privacy in the digital age, UN Doc. A/HRC/RES/34/7, 7 April 2017, See for further sources, PI, Guide to International Law and Surveillance 2.0, February 2019, https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf.

[7] UN Office of the High Commissioner for Human Rights (OHCHR), "Report on the right to privacy in the digital age", UN Doc. A/HRC37/27, 30 June 2014; Council of Europe, Commissioner for Human Rights (CoE ComHR), Issue Paper on "The rule of law on the Internet and in the wider digital world", 2014, https://rm.coe.int/16806da51c, p. 113.

> That telephone metadata do not directly reveal the content of telephone calls, however, does not vitiate the privacy concerns arising out of the government's bulk collection of such data. Appellants and amici take pains to emphasize the startling amount of detailed information metadata can reveal – 'information that could traditionally only be obtained by examining the contents of communications' and that is therefore 'often a proxy for content.' ... Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships.[8]

9. Therefore, communications data, including metadata, should enjoy at least the same protections as content and access to this data should be subject to the same conditions and protections as any other personal information.

2. Direct and unrestricted access to communications data constitutes a serious interference with the right to privacy

10. Online communications, through mobile phones, but also other connected devices, are an inextricable part of everyone's day-to-day lives today. People rely and put trust in their connected devices. Their communications data reveals so much about their identity, saying more about them than themselves perhaps realise. The communications data does not just relate to the one individual, the owner, but includes personal information related to friends, family, employers and colleagues. Therefore, police and intelligence agencies should have neither direct nor unrestricted access to this data.

11. Mobile phone ownership is at its highest level globally. In the UK alone, the vast majority of people own at least one mobile phone and carry that phone with them wherever they go.[9] This means that with direct access the police can follow everyone wherever they go. Direct and unrestricted access to communications data is, therefore, akin to giving the police and intelligence agencies a master key (*passepartout*) to open the door to every house any time they wish without a search warrant or other form of oversight. Yet in many European countries, the law on access to communications data remains woefully inadequate and open to abuse.

12. This Court has underlined that "the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."[10]

13. The access of the competent national authorities to communications data constituted a further interference with those fundamental rights, which the CJEU considered to be "particularly serious".[11] The fact that data was used without the subscriber or registered user being informed

---

[8] *American Civil Liberties Union* ***v.*** *Clapper*, 785 F.3d 787 (2d Cir. 2015).

[9] According to Deloitte's 2019 Mobile Consumer Survey, 89% of respondents (spanning the ages of 18-75 years) owned or had ready access to a smartphone. And of those who owned a smartphone, 95% reported using it at least once in the last day. Deloitte, "Global Mobile Consumer Survey 2019: UK cut", 2019, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology-media-telecommunications/deloitte-uk-plateauing-at-the-peak-the-state-of-the-smartphone.pdf.

[10] ECtHR, *S. and Marper v. UK*, Appls. nos. 30562/04 and 30566/04, Judgment, 4 December 2008, para. 112.

[11] *Tele2/Watson*, note 5, para. 100. See more recently, CJEU underlined that "national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society". CJEU, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs ao*, Case C-623/17, Judgment, 6 October 2020, para. 81.

was, according to the CJEU, likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance.

14. As a result, police and intelligence agencies should never have direct and unrestricted access to this data. Any access to communications data, including metadata, should be limited to specific conditions, such as only to fight off a serious crime, and should be subject to independent authorisation. Not only minimum but also additional safeguards should apply to regulate the access, collection and use of communications data. These additional necessary safeguards are described in more detail below.

3. Minimum and additional safeguards necessary to ensure compliance with requirements of Article 8

15. In *Weber*, this Court set out minimum necessary safeguards that must apply to any type of secret surveillance, including counter-terrorism legislation. Specifically any secret surveillance measure, including access to metadata, should respect "the following minimum safeguards that should be set out in statute law in order to avoid abuses of power": the nature of the offences; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of such measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[12]

16. These safeguards should cover all persons under the jurisdiction of the state irrespective of their nationality or other distinctive characteristic. According to Article 1 ECHR, "everyone" within the jurisdiction of a contracting party benefits from the rights and freedoms enumerated in the Convention. "Human rights are rights held simply by virtue of being a human person".[13] Nationality cannot be a criterion for lessening the safeguards applicable to secret surveillance measures, including the requirement of prior judicial authorisation.

17. The interveners submit that in order to ensure that Convention rights remain effective, it is key to ensure that the following additional necessary safeguards are also provided when governments interfere with the right to privacy by accessing communications data. These additional safeguards become imperative particularly when secret surveillance measures involve extreme and unprecedented intrusions to privacy.

a. Reasonable suspicion should always be the basis for any interference with the right to privacy

18. An authorisation should not focus only on the necessity and proportionality of a particular operation, but also on whether there is reasonable suspicion. In *Szabó*, the Court noted the requirement of "a sufficient factual basis for the application of secret intelligence gathering measures ... on the basis of an individual suspicion regarding the target person" as critical for "the authorising authority to perform an appropriate proportionality test".[14]

[12] ECtHR, *Weber and Saravia v. Germany*, Appl. No. 54934/00, Decision, 29 June 2006, para. 95.
[13] R. Higgins, *Problems and process, international law and how we use it* (1994), p. 96.
[14] ECtHR, *Szabó and Vissy v. Hungary,* App. No. 37138/14, Judgment, 12 January 2016, para. 71.

19. Similarly, in *Zakharov*, the Grand Chamber held that the authorisation procedure

> must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.[15]

20. The interveners submit that the same principle should apply when accessing communications data.

b. Any interference with the right to privacy should be subject to authorisation by an independent judicial authority

21. Intrusive, secret surveillance measures, like those at issue here, should be subject to authorisation by an independent judicial authority. In *Zakharov*, this Court referred to approval of authorisation by a non-judicial authority "provided that that authority is sufficiently independent from the executive."[16] The Court repeated the principles in *Szabó*:

> in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exceptions, warranting close scrutiny ... supervision by a politically responsible member of the executive, such as the Minister for Justice, does not provide the necessary guarantees.[17]

It added that Independent, "preferably judicial," review "reinforce[s] citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained".[18]

22. The same approach was taken by the CJEU.[19] Specifically in *Digital Rights Ireland,* the CJEU concluded that the 2006 Data Retention Directive ("Directive 2006/24"), which required communications service providers to retain customer communications data in bulk for up to two years for the sake of preventing and detecting serious crime, breached the rights to privacy and data protection under Articles 7 and 8 respectively of the EU Charter of Fundamental Rights.[20] The CJEU noted that the Directive 2006/24 did not contain sufficient substantive and procedural safeguards governing the access and use of retained data. In particular, it highlighted that "the access by the competent national authorities is not made dependent on a prior review carried out by a court or by an independent administrative body".[21] This requirement for independent authorisation has been further confirmed by international human rights bodies.[22]

23. The interveners submit that a system of prior judicial authorisation would minimise unnecessary or disproportionate interferences with privacy. A limited post-authorisation oversight regime that

---

[15] ECtHR, *Zakharov v. Russia*, App. No. 47143/06, Judgment, 4 December 2015, para. 260.
[16] *id*., para. 258. In *Weber*, across party and independent commission of the German Parliament approved surveillance and the selectors applied. *Weber,* note 12.
[17] *Szabó ao,* note 14, para. 77.
[18] *Szabó ao,* note 14, para. 79.
[19] *Tele2/Watson*, note 5, para. 120; *Digital Rights Ireland*, note 5, para. 62.
[20] *Tele2/Watson*, note 5, para. 236. See also, *Digital Rights Ireland*, note 5.
[21] *Digital Rights Ireland*, note 5, para. 62.
[22] UN Human Rights Committee, Concluding observations on the fifth periodic report of Belarus, UN Doc. CCPR/C/BLR/CO/5, 22 November 2018; UN OHCHR, Report on the right to privacy in the digital age, UN Doc. A/HRC/39/29, 3 August 2018; CoE ComHR, "Memorandum on surveillance and oversight mechanisms in the UK", CommDH(2016)20, 17 May 2016, para. 28 (referring to the Venice Commission's Report on Democratic Oversight (2007)).

only examines a restricted breadth of information is not sufficient. This is particularly the case when there is no complaint mechanism available to challenge such interferences.

c. Any interference with the right to privacy should be subject to independent and effective oversight

24. State surveillance of communications should be subject to independent, effective, adequately resourced and impartial domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability.[23] In *Big Brother Watch ao*, this Court highlighted that "the search criteria and selectors used to filter intercepted communications should be subject to independent oversight".[24]

25. As the UN High Commissioner for Human Rights noted, effective oversight should ensure that:

> Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.[25]

26. The interveners submit that effective oversight cannot be limited to an automatic and superficial review of the reported interferences, without the ability to review all available information and authority to issue binding decisions.

d. Subjects of secret surveillance should always be notified (even if *post facto*)

27. There is today an increasing consensus that notification requirements are necessary to enable individuals who are subjected to secret surveillance measures to challenge unlawful surveillance decisions. This Court has consistently recognised the importance of notification as both an adequate safeguard against the abuse of surveillance powers under Article 8 and as part of the right to an effective remedy under Article 13.[26] In *Weber,* the Court noted that there is "in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".[27]

28. The CJEU in a recent judgment added that:

> [a]ccording to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to

[23] id. See also UN General Assembly, Resolution on the Right to Privacy in the Digital Age, UN Doc. A/RES/73/179, 17 December 2018.
[24] *Big Brother Watch ao*, note 3, para. 346.
[25] UN OHCHR, Report, note 22, para. 40. See also ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, App. No. 62540/00, Judgment (28 June 2007), para. 85.
[26] *Szabó,* note 14, para. 86. See also, *Association for European Integration and Human Rights ao,* note 25, para. 91.
[27] *Weber,* note 12*,* para. 135.

personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.[28]

29. International human rights bodies and experts, including the UN High Commissioner for Human Rights, have repeatedly underlined the significance of notification to ensure effective remedy of violations of the right to privacy.[29]

30. As to when, practicably, an individual should be notified, this Court has acknowledged that "as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned".[30]

31. A consideration of other countries' legislation shows that notification is both common and possible. The following countries all have some form of notification provision: Austria;[31] Belgium;[32] Canada;[33] Chile;[34] The Czech Republic;[35] Cyprus;[36] Estonia;[37] Finland;[38] Germany;[39] Hungary;[40] Iceland;[41] Ireland;[42] Japan;[43] Montenegro;[44] The Netherlands;[45] New Zealand;[46] Peru;[47] Slovenia;[48] South Korea;[49] Switzerland;[50] Taiwan;[51] and the United States of America.[52]

32. The majority of the above listed countries are members of the Council of Europe. This Court has previously noted that "the strong consensus existing among the Contracting States (…) is of

[28] CJEU, *Data Protection Commissioner v. Facebook Ireland and Schrems (Schrems II)*, Case C-311/18, Judgment, 16 July 2020, para.187. See also, Tele2/Watson, note 5, para. 121.
[29] The right to privacy in the digital age, UN Doc. A/HRC/27/37, 30 June 2014, para 47; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40, 17 April 2013, para. 82; Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression, 21 June 2013, para. 5.
[30] *Weber,* note 12*,* para. 135. Further, this Court has, in past cases, taken note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without their knowledge, and unless the data is deleted, they should be informed, where practicable, that information is held about them as soon as the object of the police activities is no longer likely to be prejudiced. *Zakharov,* note 15, para. 287.
[31] Code of Criminal Procedure of the Republic of Austria 1975, Annex 2 (138).
[32] Belgium, Constitutional Court Case No. 145/2011 at paras 88 and 92.
[33] Canadian Criminal Code 1990, Part VI: Invasion of Privacy s 196(1).
[34] Code of Criminal Procedure, Art 244.
[35] Amendment Code of Criminal Procedure No. 177/2008 (information withheld only if this is in the interest of public security, crime prevention, health protection or the protection of the rights and freedoms of others).
[36] Law 1996 (92(I)/1996) (Amended by) Law 2015 (N. 216(I)/2015), Article 17.
[37] The Security Authorities Act, Article 29.
[38] Chapter 10, section 60 of the Finnish Coercive Measures Act.
[39] German Code of Criminal Procedure 1987, Article 101.
[40] Act on Criminal Proceedings XIX 1998, Title V, s 205(5).
[41] Code of Criminal Procedure No.88/2008, Article 85.
[42] Criminal Justice (Surveillance) Act 2009, s 10(3).
[43] Law on wiretapping for criminal investigations (Act No. 137 of 1999)
[44] Criminal Procedure Code 2009, Article 162.
[45] The Intelligence and Security Services Act 2017 (Wiv 2017), Article 59.
[46] Search and Surveillance Act 2012, Part 3, 61(c)
[47] The Criminal Procedure Code, Article 231.
[48] Criminal Procedure Code, Article 154.
[49] Protection of Communications Secrets Act 2002, Article 9-2.
[50] Federal Act on the Intelligence Service 2015, Article 33.
[51] 5 Communications Protection and Surveillance Act 1999, Article 15.
[52] 18 U.S. Code § 2518.

considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere."[53]

33. Countries have been able to develop notification procedures which do not compromise ongoing investigations. Many provisions use language that permits notification if it does not "endanger the aim" of the restriction (Estonia); "if it does not interfere with the intelligence operation" (Belgium); or if disclosure is "unlikely to hinder the investigation in future of such offences" (Ireland). Some countries require the decision of a court to justify not notifying the person (such as Switzerland, the United States, Taiwan and Montenegro). This can be at the judge's own initiative, or on application by a prosecutor.

34. Most frameworks identify timeframes. Slovenia assumes notification should be made if the prosecutor does not act on material collected within two years. Japan and South Korea require notification within 30 days. Some, like Ireland, allow the relevant Minister to enact regulations addressing the details.

35. As such, these examples of legislation indicate that it is possible to design a mechanism that appropriately balances the respective interests: protecting the investigation and ensuring that surveillance measures are not outside legal challenge.

36. The interveners submit that it is key that this Court concludes that notification is a necessary safeguard in cases of secret surveillance, as it is necessary having regard to the recent, rapid changes in communications technology; it is consistent with the development of international law; it is consistent with the comparative experience of a wide range of jurisdictions, including Canada, Germany and Sweden and the United States and it is consistent with the Court's own case law, in particular the requirement that any restriction on the right to privacy or the right to an effective remedy should not impair the very essence of the right.

37. The interveners do not submit that notification of surveillance is an absolute right in the sense that it should operate without restrictions. Rather, any restriction on notification should be strictly limited, i.e. it should only be delayed where it would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life. Any such delay in notification, moreover, must be judicially authorised and subject to continuing judicial oversight. The burden must be on the government to satisfy an independent and impartial tribunal that continued non-notification is both necessary for a legitimate aim and proportionate.

4. Enhanced protections for civil society communications is necessary

38. The knowledge that intelligence agencies may use their interception powers and capabilities to capture civil society organisations communications have a profound chilling effect on their exercise of freedom of expression in two ways:

i. First, it endangers the public watchdog function of civil society organisations by undermining the way in which they operate. They report on human rights violations, illegalities and other wrongdoings, both locally and worldwide. In order to do so, they rely on the willingness of others to pass them information in confidence, sometimes at their risk to their own lives. The

[53] *S. and Marper*, note 11, para. 112.

knowledge that intelligence services may intercept those communications – not to mention pass on their contents to a foreign government – is bound to diminish that willingness of people in other countries will have to communicate with civil society. As sources of information dry up, civil society organisations are less likely to be able to report on human rights violations and other social issues and; consequently, they will be less able to hold governments to account.

ii. Secondly, there is a very real risk that the communications of activists, whistleblowers, journalists or other non-governmental organisations (NGO)s' informants may be passed on to a foreign government with further risks of retaliation for the individuals concerned. Again, these concerns are not purely theoretical. It has emerged in some deportation cases, for instance, that the UK government wanted to retain the discretion to pass on information about activists to foreign governments such as Algeria.[54]

39. In other words, secret surveillance programmes dramatically undermine the protection of organisations' sources and their ability to carry out their work. If civil society organisations are to perform their public watchdog function, which the Court itself has recognized,[55] they must be able, like journalists, to guarantee the anonymity of their sources and the confidentiality of their communications. The chilling effect of surveillance measures on the exercise of freedom of expression is not limited to NGOs or journalists, however. It can equally have a strong negative impact on the ability of professions who rely on privileged communications to carry out their work. In its most recent *Privacy International* judgment of 6 October 2020, the CJEU held:[56]

> 72. It should also be noted that the transmission of traffic data and location data to public authorities for security purposes is liable, in itself, to infringe the right to respect for communications, enshrined in Article 7 of the Charter, and to deter users of means of electronic communication from exercising their freedom of expression, guaranteed in Article 11 of the Charter. Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistle-blowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ 2019 L 305, p. 17). Moreover, that deterrent effect is all the more serious given the quantity and breadth of the data retained.

40. The interveners submit that the particularly serious deterrent effect of surveillance measures on civil society organisations and lawyers calls at the very least for enhanced safeguards against collection and/or access to their communications data. This would also be consistent with existing law and countries in some Council of Europe Member States such as the United Kingdom[57] or France.[58]

41. In summary, it is essential for any surveillance legal framework to include at least special protections for the communications data of civil society organisations, similar to those enjoyed by lawyers and the press. In particular, the collection of these groups' metadata should only be ordered by a judge and be made subject to stringent requirements as regards access, permitted uses, preservation, retention and destruction of such data.

---

[54] *W (Algeria) v. Secretary of State for the Home Department* [2012] UKSC 8.
[55] ECtHR, *Vides Aizsardzības Klubs v. Latvia*, Appl. No. 57829/00, Judgment, 27 May 2004, para. 42. See also more recently, *Szabó ao,* note 14, para. 38.
[56] *Privacy International,* note 11, para. 72.
[57] See e.g. sections 26-29 Investigatory Powers Act 2016.
[58] See e.g. article L-821-7 du Code de la sécurité intérieure.

5. Victims status

42. In instances where an applicant has been unable to prove that they have been subjected to measures of secret surveillance, the Court has clarified conditions under which applicants can claim to be a victim. This avoids an "unacceptable" situation in which the assurance of the enjoyment of a right guaranteed by the Convention is removed by the simple fact that the person concerned is kept unaware of the violation.[59]

43. In considering the scope of legislation permitting secret surveillance measures, this Court's consistent case law requires consideration of whether

> the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted.[60]

44. Where an applicant is challenging the general legal framework for secret surveillance measures, this Court has identified the availability of an effective domestic remedy as a relevant factor in determining whether that applicant was a "victim" of the alleged violation.[61] In the context of covert surveillance, "the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts".[62]

45. The interveners submit that this Court should recognise that the right to notification is necessary for remedies to be considered practical and effective under Article 13 of the Convention.

14 October 2020

On behalf of the Interveners

Dr. Ilia Siatitsa
Legal Officer
Privacy International
London EC1M 5UY

[59] ECtHR, *Klass and Others v. Germany*, App. No. 5029/71, Judgment, 6 September 1978, para. 36.
[60] *Zakharov,* note 15, para.171. A similar conclusion on victim status was reached by the Court in *Big Brother Watch ao*, note 3.
[61] *Big Brother Watch ao*, note 3, para. 249.
[62] *Zakharov,* note 15, para. 234.