IN THE EUROPEAN COURT OF HUMAN RIGHTS APPLICATION NO. 49526/15
B E T W E E N:

ASSOCIATION CONFRATERNELLE DE LA PRESSE JUDICIARE and 11 OTHER APPLICATIONS

Applicants

-v-

FRANCE

Respondent Government

WRITTEN SUBMISSIONS ON BEHALF OF PRIVACY INTERNATIONAL

INTRODUCTION AND SUMMARY

1. Privacy International ("PI") provides these written submissions in order to elaborate upon the impact of new surveillance technologies and capabilities on the right to privacy as enshrined in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"). In particular, this submission will address (1) real-time automated data processing on operator networks, (2) hacking, and (3) International Mobile Subscriber Identity ("IMSI") catchers. PI believes these submissions provide necessary context for evaluating the surveillance powers, which authorise use of these technologies, set forth in Law No. 2015-912 of 24 July 2015 ("the Law of 24 July 2015"). PI further believes that this case provides an opportunity for the Court to apply its Article 8 jurisprudence to these novel forms of surveillance.

2. The President of the Fifth Section granted PI leave to intervene as a third party in these cases on 18 July 2017. As directed, these submissions do not comment on the facts or merits of the case.

3. Privacy International is a non-profit, nongovernmental organisation based in London, the United Kingdom ("UK"), dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into state and corporate surveillance with the aim of advancing strong national, regional, and international laws that protect privacy. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States of America, the UK, and Europe, including the European Court of Human Rights and the Court of Justice of the European Union. Privacy International employs technologists and lawyers, who work together to understand the technical underpinnings of novel surveillance technology and to consider how existing legal definitions and frameworks map onto such technology.

4. PI summarises its intervention as follows:

    a. Section I provides background on the new surveillance powers introduced in the Law of 24 July 2015 and their implications for the right to privacy;

    b. Section II provides a summary of international human rights authorities that have addressed these new surveillance powers;

I. NEW SURVEILLANCE POWERS INTRODUCED IN THE LAW OF 24 JULY 2015 AND THEIR IMPLICATIONS FOR THE RIGHT TO PRIVACY

5. The Law of 24 July 2015 authorised the French intelligence services to utilize several new surveillance powers for the purpose of preventing terrorism. In particular, the Law authorises:

    a. The installation of "black boxes" on the networks of electronic communications services (e.g. telecommunications operators), internet service providers, and web-hosting providers (together, "operators") to conduct real-time automated data processing to detect terrorism threats (Art. L. 851-3). The Law further authorises the real-time collection of metadata of individuals "identified as a [terrorist] threat", "likely to be related" to such a threat, or who belong to the "entourage" of such individuals (Art. L. 851-2, 851-3).[1] In addition, the Law authorises the installation of technical devices to collect other types of metadata, including data permitting the identification of terminal equipment used or its user subscription number as well as data relating to the location of terminal equipment (Art. L. 851-6).

    b. Hacking to (1) access, collect, retain, and transmit data stored on a computer system and (2) access, collect, retain and transmit data as it is displayed on a user's computer screen, entered by keystrokes, or as received and transmitted by audio-visual peripheral devices (e.g. microphones, cameras and sensors) (Art. L. 853-2). Hacking may only be authorised where "intelligence cannot be collected by any other legally authorized means".[2]

    c. The use of IMSI catchers, which can collect mobile phone data and track individuals' locations. The Law authorises the use of technical devices, including IMSI catchers, to enable real-time tracking of a person, vehicle or object. (Art. L. 851-5). The French Parliament has also admitted in a public statement that that IMSI Catchers may be used to intercept "telephone conversations involving individuals designated by name".[3]

---

[1] This provision originally only applied to individuals "identified as a [terrorist] threat" ("*identifiée comme présentant une menace*"). On 20 July 2016, an amendment to this provision altered this language to cover individuals "likely to be related" to such a threat ("*identifiée susceptible d'être en lien avec une menace*") or who belong to the "entourage" of such individuals ("*personnes appurtenant à l'entourage de la personne concernée*"). *See* Prorogation de l'état d'urgence, 20 July 2016, available at http://www.senat.fr/amendements/commissions/2015-2016/803/Amdt_COM-15.html.

[2] The original French reads "*lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé*").

[3] French Parliament, *Parliament Adopts the Intelligence Bill*, 30 June 2015, *available at* www.gouvernement.fr/en/parliament-adopts-the-intelligence-bill.

"Black Boxes"

6. The Law of 24 July 2015 lacks clarity in its description of the so-called "black boxes," which are simply described as "automated processing techniques."[4] Debate and commentary around the Law indicates that the "black boxes" consist of algorithmic systems designed to analyse all data flowing through operator networks to detect terrorism threats.[5] But the Law of 24 July 2015 provides no detail regarding the substance or nature of these algorithms, including whether they are machine learning (*i.e.*, learn iteratively from data without explicit programming). Nor does the Law explain whether operators are required to retain the data to facilitate their processing and if so, for how long.

7. The requirement that operators install a "black box" constitutes a form of "direct access." "Direct access" broadly describes a technical or legal practice permitting government authorities to interfere directly with data on operator networks. Traditionally, "direct access" has involved the government directly tapping into an operator's network to intercept communications or data.[6] But "black boxes", like "direct access", also give the government a direct means of interfering with users' privacy on operator networks. Importantly, "black boxes" permit the government to directly control the manner of processing personal data transiting such networks.

8. Companies have begun challenging different forms of "direct access", highlighting how this practice can facilitate unchecked government surveillance. Thus, the Telecommunications Industry Dialogue published a statement in 2014 expressing the view that:

> "Government surveillance programs should be subject to ongoing review by an independent authority and . . . governments should not conduct any type of registry, search, or surveillance by means of direct access to companies' infrastructure without any technical control by the company . . . ."[7]

9. The installation of a "black box" on an operator network subjects the data of *all* users of that network to processing. Like bulk data retention, "black boxes" are therefore a general and

[4] The original French reads "*il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destines*."
[5] *See, e.g.*, Damien Leloup & Jacques Folloru, "Loi sur le renseignment : les « boîtes noires » loin d'être mises en place", Le Monde, 15 February 2016, available at http://www.lemonde.fr/pixels/article/2016/02/15/loi-sur-le-renseignement-les-boites-noires-loin-d-etre-mises-en-place_4865698_4408996.html.
[6] *See generally*, Privacy International, Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Study on Telecommunications and Internet Access Sector, November 2016, *available at* www.privacyinternational.org/sites/default/files/UN%20SR%20FOE%20Study%20on%20ICT%20Sector%20submission.pdf.
[7] The Telecommunications Industry Dialogue at Two Years: Advances in Respecting Freedom of Expression and Privacy in 2014, p. 6, (May 2015), *available at* www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Dialogue-Annual-Report-2015.pdf (noting further that this statement "has guided the Industry Dialogue in its conversations with government authorities and its inputs to public consultations"). The Telecommunications Industry Dialogue is a group of telecommunications operators and vendors who work together to address freedom of expression and privacy rights in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights. *See* Telecommunications Industry Dialogue, About Our Initiative, *available at* http://www.telecomindustrydialogue.org/about/.

indiscriminate measure.[8] Moreover, the interference to privacy presented by "black boxes" is significant. "Black boxes" involve the processing of metadata, which tells the story of our data, answering the who, when, what, and how of a specific communication.[9] As noted by the Court of Justice of the European Union ("CJEU") in *Tele2 Sverige AB & Watson et al.*, metadata "is liable to allow very precise conclusions to be drawn concerning the private lives of . . . persons . . . , such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them." The CJEU further observed that metadata "provides the means . . . of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."[10]

10. "Black boxes" also present novel and grave concerns related to the use of automated processing in government surveillance programs. The automated processing of data to derive, infer or predict certain attributes or behaviour of a person is also referred to as profiling.[11] Profiling poses a number of related risks, particularly if used to make or inform decisions affecting individuals. First, the process of profiling can be highly opaque, in particular if it based on advanced techniques, such as machine learning. It can also be difficult even for the designers of such systems (not to speak of their operators, or those affected) to understand how or why an individual has been profiled in a particular way, or why a system has made a particular decision.[12] This opacity can weaken oversight and accountability of surveillance that relies upon algorithmic systems.

11. Second, since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, profiling may also lead to individuals being misclassified, misidentified or misjudged.[13] Moreover, these errors may disproportionately affect certain groups of people. And potentially harmful or discriminatory outcomes may be neither predictable nor discoverable by their designers, operators, or those affected. When profiling is used to inform or feed into a decision that affects individuals – as in a surveillance system – the outcome of such decisions may result in significant harm.

---

[8] *See* Tele2 Sverige AB & Watson et al., C-203/15 & C-698/15, Court of Justice of the European Union, Grand Chamber, Judgment, 21 December 2016, paras. 103, 112.
[9] *See* Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement, available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031940885&categorieLien=id.
[10] *Tele2 Sverige AB & Watson et al, supra* note 8, at para. 99.
[11] *See* Articles 4 & 22, European Union General Data Protection Regulation.
[12] The level of difficulty depends on the kinds of algorithms being used, whether these are learning, and how they are trained.
[13] *See e.g.* Bruce Schneier, *Surveillance by Algorithm*, Schneier on Surveillance Blog, 5 March 2014, *available at* www.schneier.com/blog/archives/2014/03/surveillance_by.html (noting that "any time we're judged by algorithms, there's the potential for false positives. You are already familiar with this; just think of all the irrelevant advertisements you've been shown on the Internet, based on some algorithm misinterpreting your interests. In advertising, that's okay. It's annoying, but there's little actual harm, and you were busy reading your email anyway, right? But that harm increases as the accompanying judgments become more important . . . . Computer algorithms are intimately tied to people. And when we think of computer algorithms surveilling us or analyzing our personal data, we need to think about the people behind those algorithms. Whether or not anyone actually looks at our data, the very fact that they even could is what makes it surveillance."); *see also* Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68(4) FLORIDA L. R. 1045, 1075-1079 (2016) (mapping both deontological and consequentialist harms from machine searches and concluding that the risks of such harms "points towards the need for safeguards").

Government Hacking

12. Government hacking is unlike any other form of existing surveillance technique. Hacking is an attempt to understand a system better than it understands itself, and then nudging it to do what the hacker wants. Fundamentally speaking, hacking is therefore about causing technologies to function in a manner the manufacturer, owner or user did not intend. Governments can wield this power remotely, surreptitiously, across jurisdictions, and at scale. A single hack can target many people, even those who are incidental or unrelated to a government investigation or operation.

13. Hacking permits governments remote access to systems and therefore potentially to all of the information stored on those systems. For an increasing number of people, personal digital devices contain the most private information they store anywhere, replacing and consolidating address books, physical correspondence, journals, filing cabinets, photo albums and wallets. Increasingly, government hacking powers may target new and emerging devices, like the "Internet of Things" and body-worn and –embedded devices, such as health sensors.

14. Hacking also permits governments to conduct novel forms of real-time surveillance. Hacking permits governments to covertly turn on a device's microphone, camera, and GPS-based locator technology. Through hacking, governments can also capture continuous screenshots of the hacked device or see anything inputted to and emerging from that device, including login details and passwords, internet browsing histories, and documents and communications the user never intended to disseminate.

15. The privacy intrusions of hacking are enormously amplified should a government target communications networks and their underlying infrastructure itself. By hacking a network provider, for instance, a government might gain access not only to the provider's system, but also through the data stored there, to the systems of all its users. Governments may also target different types of networks and their infrastructure, such as those connecting banks.

16. Government hacking is equally concerning from a security perspective. Computer systems are complex and, almost with certainty, contain vulnerabilities (i.e. weaknesses or flaws in a computer system or application).[14] In the surveillance context, the government identifies vulnerabilities, not to secure systems through testing and responsible disclosure, but to exploit them to facilitate a surveillance objective. This activity may not only undermine the security of the target system but also of other systems.

17. Security concerns also abound when governments take advantage of people to interfere with their own systems. Phishing, for example, is a common hacking technique whereby a hacker impersonates a reputable person or organisation. Phishing attacks typically take the form of an email or text message, which may contain a link or attachment infected with malware. These techniques prey on user trust, which is critical to maintaining the security of systems and the internet as a whole.

[14] *See* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 2014, pp. 22-23 ("A vulnerability is a weakness in a system that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system.").

IMSI Catchers

18. IMSI catchers are surveillance devices used to collect mobile phone data and track individuals' locations. Mobile phones communicate with a network of base stations, which enable the network provider to route calls, text messages and internet data to and from the mobile phone. IMSI catchers function by impersonating a base station, thereby tricking mobile phones into identifying themselves by revealing their IMSI.[15] This identification process also allows IMSI catchers to determine the location of mobile phones. Some IMSI catchers also have the capability to intercept data, including calls, text messages, and internet data as well as block service, either to all mobile phones within their range or to select devices.

19. IMSI catchers interfere with the right to privacy in several ways. Where they intercept the data transmitted from mobile phones, such as calls, text messages, and internet data, they pose the same privacy concerns as traditional methods of communications surveillance.

20. The interception of IMSI/IMEI data can also raise several privacy concerns. A mobile phone is "very intimately linked to a specific individual", meaning IMSI/IMEI data can also be tied to specific individuals.[16] By linking IMSI/IMEI data to other information, the government can not only determine the identity of individuals, but also track and profile those individuals. For example, by tracking IMSI/IMEI data across a number of locations, the government can create a profile of an individual's activities and contacts.

21. The use of IMSI catchers also raises particular concerns because of the indiscriminate nature by which they collect data. IMSI catchers trick all mobile phones within a given range to identify themselves and reveal their location. Their use can therefore interfere with the privacy rights of many persons, including those who are not the intended targets of surveillance.

22. The indiscriminate nature by which IMSI catchers collect data means that their use can also interfere with the rights to freedom of expression and to freedom of assembly and association, as enshrined respectively in Articles 10 and 11 of the ECHR. Governments can use IMSI catchers at gatherings of individuals, such as a protest, to identify those attending such gatherings.

23. Finally, the use of IMSI catchers has a number of implications for the ability of individuals to maintain their anonymity, including when attending a gathering. Privacy International has discussed the inextricable linkages between anonymity, privacy, and freedom of expression in a prior intervention before this Court.[17]

[15] IMSI catchers typically also capture the "International Mobile Station Equipment Identifier" ("IMEI") of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each Subscriber Identification Module ("SIM") card.
[16] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN, 16 May 2011, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.
[17] *See* Written Submissions on Behalf of Privacy International and Article 19, Breyer v. Germany, European Court of Human Rights, App. No. 50001/12, 5 September 2016.

II. INTERNATIONAL HUMAN RIGHTS AUTHORITIES THAT HAVE CALLED FOR THE REGULATION OF THESE NEW SURVEILLANCE POWERS

24. The relative novelty of the above surveillance technologies and capabilities means that international human rights authorities have yet to fully grapple with their implications for the right to privacy and other fundamental rights. PI therefore believes that this case provides an important opportunity for the Court to apply its Article 8 jurisprudence to these novel surveillance powers. Below, PI provides an overview of the authorities that have to date addressed these powers.

"Black Boxes"

25. With respect to "direct access", this Court has never explicitly addressed a "black box"-like surveillance measure. However, in *Zakharov v. Russia*, this Court held that:

> "[T]he requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception. In Russia . . . communications service providers must install equipment giving the law-enforcement authorities direct access to all mobile telephone communications of all users. . . . The Court considers a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great."[18]

26. In a March 2017 report, the U.N. Special Rapporteur on Freedom of Expression echoed this position, noting that:

> "Direct access to Internet and telecommunications networks enables authorities to intercept and monitor communications with limited legal scrutiny or accountability. Technological advances have enhanced the ability of law enforcement and intelligence agencies to obtain a direct connection to networks without the involvement of the network operator . . . . These activities [lack] both judicial authorization and external oversight. Furthermore, the risks they pose to the security and integrity of network infrastructure raise proportionality concerns".[19]

27. With respect to automated data processing, the U.N. Human Rights Council has noted that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights". It accordingly

[18] Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment, 4 December 2015, paras. 269-270. Although the Court implicitly addresses here the more traditional form of "direct access" – *i.e.* direct interception of communications – the principles discussed here may be applicable to other forms of "direct access", including the use of "black boxes".

[19] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/35/22, 30 March 2017, para. 22.

recognised "the need to further discuss and analyse these practices on the basis of international human rights law."[20]

28. In a recent decision, the CJEU considered the compatibility of automated data processing with Articles 7 and 8 of the EU Charter of Fundamental Rights in the context of the draft EU-Canada Passenger Name Records ("PNR") agreement.[21] Pursuant to the agreement, PNR data is "to be subject to analyses by automated means, based on pre-established models and criteria and on cross-checking with various databases." As a general matter, the CJEU held:

> "[T]he legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. *The need for such safeguards is all the greater where personal data is subject to automated processing.*"[22]

29. The CJEU noted, in particular, that analyses based on automated data processing "necessarily present some margin of error" and that "that margin of error appears to be significant." The Court accordingly held that "the pre-established models and criteria should be specific and reliable, making it possible . . . to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory." The Court further held that "any positive result obtained following the automated processing of that data must . . . be subject to an individual re-examination by non-automated means before an individual measure adversely affecting [that individual] is adopted."[23]

Hacking

30. The U.N. Special Rapporteur on Freedom of Expression has noted with respect to hacking:

> "Offensive intrusion software such as Trojans . . . constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights

[20] U.N. Human Rights Council, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 March 2017.
[21] The draft agreement provided for the bulk transfer of PNR data between the EU and Canada. PNR includes, *inter alia*, data relating to " the passenger's identity, nationality and address, all contact information (address of residence, email address, telephone number) available about the passenger who made the reservation, available payment information, including, where appropriate, the number of the credit card used to reserve the flight, information relating to luggage, passenger travel habits and habits relating to additional services requested by the passengers concerning any health problems, including mobility, or their dietary requirements during the flight, which might provide information concerning, in particular, the health of one or more passengers, their ethnic origin or their religious beliefs." Opinion of Advocate General Mengozzi, Opinion 1/15, Request for an opinion submitted by the European Parliament, Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 8 September 2016, para. 169.
[22] Opinion 1/15 of the Court, Request for an opinion submitted by the European Parliament, Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 26 July 2015, paras. 141, 168 (emphasis added).
[23] *Id*. at paras. 169-70, 172-73.

> perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy [but also] procedural fairness rights with respect to the use of such evidence in legal proceedings."[24]

In his conclusions, the Rapporteur recommended that in light of the evolution of surveillance technology, States "update their understandings and regulation of communications surveillance and modify their practices in order to ensure that individuals' human rights are respected and protected."[25]

31. In March 2017, the U.N. Human Rights Committee pronounced for the first time on the application of Article 17 of the International Covenant on Civil and Political Rights to hacking as a form of surveillance. Addressing reports of the practice by Italian intelligence agencies of intercepting communications through "hacking techniques", the Committee noted the lack of "clearly defined safeguards from abuse" and called on Italy to review its policies relating to hacking in order to ensure that:

> "(a) such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity; (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking."[26]

32. It is for the Court to apply the legal standards of "necessity" and "proportionality" in light of the particular factual context of the surveillance powers in question. As discussed above, hacking presents unique privacy and security risks, which leave open the question of whether this form of surveillance can ever be compatible with ECHR Article 8. Nevertheless, in assessing whether the hacking powers in the Law of 24 July 2015 are compliant with Article 8, the Court may wish to consider whether the Law contains measures designed to address the particular risks posed by this power. For example, the Court might consider several measures designed to address the security risks posed by hacking. With respect to the judicial authorisation process, those measures might include requiring the government to indicate the method, extent and duration of the proposed hacking measure as well as the potential risks and damage to the security and integrity of both targeted systems and systems generally posed by that measure.[27] They might further require that the judicial authorisation process include an assessment of the proportionality of

[24] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, 17 April 2013, at para. 62.
[25] *Id*. at para. 78.
[26] Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6, 28 March 2017, paras. 36-37.
[27] *See Zakharov*, *supra* note 18, at para. 233 ("In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure." (citing Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment, 6 September 1978, paras. 55-56).

the hacking measure against its security implications.[28] Finally, the Court might also consider a measure requiring that judicial authorities be able to consult persons with technical expertise in the relevant technologies, who may assist the authorities in understanding how the proposed measure will affect the targeted system and systems generally.

IMSI Catchers

33. The U.N. Special Rapporteur on Freedom of Expression has highlighted with concern government use of IMSI catchers, noting that such measures can allow States to "track the movements of specific mobile phones, identify all individuals with a mobile phone within a designated area, and intercept calls and text messages." He further noted that IMSI catchers may be "installed in a location temporarily (such as a protest or a march) or permanently (such as at an airport or other border crossings)."[29]

34. International human rights authorities have also moved towards recognising anonymity as a right under the rights to privacy and freedom of opinion and expression. The U.N. Special Rapporteur on Freedom of Expression has repeatedly identified this relationship and emphasised that any interference with anonymity should be subject to the same three-part test of legality, necessity, and proportionality as any other interference with these rights.[30] This commentary has application to the use of IMSI catchers, which are a surveillance tool that can significantly restrict the ability of individuals to maintain their anonymity.

Scarlet Kim
Legal Officer
Privacy International
Tel: +44 (0)20 7242 283
scarlet@privacyinternational.org

[28] As discussed above, hacking permits the government to interfere with a system for several different purposes – e.g. to access information, to remotely turn on a microphone or camera, or to take continuous screenshots. The use of the term "hacking measure" serves to emphasise that the government must seek separate authorisations for different purposes. In other words, it cannot seek a single authorisation to access information and to conduct real-time surveillance using a microphone or camera. Because each purpose raises distinct privacy and security concerns, they should be subject to distinct necessity and proportionality analyses.
[29] U.N. Doc. A/HRC/23/40, *supra* note 24, at para. 36.
[30] *Id*. at para. 79; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/29/32, 22 May 2015, para. 16; Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27, 16 May 2011, paras. 24, 59; *see also* Written Submissions, *Breyer*, *supra* note 17, at paras. 12-23.