IN THE EUROPEAN COURT OF HUMAN RIGHTS **APP. NO. 46069/13**
B E T W E E N:-

OLEV LÜÜTSEPP

Applicant

-v-

ESTONIA

Respondent Government

WRITTEN SUBMISSIONS ON BEHALF OF PRIVACY INTERNATIONAL AND ARTICLE 19[1]

INTRODUCTION AND SUMMARY

1. These are the written submissions of Privacy International and ARTICLE 19 ('the Interveners'). The Interveners are the leading international human rights organisations on the right to privacy and the right to freedom of expression respectively. Both organisations have considerable expertise in their respective fields, as well as substantial experience of human rights litigation at the domestic, regional and international levels. Both organisations welcome the opportunity to intervene jointly as a third party in this case, by the leave of the Court granted 1 September 2014.

2. In outline, the Interveners submit that:

   (i) the requirement to notify a person that they have been the subject of surveillance has been recognised by the Court as an important safeguard against the abuse of surveillance powers under Article 8, part of the right to an effective remedy under Article 13, and a trigger for the fair trial guarantees of Article 6;

   (ii) recent rapid changes in communications technology have led to an unprecedented increase in the amount of surveillance, especially digital surveillance;

   (iii) in response to these changes, international law increasingly recognises the requirement to notify a person that they have been the subject of surveillance as a *necessary* safeguard, rather than merely a desirable one;

   (iv) the comparative experience of a broad range of jurisdictions shows that notification requirements are also widely-regarded as a necessary safeguard against the abuse of surveillance powers;

   (v) the Court should therefore take this opportunity to clarify its case law in order to make clear that notification is a *necessary* safeguard against the abuse of surveillance powers under Article 8, an *essential* part of the right to an effective remedy under Article 13, and a *necessary* trigger for the fair trial guarantees of Article 6.

3. As directed, these submissions do not comment on the facts or merits of the case.

THE COURT'S CASE LAW ON NOTIFICATION OF SURVEILLANCE

4. The question of whether an individual is entitled to be notified that he or she has been the subject of covert surveillance arises in at least two contexts under the framework of the Convention: first, as a potential safeguard against possible abuse of surveillance powers under Article 8, and secondly as part of the right to an effective remedy under Article 13.

Article 8

5. In *Klass v Germany*, no. 5029/71, 6 September 1978, the Court noted that the question of whether the authorities should be obliged to notify a person that he or she had been under surveillance was "inextricably linked" to *a posteriori* judicial control of surveillance:

> since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality (para 57).

6. It went on to consider whether "it is even feasible in practice to require subsequent notification in all cases" (para 58), on the basis that the "activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures", and notification "might well jeopardise the long-term purpose that originally prompted the surveillance". It also noted that "such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents" (ibid). Lastly, it noted the decision of the German Constitutional Court that "the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction" (ibid).

7. It was on this basis that the Court in *Klass* concluded that Article 8 ECHR did not impose a *general* requirement on Contracting States to ensure that individuals subject to surveillance were subsequently notified of this. In the subsequent case of *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, no. 62540/00, 28 June 2007, the Court found *inter alia* that the relevant Bulgarian law did "not provide for notification of persons subjected to surreptitious monitoring under any circumstances and at any point in time" (para 91). It went on to state that:

> According to the Court's case law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned...

8. Notification, the Court concluded, was "an important safeguard against the improper use of special means of surveillance" (para 91). It has stopped short, however, of concluding that notification is a *necessary* safeguard. In *Kennedy v United Kingdom*, no. 26839/05, 18 May 2010, for example, the Court held that the Regulation of Investigatory Powers Act 2000 was not incompatible with the requirements of Article 8 notwithstanding that the absence of any requirement on the authorities to notify individuals that they had been subject to surveillance (namely because "the jurisdiction of the [Investigatory Powers Tribunal] does not ... depend on notification" (para 167)).

Article 13

9. In *McFarlane v Ireland*, no. 31333/06, 10 September 2010, the Grand Chamber held that - in the context of the right to an effective remedy - the term 'effective' meant, among other things, that the remedy must be *accessible* (para 108). In the context of secret surveillance, however, the Court in *Klass* stated that "it is the secrecy of the measures which renders it difficult, if not impossible, for the person concerned to seek any remedy of his own accord, particularly while surveillance is in progress" (para 68). Consistent with its conclusions on Article 8, the Court therefore held that a lack of notification did not, in cases involving surveillance, entail a breach of Article 13 (ibid). Instead, the Court held that - in this context - an 'effective' remedy meant a remedy "that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance" (para 69).

10. Noting, among other things, the requirement of German law that "the competent authority is bound to inform the person concerned as soon as the surveillance measures are discontinued and notification can be made without jeopardising the purpose of the restriction" and that "[f]rom the moment of such notification, various legal remedies - before the courts - become available to the individual" (para 71), the Court in *Klass* concluded that the aggregate of remedies provided for under German law satisfied the requirements of Article 13. Provision for notification, therefore, played a central part in ensuring the compatibility of the German surveillance regime with fundamental rights.

11. It is equally is clear that the *absence* of provision for notification has played a key role in findings of incompatibility of surveillance laws with Article 13. In *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria,* for example, the Court again noted that:

> the SSMA does not provide for notification of the persons concerned at any point in time and under any circumstances. On the contrary, in two judgments of 12 February and 15 May 2004 the Supreme Administrative Court held that the information whether a warrant for the use of means of secret surveillance had been issued was not to be disclosed. The second judgment stated that such information was classified (see paragraphs 49 and 50 above). It thus appears, that, unless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them.

12. As with Article 8, however, the Court has yet to take the step of concluding that notification is a *necessary* aspect of the right to an effective remedy in the context of secret surveillance. The Interveners submit that the time has now come for the Court to take that step, for the reasons set out below.

Article 6

13. In respect of the application of Article 6 to surveillance decisions, the Interveners submit that there is a conflict between the Court's well-established case law from *Klass* onwards and its decision in *Kennedy*. In the former, the Court held that

> As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6 ... as a consequence, it of necessity escapes the requirements of that Article (para 75).

14. In *Kennedy*, however, the Court considered the application of Article 6 to the procedures of the Investigatory Powers Tribunal and concluded that they were not incompatible with the requirements of Article 6 in its civil head, notwithstanding that that Tribunal places sweeping restrictions on the right of

an individual to know the case against them, the right to equality of arms, the right to a reasoned decision, and the right to challenge witnesses.

15. In light of this conflict, and the highly unfortunate distortions that it has wrought on the Article 6 safeguards, the Interveners invite the Court to follow the approach taken in *Klass* and more recently, for example, in *Hadzhiev v Bulgaria*, no. 22373/04, 23 October 2012, at paras 48-49, that it is better to analyse the relevant safeguards by reference to Articles 8 and 13 in the first instance. As Lord Kerr noted in the case of *Tariq v Home Office* [2011] UKSC 35, "the decision in *Kennedy* ought to have been made on the basis that article 6 was not engaged because the issues that the case raised were simply not justiciable" (para 128).

16. Understood in this way, the Interveners submit that the importance of notification becomes clear. Notification is the means whereby a non-justiciable surveillance decision becomes justiciable. It is the means by which a person who has been the subject of surveillance becomes vested with the fair trial guarantees of Article 6, and the best means by which an effective remedy may be secured. For this reason, the Interveners submit, it is all the more important that the Court's case law

THE CHANGING TECHNOLOGICAL CONTEXT OF SURVEILLANCE

17. The Interveners note that the Court's conclusion on the "feasibility" of notification requirements in *Klass* was delivered in 1978, at a time when all telephone calls were made via fixed landlines and the possibility of communication by email, text messages or videochat were entirely unknown to the general public. In the past three and a half decades, communications technology has advanced to the point where anyone who uses a computer or a mobile phone generates an enormous amount of data on a daily basis. When analysed, moreover, this communications data that is routinely collected and stored on each individual is capable of revealing highly sensitive details about their private life, including their financial status, political opinions, religious beliefs, and sexual orientation. As the Council of Europe Committee of Ministers declared in June 2013:[2]

> People nowadays rely on a growing range of both fixed-location and mobile electronic devices which enhance their possibilities to communicate, participate and manage their everyday lives. However, a growing number of these devices are equipped with software that are capable of collecting and storing data, including personal data (e.g. keystrokes that reveal passwords) and private information such as user generated content, websites visited, and geographical locations that potentially allow tracking and surveillance of people. This data can reveal delicate and/or sensitive personal information (such as financial, health, political, religious preferences, sexual habits) which can be aggregated to provide detailed and intimate profiles of them.

18. This rapid expansion in the number of electronic communications and the data relating to those communications has also been accompanied by a corresponding expansion in surveillance technologies relating to those communications. These surveillance technologies are increasingly broad-based, involving the identification of patterns of communication in very large data-sets. Consequently, Contracting States are more likely to employ measures that involve accessing the communications data of individuals who are not themselves the *target* of surveillance - in that they are suspected of involvement in serious crime, etc - but who are nonetheless the *subject* of surveillance. In other words, it is now more likely than ever before that an ordinary individual who is of no particular interest to the authorities will nonetheless be a subject of a surveillance measure, whether inadvertently or (as is more often the case) indiscriminately.

19. It is now clear that, within a relatively short space of time, the scope and prevalence of surveillance measures have rapidly expanded. They are, moreover, likely to continue to expand for as long as democratic societies are reliant on the use of electronic communications, i.e. for the foreseeable future.

Having regard to these changes, the Interveners submit that provision for notification is no longer merely a desirable feature of surveillance laws - as the Court indicated in 1978 - but rather an essential safeguard against unnecessary and disproportionate surveillance.

INTERNATIONAL LAW ON NOTIFICATION OF SURVEILLANCE

20. The rapid growth in surveillance in recent years has also prompted greater recognition at the international level about the need for adequate safeguards against abuse. In particular, there is now an increasing consensus that notification requirements are necessary to enable individuals to challenge unlawful surveillance decisions.

April 2013 report of the UN Special Rapporteur on freedom of expression

21. In his April 2013 report to the General Assembly concerning the implications of communications surveillance on freedom of expression, the UN Special Rapporteur on freedom expression Frank La Rue stated that:[3]

> Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, *individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath*.

June 2013 joint declaration by special rapporteurs on the impact of surveillance on free expression

22. In June 2013, a joint declaration by the UN Special Rapporteur on freedom of expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights expressed concern that:[4]

> legislation on intelligence and security has remained inadequate as new technologies have been developed in the digital era. It is especially concerning that indiscriminate access to information on communication between persons can have a chilling effect on the free expression of thought and the search for and distribution of information in the region.

23. The Declaration went on to urge states to "amend their laws to establish limits on the power to carry out surveillance of private communications", including limits with regard to "the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; *and the legal mechanisms by which they may be challenged*".[5] The Declaration also stressed the need for states to "divulge information regarding the existence of illegal programs of surveillance of private communication" and "carry out exhaustive investigations to identify and punish those who pursue these types of practices and *report in a timely fashion to those who may have been victims of them*".[6]

International Principles on the Application of Human Rights to Communications Surveillance

24. In May 2014, a coalition of hundreds of civil society groups - including the Interveners - from more than 180 countries launched the International Principles on the Application of Human Rights to Communications Surveillance[7] in order to identify the fundamental requirements of international standards in the context of digital surveillance. Its preamble states that:

> Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to Communications Surveillance by States. In

recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and -- information about an individual's communications or use of electronic devices -- the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make Communications Surveillance by States possible at an unprecedented scale. Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing Communications Surveillance technologies and techniques of the State, the ability of the State to combine and organize information gained from different surveillance technologies and techniques, or the increased sensitivity of the information available to be accessed.

25. In respect of notification, the Principles state as follows:

> Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:
>
> (1) Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and
>
> (2) Authorisation to delay notification is granted by a Competent Judicial Authority; and
>
> (3) The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.
>
> The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

June 2014 report of the UN High Commissioner for Human Rights

26. In her 2014 report, *The Right to Privacy in the Digital Age*, the UN High Commissioner on Human Rights noted that, although international human rights law "provides a clear and universal framework for the promotion and protection of the right to privacy" in the context of surveillance, practices in many states have:[8]

> revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.

27. In particular, the High Commissioner stressed the need for the right to effective remedies in the context of surveillance:[9]

> Effective remedies for violations of privacy through digital surveillance can ... come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations

have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored.

28. In addition:[10]

> Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an "independent oversight body […] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society." Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation. Such remedial bodies must have "full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders". Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required.

COMPARATIVE LAW ON NOTIFICATION OF SURVEILLANCE

29. In addition to the evolving international standards in respect of surveillance and human rights, the Interveners note that notification requirements are now an established feature of many jurisdictions:

Belgium

30. In September 2011, the Belgian Constitutional Court ruled that the provisions of Belgian Secret Service Act were in breach of the right to privacy under Article 22 of the Belgian Constitution, on the basis that the Act failed to require notification to the subject of surveillance. The Court held that the right to privacy entailed a duty to notify the individual who was the subject of surveillance as soon it was possible to do so without prejudicing the interests of national security.[11]

Bulgaria

31. Following a series of adverse judgments from the Court including *Association for European Integration and Human Rights and Ekimdzhiev; Hadzhiev v Bulgaria*, no. 22373/04, 23 October 2012; and *Lenev v Bulgaria*, no. 41452/07, 4 December 2012, section 34h of the Special Surveillance Means Act 1997 has been amended such that the supervising commission "must *inform of its own motion* persons who have been unlawfully subjected to secret surveillance, unless notification might jeopardise the purpose of the surveillance, allow the divulgation of operational methods or technical devices, or put the life or health of an undercover agent or his or her relatives or friends in jeopardy."[12]

Canada

32. Section 196(1) of the Criminal Code provides that, 90 days after the period for which surveillance was authorised, the relevant Attorney General or government minister must notify the person who was the object of surveillance. Section 196(2) provides that the notification requirement may be delayed subject to judicial authorisation under section 196(3) where the judge is satisfied that the investigation is a continuing one or that notification would impede a subsequent investigation into the same matter. Section 196(3) further provides that notification may not be delayed more than three years.

EU data protection regime

33. The notification of individuals as to the processing of their personal data is a core requirement of the EU data protection regime. As the 38th recital to the Data Protection Directive 95/46/EC provides:[13]

> Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection

The Interveners note that the right to data protection under Article 8 of the EU Charter of Fundamental Rights is an increasingly important aspect of the protection of privacy under EU law: see in particular, the judgment of the CJEU in *Digital Rights Ireland*.[14]

Germany

34. As made clear by the Court's judgment in *Klass* and by its subsequent admissibility decision in *Weber and Saravia v Germany*, no. 54934/00, 29 June 2006, German law governing the use of surveillance (including strategic monitoring) requires the competent authority "to inform the person concerned as soon as notification can be made without jeopardising the purpose of the restriction" (*Klass*, para 19; *Weber*, para 136). In addition, the Minister's decision as to whether to notify a person that he or she has been the subject of surveillance is itself subject to review by the G10 Commission. Once notified, an affected individual has several legal rights available to them, including challenging the action by way of an administrative court declaration or seeking damages in a civil court.

Ireland

35. Section 10(3) of the Criminal Justice (Surveillance) Act 2009 provides that the responsible Minister may make regulations providing for disclosure of the surveillance "to the person who was its subject or other persons whose interests are materially affected by it" provided that any such disclosure is (a) consistent with the purposes for which the authorisation was granted; (b) consistent with the security of the State, the protection of persons' privacy and other rights and the aims of preventing and detecting the commission of arrestable offences; and (c) "unlikely to hinder the investigation in the future of such offences".

The Netherlands

36. Article 34(1) of the Intelligence and Security Services Act 2002 requires that 5 years after an interception of communications under Article 25(1) a Minister must consider whether "whether a report of the event can be submitted to the person with regard to whom one of these special powers has been exercised. If this is possible, this will take place as soon as possible". If the Minister determines that the person cannot be notified, he must notify the supervisory committee (Article 34(2)). The grounds for non-notification are where notification "can reasonably be expected to result in (a) sources of a service, including intelligence and security services of other countries, being disclosed; (b) relations with other countries and international organisations being seriously damaged; and (c) a specific use of a method of a service or the identity of a person who has assisted the relevant service in using the method, being disclosed.

New Zealand

37. Sections 61 and 62 of the Search and Surveillance Act 2012 permits a judge to order that the subject of surveillance (including the use of an interception device) be notified if he or she is satisfied that "the public interest in notification outweighs any potential prejudice" to (a) any investigation by the law enforcement agency, (b) the safety of information or undercover officers; or (c) the supply of information to the law enforcement agency.

Sweden

38. Section 11(a) of the 2008 law on Signals Intelligence (SFS 2008:717) provides that, where any signals have been searched "using search terms that are directly attributable to a specific individual, the individual shall be informed thereof", unless there is a continuing need for confidentiality (see 11(b). Notice should be provided as soon as possible, but ordinarily within 1 month of the conclusion of the investigation.

United States

39. Under 18 US Code § 2518(8)(d), a judge issuing a warrant for the interception of communications must "within a reasonable time but not later than ninety days" of the making of the warrant, "cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice", notification of the interception, including - at the judge's discretion, "such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice". However, "on an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed".

NOTIFICATION AS AN ESSENTIAL SAFEGUARD AGAINST THE ABUSE OF SURVEILLANCE POWERS

40. As noted above, the 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. In both cases, however, the Court has yet to take the step of concluding that notification is a *necessary* safeguard in such cases. The Interveners submit that the time has now come for the Court to take that step, for the following reasons:

    (a) It is necessary having regard to the recent, rapid changes in communications technology, as set out above, and the corresponding growth in surveillance, especially digital surveillance.

    (b) It is consistent with the development of international law in the field of surveillance, privacy and freedom of expression, c.f. in particular the 2013 report of the UN Special Rapporteur on Freedom of Expression.

    (c) It is consistent with the comparative experience of a wide range of jurisdictions, including Canada, Germany, Sweden and the United States. Not only are notification requirements properly understood as an essential aspect of the right to privacy but also there is no evidence to suggest that such requirements have in any way undermined the effectiveness of surveillance measures in general.

    (d) 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, i.e. the right to know of a highly intrusive governmental measure affecting one's privacy.

41. In this context, the Interveners note that many of the arguments against treating notification as a necessary safeguard rely on the alleged impracticality of notification requirements. Yet the Interveners note that notification requirements operate in many countries without apparent difficulty. A more substantial ground of resistance to notification requirements is that it would undermine the approach of 'Neither Confirm Nor Deny' ('NCND') adopted by many governments in respect of secret surveillance. However, the Interveners caution against regarding NCND as a paramount principle of law, particularly in the context of fundamental rights. As Lord Justice Maurice Kay noted in a recent decision of the

English Court of Appeal concerning a covert operation by one of the UK intelligence services in Somaliland:

> Lurking just below the surface of a case such as this is the governmental policy of "neither confirm nor deny" (NCND), to which reference is made. I do not doubt that there are circumstances in which the courts should respect it. *However, it is not a legal principle*. Indeed, it is a departure from procedural norms relating to pleading and disclosure. It requires justification similar to the position in relation to public interest immunity (of which it is a form of subset). It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it. Where statute does not delineate the boundaries of open justice, it is for the court to do so. In the present case I do not consider that the appellants or the public should be denied all knowledge of the extent to which their factual and/or legal case on collusion and mistreatment was accepted or rejected. Such a total denial offends justice and propriety. It is for these fundamental reasons that I consider the appellants' principal ground of appeal is made out. The approach to their abuse of process applications was largely flawed. I make no comment on the merits of those applications (*Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 at para 20) .

42. In a subsequent English case involving the use of undercover police officers engaged in long-term sexual relationships, a tactic which had been abandoned by the Metropolitan police, Mr Justice Bean in the High Court similarly declined to treat NCND as a paramount principle:

> One of the justifications for NCND is that police operational methods should not be revealed. This is in my view clearly intended to apply to operational methods which continue to be in use or are likely to be used in future. Moreover, just as (in the well-known words of Page Wood V-C in *Gartside v Outram* (1856) 26 L.J.Ch 113) "there is no confidence as to the disclosure of iniquity", so there can be no public policy reason to permit the police neither to confirm nor deny whether an illegitimate or arguably illegitimate operational method has been used as a tactic in the past (DIL and others v Commissioner of Police of the Metropolis [2014] EWHC 2184 (QB) para 42).

43. Having regard to the above, the Interveners submit that the Court should be similarly wary of governmental claims about the need to maintain the secrecy of surveillance measures. While such claims may be accorded weight, they should not be elevated above the core requirements of the right to privacy and the right to an effective remedy. Instead, the Interveners invite the Court to clarify its existing case law on notification, to make clear that notification is not merely one adequate safeguard among others, but an essential part of the right to an effective remedy.

44. The Interveners do not suggest that notification of surveillance is an absolute right in the sense that it should operate without restrictions. Rather, consistent with the International Principles on the Application of Human Rights to Communications Surveillance, the Interveners submit that 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.

Carly Nyst
Legal Director
Privacy International
London EC1M 5UY

Gabrielle Guillemin
Senior Legal Officer
ARTICLE 19
London EC1R 3GA

Eric Metcalfe
Monckton Chambers
London WC1R 5NR

22 September 2014

[1] Pursuant to Art.36(2) and Rule 44(3).
[2] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, adopted 11 June 2013, para 5.
[3] A/HRC/23/40, 17 April 2013, at para 82.
[4] Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression, 21 June 2013, para 5.
[5] Ibid, para 8.
[6] Ibid, para 14.
[7] https://en.necessaryandproportionate.org/text
[8] *The right to privacy in the digital age*, A/HRC/27/37, 30 June 2014 at para 47.
[9] Ibid, para 40.
[10] Ibid, para 41.
[11] Belgian Constitutional Court, case no. 145/2011. 22 September 2011 at paras B.82-B92.
[12] *Lenev*, para 82.
[13] Similar requirements in respect of data protection in the law enforcement context have also been recognized by the Council of Europe in Principle 2.2 of the Committee of Ministers' 1987 Recommendation on the use of personal data in the police sector: "Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced".
[14] C-293/12, ECLI:EU:C:2014:238.