IN THE EUROPEAN COURT OF HUMAN RIGHTS
APP NO. 24960/15
BETWEEN:-

Applicant

10 Human Rights Organisations

- v -

Respondent Government

United Kingdom

THIRD-PARTY INTERVENTION SUBMISSIONS BY ARTICLE 19

---

1. This third-party intervention is submitted on behalf of ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19), 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. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally.

2. ARTICLE 19 welcomes the opportunity to intervene as a third party in this case, by leave of the President of the Court, which was granted on 08 February 2016 pursuant to Rule 44 (3) of the Rules of Court. These submissions do not address the facts or merits of the applicants' case.

3. In our view, this case concerns not only the compatibility of the UK surveillance regime with the right to private life under Article 8 of the Convention, it also raises fundamental issues for the right to freedom of expression ('freedom of expression') under Article 10 of the Convention. We believe that this case therefore presents the Court with an important opportunity to affirm that the indiscriminate interception, storage and analysis of online communications has a chilling effect on the freedom of expression of non-governmental organisations ('NGOs'). In these submissions, ARTICLE 19 addresses the following: (i) the principle of source protection for NGOs in the case law of the Court; (ii) the practical importance of source protection for NGOs; (iii) the inherent chilling effect of bulk interception capabilities and powers on NGOs' freedom of expression; (iv) international criticism of bulk surveillance powers; (v) emerging consensus on the required legal safeguards for the protection of the right to privacy in the context of surveillance.

I. NGOs ENJOY EQUAL PROTECTION FOR THEIR SOURCES AS THE PRESS

4. The European Court of Human Rights has long recognised that NGOs perform an important public watchdog function equivalent to that of the press. In *Steel and Morris v the United Kingdom*, no. 68416/01, para. 95, 15 February 2005, the Court noted "*the legitimate and important role that campaign groups can play in stimulating public discussion*". In *Társaság a Szabadságjogokért v Hungary*, no 37374/05, para. 27, 14 April 2009, the Court went further and considered that the applicant organization, which was involved in the protection of the right to information, *"[could] be characterised, like the press, as a social "watchdog.""* The Court has further recognised the important role of NGOs in holding governments to account in cases involving NGOs specializing in environmental issues (*Vides Aizsardzības Klubs v. Latvia*, no. 57829/00, para. 42, 27 May 2004), animal rights groups (*Animal Defenders International v United Kingdom*, [GC], no. 48876/08, para. 103, 22 April 2013) and NGOs working on ensuring respect for human rights, democracy and the rule of law (*Youth Justice Initiative for Human Rights v Serbia*, no. 48135/06, 25 June 2013).

5. One of the important corollaries of NGOs' public watchdog functions, is that, like the press, they must be able to disclose facts in the public interest, comment on them and contribute to the transparency of the activities of public authorities (*Vides Aizsardzības Klubs,* cited above, para.42). More generally, they must benefit from the same Convention protection to that afforded to the press (*Társaság a Szabadságjogokért v Hungary*, no 37374/05, para. 27, 14 April 2009).

6. ARTICLE 19 submits that in circumstances where NGOs draw attention to matters of public interest, such as human rights violations, they should benefit from the same legal protections as the press, including the protection of journalistic sources (see, *mutatis mutandis, Társaság a Szabadságjogokért v Hungary*, no 37374/05, para. 27, 14 April 2009). As the Court noted in *Társaság a Szabadságjogokért, "[t]he function of the press includes the creation of forums for public debate. However, the realisation of this function is not limited to the media or professional journalists"*. ARTICLE 19 therefore invites the Court to make clear that any person or organisation, who is regularly or professionally engaged in the collection and the dissemination of information to the public via any means of communication is entitled to the same protection.[1] As we shall demonstrate in the following section, such protection is especially important in the case of NGOs, whose reporting and advocacy depends on individuals coming forward with information.

II. THE IMPORTANCE OF SOURCE PROTECTION FOR NGOs

7. For NGOs, the protection of sources and the confidentiality of communications is vital to the proper exercise of their function as public watchdog. NGOs work tirelessly both domestically and around the world to investigate and denounce human rights violations and other social ills. As a free speech organization, ARTICLE 19 routinely deals with activists, whistleblowers and human rights defenders, who rely on us to protect them and denounce the violations of freedom of expression taking place in their own countries. Without the information they provide, the quality of our research into particular country situations, such as Iran or Egypt, would be severely limited. This would in turn hamper our ability to carry out effective advocacy both domestically and with international institutions.

8. Since the Snowden revelations about mass surveillance programmes, ARTICLE 19 has had the following specific concerns in relation to our online communications:

i. As the UK's diplomatic and business relations with Iran are being restored, our staff working in the Iran programme are worried that the identity of their sources might be revealed by mass surveillance programmes and shared with the Iranian government. This would not only compromise the safety of our sources and the support we provide to activists and human rights defenders, but it would also undermine our research into violations of freedom of expression online in Iran.

ii. The communications of our staff dealing with certain issues, such as Wikileaks - which might be of interest to governments friendly to the UK - may well have been intercepted. This is equally true of the communications of our staff working on countries in which the human rights situation is sensitive, such as Russia, Azerbaijan or Bangladesh.

9. Our concerns about the interception of NGO's communications by mass surveillance programmes are not merely hypothetical. In *Liberty and others v GCHQ* [2015] UKIPTTrib 13_77-H2: the Investigatory Powers Tribunal found that GCHQ had intercepted and unlawfully retained the private communications of Amnesty International and the Legal Resources Centre, a South African NGO. Despite the assurances of the Interception of Communications Commissioner that "the interception agencies do not engage in indiscriminate random mass intrusion" (para 6.6.2 of the 2013 report), it has now become clear that NGOs communications worldwide are liable to be intercepted by the intelligence agencies.

III. MASS SURVEILLANCE HAS A CHILLING EFFECT ON THE FREEDOM OF EXPRESSION OF NGOs AND THE PRESS

10. The knowledge that intelligence agencies may use their interception powers and capabilities to capture NGOs communications have a profound chilling effect on NGOs' exercise of freedom of expression in two fundamental ways.

i. First, it endangers the public watchdog function of NGOs by seriously undermining the way in which they operate. NGOs 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 knowledge that the UK intelligences 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 NGOs. As sources of information dry up, NGOs 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 NGOs' 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.[2]

11. In other words, mass surveillance programmes dramatically undermine the protection of NGOs' sources and the ability of NGOs to carry out their work. If NGOs are to perform their public watchdog function, which the Court itself has recognized,[3] they must be able, like journalists, to guarantee the anonymity of their sources and the confidentiality of their communications. ARTICLE 19 further submits that bulk interception and acquisition capabilities without any requirement of targeting and

without adequate safeguards contribute to a global chilling on free expression, including among those NGOs who are working worldwide under dangerous conditions.

12. The chilling effect of mass surveillance is not limited to NGOs however. At the end of 2014, the UK Interception of Communications Commissioner's' Office launched an inquiry, in response to serious concerns being raised in the media about the protection of journalistic sources, and the allegations that the police had misused their powers under the Regulation of Investigatory Powers Act 2001 ('RIPA') to acquire communications data. The Interception Commissioner found that in the three year period covered by the inquiry 19 police forces reported undertaking 34 investigations which sought communications data in relation to suspected illicit relationships between public officials (sources) and journalists. The 34 investigations concerned relationships between 105 journalists and 242 sources. 608 applications were authorised to seek this communications data. While the Interception Commissioner concluded that police forces had not circumvented other legislation by relying on RIPA, he found that the legal framework and practice lacked sufficient procedural safeguards. He therefore recommended that access to communications data for the purpose of identifying journalistic sources should be authorised by a judge and that more specific guidance be issued in other cases. In March 2015, the UK government adopted the Interception Commissioners' recommendations in the Acquisition and Disclosure of Communications Data Code of Practice 2015 pending new legislation in this area. In July 2015, the UK Interception Commissioner revealed that two police forces had bypassed judicial approval to obtain phone records.

13. ARTICLE 19 further notes that the chilling effect of mass surveillance has also been documented in countries with similar programmes such as the United States. In July 2014, for instance, Human Rights Watch and Pen International published a report in which it detailed the impact of surveillance on lawyers and journalists in the US.[4] They were told by journalists that government officials were substantially less willing to be in contact with the press.[5] Similarly, lawyers were concerned about their ability to defend their clients in cases in which the intelligence agencies might have an interest.[6]

14. More generally, the knowledge that our communications might be intercepted, read, analysed by government officials seriously undermines individuals' ability to exercise their right to freedom of expression; it makes them more cautious about what they say and how they behave online.[7] It breeds conformity and deters the most vulnerable from coming forward, and discourages the expression of controversial viewpoints. To hold that mass surveillance programmes are compatible with Article 10 of the Convention would likely result in a diminished public ability to obtain information and an erosion of our fundamental values as a democratic society.

IV. INTERNATIONAL CRITICISM OF BULK SURVEILLANCE POWERS

International mechanisms

15. The protection of the right to privacy is a fundamental pre-requisite to the meaningful exercise of freedom of expression. As the UN Special Rapporteur on freedom of expression noted in his 2013 report to the UN General Assembly on the implications of States' surveillance of communications on the rights to privacy and freedom of expression: [8]

> Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas (…) The right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to

> the desired recipient without the interference or inspection by State organs or by third parties.

16. The Special Rapporteur concluded that "*in order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks".*[9]

17. Following the Snowden revelations, human rights institutions, including the Office of the High Commissioner for Human Rights (OHCHR) and the UN Special Rapporteur on Counter-terrorism, have cast serious doubt upon the necessity and proportionality of mass surveillance capabilities and powers.

18. For instance, in its June 2014 report on the right to privacy in the digital age, the OHCHR noted that:[10]

> Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate

19. Similarly, the OHCHR considered that mandatory third-party data retention, a feature of surveillance regimes in many States, appeared to be "neither necessary nor proportionate".[11]

20. In September 2014, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism made similar findings in his report to the General Assembly on mass surveillance. In particular, he rebuked the argument of law enforcement agencies that the value of bulk interception lay in the absence of suspicion as a requirement to carry out surveillance:[12]

> From a law enforcement perspective, the added value of mass surveillance technology derives from the very fact that it permits the surveillance of the communications of individuals and organizations that have not previously come to the attention of the authorities. The public interest benefit in bulk access technology is said to derive precisely from the fact that it does not require prior suspicion. The circularity of this reasoning can be squared only by subjecting the practice of States in this sphere to the analysis mandated by article 17 of the International Covenant on Civil and Political Rights.

21. He went on to consider that:[13]

> Merely to assert — without particularization —that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use. The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful (in terms of international or domestic law).

22. In particular, the UN Special Rapporteur on counter-terrorism made plain the magnitude of the interference with the right to privacy:[14]

> The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether. By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality.

23. As an absolute minimum, therefore, he called on to States using mass surveillance technology to give a meaningful public account of the tangible benefits that accrue

from its use. Otherwise, there would simply be no means by which to measure the compatibility of this emerging State practice with the requirements of Article 17 ICCPR. In particular, he observed:[15]

> [It is] a prerequisite for any assessment of the lawfulness of these measures that the States using the technology be transparent about their methodology and its justification. Otherwise, there is a risk that systematic interference with the security of digital communications will continue to proliferate without any serious consideration being given to the implications of the wholesale abandonment of the right to online privacy.

24. He concluded that:[16]

> **Assuming therefore that there remains a legal right to respect for the privacy of digital communications** (and this cannot be disputed (see General Assembly resolution 68/167)), **the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right** (see paras. 51 and 52 below). **It is potentially inconsistent with the core principle that States should adopt the least intrusive means available when entrenching on protected human rights** (see para. 51 below); it excludes any individualized proportionality assessment (see para. 52 below); and it is hedged around by secrecy claims that make any other form of proportionality analysis extremely difficult (see paras. 51 and 52 below). The States engaging in mass surveillance have so far failed to provide a detailed and evidence-based public justification for its necessity, and almost no States have enacted explicit domestic legislation to authorize its use (see para. 37 below). **Viewed from the perspective of article 17 of the Covenant, this comes close to derogating from the right to privacy altogether in relation to digital communications**. For all these reasons, mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law. **In the view of the Special Rapporteur, the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy. Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by- case basis** (see para. 51 below) [emphasis added**]**

European institutions

25. European institutions have also roundly condemned bulk surveillance powers. In February 2014, the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) of the European Parliament, published the findings of its inquiry into US NSA mass surveillance programmes, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights.[17] While strongly denouncing terrorism, the LIBE Committee considered:[18]

> [T]he fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; [the Committee] takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society

26. The LIBE Committee went on to condemn the indiscriminate, suspicionless, collection of individual's private communications in the following terms:[19]

> Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and

> democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing significant potential for abusive of the information gathered against political adversaries…

27. At Council of Europe level, the Commissioner for Human Rights has found that:[20]

> [I]t is becoming increasingly clear that secret, massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fights against terrorism or other important threats to national security.

28. Similarly, in April 2015, the Parliamentary Assembly of the Council of Europe ('PACE') warned in Resolution 2045 (2015):[21]

> The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights (ETS No. 5)), freedom of information and expression (Article 10), a fair trial (Article 6) and freedom of religion (Article 9) – especially when confidential communications with lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardises the rule of law.

29. The PACE went on to unequivocally condemn "*the extensive use of secret laws and regulations, applied by secret courts using secret interpretations of the applicable rules, as this practice undermines public confidence in the judicial oversight mechanisms*."[22]

30. Finally, more recently, the Court of Justice of the European Union ('CJEU') invalidated Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services ('Data Retention Directive') in the *Digital Rights Ireland* case.[23] It did so on the ground that the indiscriminate retention of individuals' personal data regardless of any suspicion of involvement in criminal activity or threat to public security, as provided for under the Directive, constituted a disproportionate restriction on the rights to privacy and personal data under Articles 7 and 8 of the EU Charter of fundamental Rights.[24] Both the *Digital Rights Ireland* and related *Schrems* cases are due to be revisited by the CJEU in April 2016.

31. In ARTICLE 19's view, the above findings clearly indicate that the indiscriminate, suspicionless, collection, analysis, storage and retention of individuals' communications are inherently disproportionate. By their very nature, they are also inherently incapable of distinguishing between the communications of NGOs, journalists and other protected professions and those of individuals who are suspected of being involved in criminal activity. As such, they are not only incompatible with the right to privacy under Article 8 but also with Article 10 of the Convention. ARTICLE 19 therefore invites the Court to make clear that bulk surveillance powers are incompatible with the rule of law and the fundamental values of a democratic society.

V. NECESSARY LEGAL SAFEGUARDS IN THE CONTEXT OF SURVEILLANCE

Surveillance must be targeted and based on reasonable suspicion

32. As the basic values of democratic societies are being tested by mass surveillance programmes, ARTICLE 19 submits that it is essential for the Court to underline that only targeted surveillance based on reasonable suspicion constitutes a legitimate restriction on the rights to privacy and freedom of expression. In our view, this would reflect growing consensus under international law and would be consistent with the principles enunciated by the Court in *Roman Zakharov v Russia*, [GC], no. 47143/06, 4 December 2015.

33. In particular, we note that the principle of 'targeted' surveillance based on 'reasonable suspicion' is supported by the UN Special Rapporteur on Counter-Terrorism, [25] OHCHR, [26] the European Parliament, [27] PACE [28] and the Council of Europe Commissioner for Human Rights.[29] In *Roman Zakharov v Russia,* the Court confirmed this standard, holding that:

> 260. Turning now to the authorisation authority's scope of review, the Court reiterates that it 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. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means (see Klass and Others, cited above, § 51; Association for European Integration and Human Rights and Ekimdzhiev, cited above, §§ 79 and 80; Iordachi and Others, cited above, § 51; and Kennedy, cited above, §§ 31 and 32).

34. ARTICLE 19 notes, however, that in *Szabó and Vissy v. Hungary,* no. 37138/14, 12 January 2016, the Court apparently proceeded on the assumption that mass surveillance programmes are inevitable.[30] This is also the starting point of the Venice Commission in its 2015 *Report on Democratic Oversight of Signals Intelligence Agencies*.[31] In particular, the Court found in *Szabó* that:[32]

> For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen (see the CDT's submissions on this point in paragraphs 49-50 above), especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights.

35. The Court therefore did not question whether bulk interception powers were *per se* inherently incompatible with the requirements of the Convention, but rather whether those powers were meted out with sufficient safeguards. We therefore agree with

Judge Pinto de Albuquerque that the *Szabó* judgment potentially contradicts the Court's findings in the *Roman Zakharov* case.[33] It is therefore essential for the Court to clarify that only targeted surveillance based on reasonable suspicion is consistent with the requirements of the Convention. In our view, this would also be more consistent with the principles underlying the decision of the CJEU in the *Digital Rights Ireland* case, i.e. that the mass collection and retention of personal data is a disproportionate restriction on the rights to privacy and data protection.[34] Moreover, we note that the US courts have not hesitated to find that at least some US mass surveillance programmes were unconstitutional.[35] In our view, the Court should be slow to legitimise mass surveillance programmes simply because they are perceived as inevitable in the fight against terrorism and other threats. To do otherwise would fundamentally undermine the protection of the rights to freedom of expression and privacy.

Judicial authorization

36. Although the Court's decisions in *Klass and Others v. Germany*[36] and *Kennedy v. the United Kingdom*[37] required only that authorisation of intrusive surveillance powers should be granted by a body that was independent, a growing consensus has emerged in support of the view that such powers should only be authorized by a judge.[38]

37. More recently, the Court itself has stressed the importance of judicial authorisation in this context. In *Roman Zakharov*, the Court noted that an important safeguard against arbitrary and indiscriminate secret surveillance in Russia law was that any interception of telephone or other communications was authorized by a court.[39] In *Szabò*, the Court further considered that a central issue in the case, common to both the stage of authorisation of surveillance measures and the one of their application, was the absence of judicial supervision.[40] The Court took the view that a system whereby supervision was exercised by a Minister was eminently political and was as such inherently incapable of ensuring the requisite assessment of strict necessity and proportionality of surveillance measures.[41] The Court concluded that in the field of secret surveillance, control by an independent body - normally a judge with special expertise - should be the rule and substitute solutions the exception, warranting close scrutiny.[42] In *Kennedy v the United Kingdom,* however, the Court seemed to accept that ministerial authorisation coupled with ex-post facto (random) review by an independent authority was sufficient.[43]

38. ARTICLE 19 submits that the support given by the Court in *Kennedy* to ministerial authorisation coupled with ex post-facto review is not only at odds with the clear requirement for independent prior authorisation expressed in *Klass* but also amounts to a wholly inadequate safeguard in the context of surveillance powers. In line with the emerging international consensus, ARTICLE 19 invites the Court to clarify its case law in order to make clear that judicial authorisation is an *essential* – rather than merely desirable - safeguard against the abuse of surveillance powers under Articles 8 and 10 of the Convention.[44]

CONCLUSION

39. Bulk interception powers represent one of the greatest threats to fundamental rights in the digital age. This threat is particularly acute in the case of NGOs, whose public watchdog function is at serious risk of being undermined by bulk collection of their private communications by governments around the world. The potential for a global chilling effect on NGOs activities is immense. For this reason, the Court should make clear that the long-established protections enjoyed by the press for the protection of their sources must apply with equal weight to NGOs.

40. By their very nature, mass interception powers are incapable of distinguishing between the communications of NGOs or other protected professions, those of ordinary persons, and those individuals involved in criminal activity. Such blanket powers are therefore inherently incapable of being exercised in a proportionate manner. As such, ARTICLE 19 submits that they are fundamentally incompatible with the requirements of the Convention. We therefore urge the Court to conclude that only targeted surveillance based on reasonable suspicion and authorized by a judge constitutes a legitimate restriction on the rights to privacy and freedom of expression. Anything less would seriously under individuals' rights to free expression, privacy, democracy and the rule of law.

Gabrielle Guillemin
Senior Legal Officer
ARTICLE 19
02 March 2016

---

[1] This corresponds to the definition of 'journalist' in Recommendation No. R (2000)7 of the Committeen of Ministers to Member States on the right of journalists not to disclose their sources of information adopted 8 March 2000, available from here: https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM
[2] *W (Algeria) v Secretary of State for the Home Department* [2012] UKSC 8
[3] *Vides Aizsardzības Klubs v. Latvia*, no. 57829/00, § 42, 27 May 2004; see also more recently, *Szabó and Vissy v. Hungary,* no. 37138/14, 12 January 2016, at para.38.
[4] See Human Rights Watch and Pen International, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy,* July 2014: https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf
[5] *Ibid*. page 3.
[6] *Ibid*. page 4.
[7] See A/HRC/23/40, 17 April 2013, para. 79, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[8] Ibid. para. 24.
[9] Ibid. para.80.
[10] A/HRC/27/37, 30 June 2014, at 25, available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[11] Ibid. at para. 26.
[12] See A/69/397, 23 September 2014, at para. 10, available at: http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf
[13] Ibid. para. 11.
[14] Ibid. para. 12.
[15] A/69/397, 23 September 2014, at para 14.
[16] Ibid. para. 18.
[17] The report is available from here: https://polcms.secure.europarl.europa.eu/cmsdata/upload/73108fba-bb11-4a0b-83b8-54cc99c683b5/att_20140306ATT80632-1522917198300865812.pdf
[18] Ibid., Motion of a resolution, at para. 5.
[19] Ibid., Motion for a resolution, para. 10. The motion for a resolution was adopted on 12 March 2014.
[20] Council of Europe Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world,* Issue Paper, December 2014, page 16, available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2
[21] See para. 4
[22] Ibid. para. 7. See also para. 11 of the Resolution concerning the need for targeted surveillance and how independent reviews in the US suggest that mass surveillance have not contributed to preventing terrorist attacks.
[23] Cases C-293/12 and C-594/12, judgment of 8 April 2014, available from here: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5a59af9b9d34044408dd9cc4db8cc1795.e34KaxiLc3qMb40Rch0SaxuSbhz0?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=77246
[24] For a summary of the *Digital Rights Ireland* case, we refer to the Court's own summary in *Roman Zakharov v Russia*, [GC], no. 47143/06, 4 December 2015, para. 47.
[25] See A/69/397, 23 September 2014, at para. 30 and, *mutatis mutandis*, para. 55.

[26] *Op. cit*, paras. 25-26
[27] Resolution of 12 March 2014, cited at fn 19 above.
[28] See Resolution 2015 (2015), at para. 19.1.
[29] *Op. cit*.
[30] See para. 68 of the judgment.
[31] See Venice Commission, CSL-AD(2015)011, 15 December 2015, paras. 97 ff, available from here: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD%282015%29011-e
[32] See para. 78 of the judgment.
[33] See Concurring Opinion of Judge Pinto de Albuquerque, at para. 20.
[34] See para. 57-62 of the *Digital Rights Ireland* case.
[35] See *ACLU v Clapper*, United States Court of Appeal for the Second Circuit, 7 May 2015, available from: https://www.eff.org/document/aclu-v-clapper-second-circuit-opinion
[36] 6 September 1978, Series A no. 28
[37] app no. 26839/05, 18 May 2010.
[38] See UN Special Rapporteur on freedom of expression's report, A/HRC/23/40, 17 April 2013, para. 81; PACE Resolution 2045 (2015), para. 19.2; Human Rights Committee Concluding Observations on the 4th USA report, CCPR/C/USA/CO/4, 26 March 2014, paragraph 22(d); OHCHR, A/HRC/27/37, para. 38 and, *mutatis mutandis,* Venice Commission, CSL-AD(2015)011, 15 December 2015, paras. 107 ff.
[39] *Roman Zakharov v Russia*, [GC], no. 47143/06, 4 December 2015, para. 259.
[40] *Szabó and Vissy v. Hungary,* no. 37138/14, 12 January 2016, para. 75.
[41] Ibid. para. 75
[42] Ibid. 77.
[43] See para. 166 of the judgment; *Szabó and Vissy v. Hungary,* cited above para. 77.
[44] ARTICLE 19 also refers the Court to our joint submissions with Privacy International in *Luutsepp v Estonia* (no. 46069//13), in which we argued that the right to notification should now be considered a requirement under the Convention. Our submissions are available from here: https://www.article19.org/data/files/medialibrary/37720/Luutsepp-v-Estonia-intervention-22-09-14.pdf