**IN THE GRAND CHAMBER OF THE EUROPEAN COURT OF HUMAN RIGHTS**
**B E T W E E N:-**

**APP NOs 58170/13, 62322/14 and 24960/15**

**BIG BROTHER WATCH & OTHERS**

**Applicants**

**-v-**

**THE UNITED KINGDOM**

**Respondent Government**

---

**THIRD PARTY INTERVENTION SUBMISSIONS BY ARTICLE 19[1]**

---

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 was granted permission by the President of the European Court of Human Rights (the Court) to intervene in the proceedings on 8 February 2016 pursuant to Rule 44 (3) of the Rules of Court. On 4 February 2019, the Applicants' case was referred to the Grand Chamber. On 3 April 2019, the Court invited ARTICLE 19 to make further submissions. These further submissions do not address the particular facts or merits of the Applicants' case.

3. In ARTICLE 19 believes that the referral to Grand Chamber concerns both the compatibility of the UK surveillance regime with the right to private life under Article 8 of the Convention but also raises fundamental issues for the right to freedom of expression (freedom of expression) under Article 10 of the Convention. Although the Court first addressed the issue of surveillance in its decision in *Klass v Germany* more than forty years ago, and has addressed it in numerous cases since, the present case represents the very first time that the Grand Chamber will address the unprecedented scale and scope of mass surveillance in the digital age. The case presents the Grand Chamber 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). Hence, in ARTICLE 19's view, the Grand Chamber's decision on these issues will have far-reaching implications for the rights to privacy and freedom of expression far beyond the territory of the Council of Europe for years to come.

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

4. The Court 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*, the Court noted "*the legitimate and important role that campaign groups can play in stimulating public discussion.*"[2] In *Társaság a Szabadságjogokért v Hungary*, 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.""*[3] The Court has further recognised the important role of NGOs in holding governments to account in cases involving NGOs specializing in environmental issues,[4] animal rights groups[5] and NGOs working on ensuring respect for human rights, democracy and the rule of law.[6]

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.[7] More generally, they must benefit from the same Convention protection to that afforded to the press.[8]

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. As the Court noted in *Társaság,"[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*."[9]

7. In its judgment, the Chamber declared the Applicants' arguments concerning the applicability of Article 10 of the European Convention to the investigative activities of NGOs to be inadmissible on the basis that they had failed to exhaust domestic remedies (para 473). To the extent that it addressed Article 10 of the European Convention, it did so only in relation to those applicants it described as a "a journalist and a newsgathering organisation" (para 475). While ARTICLE 19 welcomes the Chamber's recognition of "*the importance of the protection of journalistic sources for the freedom of the press in a democratic society*" (para 492) and its conclusion that the lack of sufficient safeguards under the bulk interception regime and the Chapter II regime in respect of confidential journalistic material breached Article 10 of the European Convention (para 495), ARTICLE 19 nonetheless considers that there is an urgent need for further clarification of the scope of that protection.

8. ARTICLE 19 therefore invites the Grand Chamber 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.[10] 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

9. 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, whistle-blowers 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.

10. Since the Snowden revelations about mass surveillance programmes in 2013, 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.

11. These concerns about the interception of NGO's communications by mass surveillance programmes are not hypothetical. In *Liberty and others v GCHQ*,[11] 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,"[12] it is now plain beyond doubt that NGOs communications worldwide are liable to be intercepted by intelligence agencies of States Parties to the Convention.

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

12. 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, whistle-blowers, 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.[13]

13. 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,[14] 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.

14. The chilling effect of mass surveillance has also been well-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.[15] They were told by journalists that government officials were substantially less willing to be in contact with the press.[16] Similarly, lawyers were concerned about their ability to defend their clients in cases in which the intelligence agencies might have an interest. A July 2017 report from Human Rights Watch similarly detailed the impact of mass surveillance by the Russian authorities on online expression, quoting one Russian lawyer as saying that "*Internet users might not be afraid of being blocked but everyone fears jail time.*"[17]

15. In its judgment, the Chamber accepted that the lack of sufficient safeguards in the s8(4) regime in respect of the bulk interception of the communications of journalists and their sources, as well a similar lack of safeguards in the Chapter II regime in respect of communications data, posed a "*potential chilling effect*" giving rise to a violation of Article 10 of the European Convention (para 495). ARTICLE 19 urges the Grand Chamber to recognise that this chilling effect extends not only to journalists and their sources but also to the activities of NGOs in communicating information in the public interest, not to mention the willingness of members of the public to engage in the free and open exchange of information and ideas.[18]

## IV. INTERNATIONAL CRITICISM OF BULK SURVEILLANCE POWERS

### *International mechanisms*

16. 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:

> 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.[19]

17. 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.*"[20]

18. 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.

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

> 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.[21]

20. 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.*"[22]

21. 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:

> 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. [23]

22. Noting that the fact that something is technically feasible or useful *"does not by itself mean that it is either reasonable or lawful (in terms of international or domestic law),"*[24] the Special Rapporteur on counter-terrorism noted the "*hard truth*" 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,*"[25] He went on to conclude as follows:

> 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). [26]

***European institutions***

23. 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.[27] While strongly denouncing terrorism, the LIBE Committee considered:

> [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.[28]

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

> 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…[29]

25. At Council of Europe level, the Commissioner for Human Rights has found that:

> [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.[30]

26. Similarly, in April 2015, the Parliamentary Assembly of the Council of Europe (PACE) warned in Resolution 2045 (2015):

> 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.[31]

27. 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.*"[32]

28. In April 2014, in its decision in C-293/12 *Digital Rights Ireland*, the Court of Justice of the European Union (CJEU) invalidated Directive 2006/24/EC (the Data Retention Directive) 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, constituted a disproportionate restriction on the rights to privacy and personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights.

29. In December 2016, in *Tele2 Sverige AB,* the CJEU affirmed its conclusion in *Digital Rights Ireland*, holding that the rights to privacy and protection of personal data "*preclude national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*"[33] Any legislation requiring the retention of communications data must "*be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security.*"[34]

30. 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 European Convention. ARTICLE 19 therefore invites the Grand Chamber to make clear that bulk surveillance powers are incompatible with the rule of law and the fundamental values of a democratic society.

31. ARTICLE 19 notes that, although the Chamber referred to both *Digital Rights Ireland* and *Tele2* in its judgment, when it came to the assessment of the necessity and proportionality of bulk interception, it did not address the CJEU's reasoning in those cases in any meaningful respect. The Chamber noted that national authorities "*enjoy a wide margin of appreciation*" when choosing "*how best to achieve the legitimate aim of national security,*"[35] though it also found that "*the discretion afforded to them in operating an interception regime must necessarily be narrower.*"[36] The Chamber, however, took no account of the detailed observations of the Grand Chamber in *S and Marper v United Kingdom* concerning the margin of appreciation in cases involving highly sensitive personal information, in particular the Grand Chamber's injunction that "*the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned,*"[37] particularly one involving "*such an indiscriminate and open-ended retention regime.*"[38]

32. Indeed, there is something of a disconnect between the Chamber's acceptance in the present case that the bulk acquisition of communications data "*could be 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*" (para 356), on the one hand, and its conclusion that "*the operation of a bulk interception regime in principle falls within a State's margin of appreciation*" (para 317), on the other. It is difficult to understand how the sensitivity of a person's genetic data warrants a narrow margin of appreciation, on the one hand, and yet the indiscriminate collection of that same person's most private communications (alongside the equally indiscriminate collection of the private communications of millions and millions of others) is not thought to warrant an equally narrow margin. As the Grand Chamber noted in *Marper*, 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.*"[39] The Grand Chamber went on to note that "*any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.*"[40] Despite the unprecedented scope and scale of the bulk interception programme at issue in the present case, however, the Chamber's judgment did not require the UK government to demonstrate any such careful balancing of "*important private-life interests.*"

33. In ARTICLE 19's view, the Chambers' failure to follow the Grand Chamber's approach in *Marper* or that of the CJEU in *Digital Rights Ireland* and *Tele2* means that the Court's case law on the issue of mass surveillance and bulk collection is not only at odds with its previous decisions but also lags significantly behind that of the Luxembourg Court. In ARTICLE 19 urges the Grand Chamber not to cede its pre-eminence in the protection of fundamental rights in Europe to the CJEU and to ensure consistency with the approach that it took in *Marper* and *Catt.*

## V. NECESSARY LEGAL SAFEGUARDS IN THE CONTEXT OF SURVEILLANCE

***Surveillance must be targeted and based on reasonable suspicion***

34. 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 Grand Chamber in *Roman Zakharov v Russia*.[41]

35. In particular, we note that the principle of '*targeted'* surveillance based on '*reasonable suspicion*' is supported by the UN Special Rapporteur on Counter-Terrorism,[42] the OHCHR,[43] the European Parliament,[44] PACE,[45] and the Council of Europe Commissioner for Human Rights.[46] In *Zakharov*, the Court confirmed this standard, holding that:

> 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, §§ 31 and 32).[47]

36. In *Szabó and Vissy v. Hungary*,[48] and in the Chamber judgment in the present case, however, the Court appears to have proceeded on the wholly unargued assumption that mass surveillance programmes are inevitable.[49] The Chamber held that requiring "*objective evidence of reasonable suspicion*" would be "*inconsistent"* with broad margin of appreciation afforded to States in the field of national security, noting that bulk interception "*is by definition untargeted, and to require 'reasonable suspicion' would render the operation of such a scheme impossible.*"[50] ARTICLE 19 submits, however, that precisely the blanket and indiscriminate nature of bulk interception which places it outwith the scope of any margin of appreciation enjoyed by States in relation to the right to privacy and freedom of expression and destroys the very essence of those rights. Nor is it the Court's task to make bulk interception workable: the requirement of reasonable suspicion is not a nicety to be dispensed with when it becomes inconvenient, but a necessary safeguard for the protection of fundamental rights.

37. For these reasons, ARTICLE 19 believes that it is essential for the Grand Chamber 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.[51] Moreover, we note that the US courts have not hesitated to find that at least some US mass surveillance programmes were unconstitutional. In our view, the Grand Chamber should be slow to legitimise mass surveillance programmes simply because they are perceived as inevitable in the fight against terrorism and other threats.[52] To do otherwise would fundamentally undermine the protection of the rights to freedom of expression and privacy.

***Judicial authorization***

38. In its judgment, the Chamber noted that judicial authorisation was "*not inherently incompatible with the effective functioning of bulk interception*" (para 318) and also agreed that it was "*an important safeguard and perhaps even 'best practice'*" but held that, by itself, it was neither "*necessary nor sufficient to ensure compliance*" with Article 8 of the European Convention (para 320).

39. Although ARTICLE 19 accepts that the Chamber's conclusion is consistent with the Court's long-standing case law on this point, it is readily apparent that the vast scale and extent of bulk interception programmes operated by governments in 2019 – quite literally, the interception of the content of millions of private communications on a daily basis - greatly exceeds anything that could have been contemplated when *Klass v Germany* was first decided more than forty years ago. In this respect, the Chamber has simply failed to attach sufficient weight to the importance of judicial authorisation as a safeguard given the sheer *scale* of the interference with the fundamental rights of millions of internet users. As the Court found in *Szabò and Vissy v Hungary*,[53] it is in this context that "*external, preferably judicial,* a posteriori *control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance … by reinforcing 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.*"[54] As Judge De Albuquerque noted in his concurring opinion, "*[i]n view of the enlarged consensus in international law mentioned above and the gravity of the present-day dangers to citizens' privacy, the rule of law and democracy, the time has come not to dispense with the fundamental guarantee of judicial authorisation and review in the field of covert surveillance gathering.*"[55]

40. In line with the ever-growing international consensus in favour of judicial authorisation as a core safeguard,[56] 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 European Convention.[57]

***Notification of surveillance***

41. In *Zakharov,* the Grand Chamber held that the question of subsequent notification of surveillance measures was "*inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers*", and that there was "*in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his knowledge and thus able to challenge their legality retrospectively.*"[58] The alternative, the Grand Chamber noted, was that identified in *Kennedy,* i.e. where "*any person who suspects that his communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications.*"[59]

42. In the present case, the Chamber cited the Grand Chamber's approach in *Zakharov* but concluded that the "*extensive jurisdiction*" of the Investigatory Powers Tribunal provided a sufficient safeguard in this respect (para 379). It also noted that the requirement of subsequent notification "*assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime*" (para 317). ARTICLE 19 submits, however, that the IPT's jurisdiction is no more than an illusory safeguard, for absent notification, a person would not have any cause to suspect their communications were being intercepted or, worse, would be obliged to spend their time making purely speculative complaints. ARTICLE 19 submits that this approach is wholly at odds with the requirement that remedies be "*practical and effective*" rather than "*theoretical and illusory*". Indeed, in the applicants' case, it was only the disclosure of the whistle-blower Edward Snowden that alerted them to the possibility that their private communications were subject to interception in this manner.

43. As regards the practicality of notification, ARTICLE 19 submits that the Chamber was too quick to assume that notification entailed the existence of "*clearly defined targets*" (para 317). In point of fact, ARTICLE 19 notes that there is nothing inherently impractical about requiring an intercepting agency to identify the communications it intercepts, in order that they be notified. As the Grand Chamber found in *Zakharov,* the fact that it "*may not be feasible in practice to require subsequent notification in all cases*" does not relieve the intercepting body of providing notification "*as soon as [it] can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure.*"[60] Similarly, the CJEU stated in *Tele2* that competent national authorities are required to *"notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy … where their rights have been infringed."*[61] If notification is possible in

respect of the bulk retention of communications data, ARTICLE 19 notes, it should be no less possible in respect of bulk interception.

## CONCLUSION

44. 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 Grand Chamber 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.

45. 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 Grand Chamber 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.

In London, 23 April 2019

Gabrielle Guillemin
Senior Legal Officer
ARTICLE 19
Free Word Centre,
London EC1R 3GA

Eric Metcalfe
Monckton Chambers
Gray's Inn
London WC1R 5NR

## Endnotes

[1] Pursuant to Art.36(2) and Rule 44(2).
[2] *Steel and Morris v the UK,* App. No. 68416/01, 15 February 2005, para 95.
[3] *Társaság a Szabadságjogokért v Hungary*, App. No 37374/05, 14 April 2009, para 27.
[4] *Vides Aizsardzības Klubs v. Latvia*, App. No. 57829/00, 27 May 2004, para 42.
[5] *Animal Defenders International v the UK* [GC], App. No. 48876/08, 22 April 2013, para 103.
[6] *Youth Justice Initiative for Human Rights v Serbia*, App. No. 48135/06, 25 June 2013.
[7] *Vides Aizsardzības Klubs*, *op.cit*., para 42.
[8] *Társaság a Szabadságjogokért*, *op.cit*., para 27.
[9] *Ibid.,* para 27.
[10] This corresponds to the definition of 'journalist' in Recommendation No. R (2000)7 of the Committee of Ministers to Member States on the right of journalists not to disclose their sources of information adopted 8 March 2000.
[11] *Liberty and others v GCHQ* [2015] UKIPTTrib 13_77-H2.
[12] 2013 Annual Report of the Interception of Communications Commissioner, The Rt Hon.Sir Anthony May, para 6.6.2.
[13] *W (Algeria) v Secretary of State for the Home Department* [2012] UKSC 8
[14] *Vides Aizsardzības Klubs*, *op.cit.,* para 42; see also*Szabó and Vissy v. Hungary,* App. No. 37138/14, 12 January 2016, para 38.
[15] 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.
[16] *Ibid.*, p.3.
[17] Pavel Chikov, in Human Rights Watch, Online and On All Fronts: Russia's Assault on Freedom of Expression, July 2018, p. 57.
[18] See A/HRC/23/40, 17 April 2013, para 79.
[19] *Ibid.*, para 24.
[20] *Ibid.*, para 80.
[21] A/HRC/27/37, 30 June 2014, para 25.
[22] *Ibid.*, para 26.
[23] See A/69/397, 23 September 2014, para 10.
[24] *Ibid*., para. 11.
[25] *Ibid*., para 12.
[26] *Ibid*., para 18.
[27] European Parliament, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, (2013/2188(INI)), 21 February 2014.
[28] *Ibid.*, Motion of a resolution, at para. 5.
[29] *Ibid.*, Motion for a resolution, para. 10. The motion for a resolution was adopted on 12 March 2014.
[30] Council of Europe Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world,* Issue Paper, December 2014, p. 16.
[31] Council of Europe, Resolution 2045 (2015) – Mass surveillance, 21 April 2015, **para 4.**
[32] *Ibid.*, para 7.
[33] CJEU [GC],*Tele2 Sverige AB*, Joined Cases C-203/15 and C-698/15, 21 December 2016, para 112.
[34] *Ibid.,* para 111.
[35] *Op.cit*., para 314 and para 387.
[36] *Ibid.,* para 315
[37] *S and Marper v the UK* [GC], App. Nos. 30562/04 and 30566/04, para 104.
[38] *Ibid.,* para 120. See also *Catt v the UK,* App. No 43514/15, 24 January 2019, in which the Court found that a narrower margin of appreciation was warranted given the particular sensitivity of data relating to political opinion attracted "*a heightened level of protection.*"
[39] *S and Marper, op.cit.,* para 112.
[40] *Ibid*.
[41] *Roman Zakharov v Russia* [GC], App. No. 47143/06, 4 December 2015.
[42] See A/69/397, 23 September 2014, para. 30 and, *mutatis mutandis*, para 55.
[43] *Op. cit*., paras. 25-26
[44] Resolution of 12 March 2014, *op.cit*.
[45] See Resolution 2015 (2015), *op.cit.,* para 19.1.
[46] *Op. cit*.
[47] *Zakharov v Russia*, *op.cit.,* para 260.
[48] *Szabó and Vissy v. Hungary*, App. No. 37138/14, 12 January 2016, para 68.
[49] This is also the starting point of the Venice Commission in its 2015 Report on Democratic Oversight of Signals Intelligence Agencies.
[50] *Szabó and Vissy, op.cit.,* para 317.
[51] *Digital Rights Ireland* , paras 57-62.
[52] See *ACLU v Clapper*, United States Court of Appeal for the Second Circuit, 7 May 2015.

[53] *Szabó and Vissy, op.cit.*
[54] *Ibid.*, para 79
[55] *Ibid.*, para 23
[56] 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.
[57] 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.
[58] *Zakharov* , *op.cit.,* para 234.
[59] *Ibid.*
[60] *Ibid.*, para 287.
[61] *Tele2, op.cit.,* para 121