IMSI catchers legal analysis

June 2020

privacyinternational.org

Executive Summary

The majority of people today carry a mobile phone with them wherever they go, which they use to stay connected to the world. Yet an intrusive tool, known as an International Mobile Subscriber Identity catcher, or "IMSI catcher" is a form of surveillance equipment that enables governments and state authorities to conduct indiscriminate surveillance of mobile devices, and by extension, on users.

IMSI catchers can do much more than monitor and intercept mobile communications. Designed to imitate mobile phone towers, they also entice mobile phones to reveal their IMSI and International Mobile Equipment Identity ("IMEI") data, which is data tied to individuals. This allows otherwise anonymous people to be readily identified, and their locations to be tracked.

The government use of IMSI catchers has major implications for our fundamental rights, not least because as with other indiscriminate forms of mass surveillance, IMSI catchers have a chilling effect on civic society.

In this legal analysis, we examine how the intrusive and unregulated use of IMSI catchers infringes on our right to privacy, freedom of expression, and freedom of assembly and association, as guaranteed under international human rights law. IMSI catchers are often deployed in secret, without a clear legal basis, and without the safeguards and oversight mechanisms.

To date, there has been insufficient public debate about the scope and nature of government IMSI catcher use, including the extent that this surveillance technique interferes with human rights in a democratic society.

Contents

1. IMSI catchers

1.1. What IMSI catchers are

An International Mobile Subscriber Identity catcher – often referred to as an "IMSI catcher" – is a surveillance tool for mobile devices. An IMSI catcher is an intrusive piece of technology that can be used to locate and track all mobile phones that are switched on in a certain area.[1]

An IMSI catcher does this by 'pretending' to be a mobile phone tower - tricking the user's phone into connecting to the IMSI catcher, and then revealing the phone user's personal details without the user's knowledge.[2]

The image to the left is an example of an IMSI catcher that is likely to be used by police forces operationally.[3] The IMSI catcher itself has the size and 'look' of a wifi access point.

By enticing all mobile phones within their range to connect to them, IMSI catchers force those mobile phones to transmit their IMSI and International Mobile Equipment Identity ("IMEI") data.[4] The IMSI is a unique number found in a SIM card, whereas the IMEI is a unique number bound to

[1] Privacy International, "IMSI Catchers", 6 August 2018, available at https://privacyinternational.org/explainer/2222/imsi-catchers (accessed 01/04/2020).

[2] N.B. IMSI catchers affect all mobile devices that have an IMEI number and sim card connected to a mobile network, including mobile tablets. However, this briefing primarily focuses on how IMSI catchers interfere with mobile phones.

[3] See Witness Statement of Silke Holtmanns, *Privacy International v. Information Commissioner's Office and Others* case no. EA/2018/0164-0172, UK first-tier tribunal, 15 April 2019, available at https://privacyinternational.org/sites/default/files/2019-09/Silke%20Holtmanns%20Witness%20Statement%20-%20readacted.pdf (accessed 01/04/2020).

[4] For further information on the technical operation of IMSI catchers, see Witness Statement of Silke Holtmanns, *supra* note 3.

a mobile device that is used to identify the device on a mobile network. This is very personal information, as it is explained below in section **2.3**.

N.B. Before we explore they ways in which IMSI catchers can interfere with our fundamental human rights, it should be made clear that:
a) The capabilities of IMSI catchers vary from model to model.
b) Given the capability of the IMSI catcher, the way it functions (meaning the type of interception it carries out) is determined by the person operating it.

Some IMSI catchers can be used to 'intercept' our text messages, calls and internet traffic. This would allow whoever is operating the IMSI catcher to read or listen to our personal communications. Some IMSI catchers can even re-route or edit communications and data sent to and from our phone. This means that they can be used to edit a message we wrote without our knowledge. Finally, some IMSI catchers can be used to block service so we can no longer use our phone to make or receive calls and text messages – even for emergency calls.

1.2. Why IMSI catchers matter

IMSI catchers can be used to identify people. This matters due to the way that individuals throughout the world use and depend on their mobile phones.

Mobile phone ownership is at its highest level globally. In the UK alone, the vast majority of people own at least one mobile phone and carry that phone with them wherever they go.[5] Further, within the large majority of phone owners it is much more common to own one's own phone than to share it with someone else.[6] As a result, because a mobile phone is "very intimately linked to a specific individual" and "it seldom happens that a person lends such a device to another person",[7] IMSI and IMEI data are typically tied to a specific person and can be used to identify that person, like a social identity or passport number.[8]

[5] According to Deloitte's 2019 Mobile Consumer Survey, 89% of respondents (spanning the ages of 18-75 years) owned or had ready access to a smartphone. And of those who owned a smartphone, 95% reported using it at least once in the last day. Deloitte, "Global Mobile Consumer Survey 2019: UK cut", 2019, available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology-media-telecommunications/deloitte-uk-plateauing-at-the-peak-the-state-of-the-smartphone.pdf (accessed 31/03/20).

[6] Pew Research Center, "Mobile Connectivity in Emerging Economies", March 2019, available at https://www.pewresearch.org/internet/2019/03/07/use-of-smartphones-and-social-media-is-common-across-most-emerging-economies/ (accessed 31/03/20).

[7] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN, 16 May 2011, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf p.7 (accessed 31/03/20).

[8] See Witness Statement of Silke Holtmanns, *supra* note 3, §6.

IMSI catchers are indiscriminate surveillance tools: just like the target of the surveillance, bystanders in the vicinity will be unlikely to control or notice when their phone tries to connect to the fake mobile phone tower. As a result, IMSI catchers cause mobile devices to act in a manner the manufacturer, owner or user did not intend or did not foresee. Indiscriminate surveillance of non-suspects is a contravention of rights and a failure of the rule of law. As with other forms of secret mass surveillance, it is impossible for states to carry out an individualised assessment of necessity and proportionality, which is not permissible under international human rights law.[9]

Hence, IMSI catchers are a cause for concern. They collect IMSI and IMEI data to identify people, and so can track who attends public events, ranging from a political demonstration to a football match. Not only that, IMSI catchers can monitor our calls and edit our messages, and even block access to emergency calls – all without us knowing it was happening.

In comparison to more traditional surveillance methods where for example, authorised government officials could obtain similar data directly from the mobile operator for a specific target, IMSI catcher activities are less traceable in terms of how they operate and what persons, including bystanders, have been affected.[10]

2. IMSI catchers and the right to privacy

Given the way that they operate and the variety of capabilities they may have, IMSI catchers can interfere with the right to privacy in a number of ways.

This includes the following:

- By monitoring and intercepting communications, including phone calls and text messages;
- By monitoring and intercepting communications data;
- By forcing all mobile phones within range to transmit their IMSI and IMEI data, which can identify people;
- By enabling the location tracking of mobile phones (and therefore their users); and

[9] UN High Commissioner for Human Rights, the right to privacy in the digital age, UN Doc. No. A/HRC/39/29, 3 August 2018, §17, available at https://undocs.org/A/HRC/39/29 (accessed 01/04/2020).
[10] See Witness Statement of Silke Holtmanns, *supra* note 3.

- By indiscriminately monitoring and collecting people's data (including those of non-suspects).

2.1. Monitoring and intercepting communications

Mobile phones must connect to base stations (also known as mobile phone towers) to receive calls and texts. IMSI catchers can intercept communications by acting as a 'man-in-the-middle' between a person's phone and a real base station. An IMSI catcher will present itself to the phone as a real base station, while presenting itself to the real base station as the phone. In this way, the IMSI catcher can monitor activity between the phone and the network and intercept incoming and outgoing communications.

Where IMSI catchers intercept communications transmitted to and from mobile phones, such as phone calls and text messages, they interfere with the right to privacy in a similar way to traditional methods of communications surveillance, such as wiretapping.

International human rights law has long recognised the intrusiveness inherent in government interception of the content of communications. The UN Human Rights Committee, the treaty body charged with monitoring implementation of the International Covenant on Civil and Political Rights ("**ICCPR**"), has explicitly addressed the nature of interference posed by communications interception in its interpretation of the right to privacy recognised by Article 17 of the ICCPR:

> "Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[11]

The European Court of Human Rights ("**ECtHR**") also has a considerable body of jurisprudence recognising that government interception of communications constitutes an interference with the right to privacy enshrined in Article 8 of the European Convention on Human Rights ("**ECHR**").

[11] UNHRC, General Comment No. 16: Article 17 (Right to Privacy), UN Doc. HRI/GEN/1/Rev.9 (Vol. 1), available at https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=HRI/GEN/1/Rev.9%20%28Vol.%20I%29&Lang=en (accessed 01/04/2020).

In *Klass v. Germany*, the European Court held that "telephone conversations" are "covered by the notions of 'private life' and 'correspondence'" referred to in Article 8 para. 1.[12] Since *Klass*, advancements in modern technologies, including the advent of the internet, have revolutionised the way we communicate. The Court has acknowledged these developments, expanding the scope of Article 8 protection to modern forms of communication, including "mobile telephone communications"[13] and "personal information related to telephone, email and internet usage".[14] And more recently, the Court has reasoned that "[g]iven the technological advances since the *Klass and Others* case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely".[15]

2.2. Monitoring and intercepting communications data

Once connected to a mobile phone, an IMSI catcher may not only intercept communications (meaning the content of communications) but also communications data transmitted to and from that phone.[16]

Communications data (sometimes called metadata) is information about a communication, such as the sender and recipient, the date and location from where it was sent, and the subject line.[17] The interception of communications data concerns not only data about telephone and text communications, but also data concerning the increasing amount of internet activity people conduct on the phone.

European courts have recognised that the interception of communications data can be as intrusive to privacy as the interception of content. Recently, in *Big Brother Watch and Others v. United Kingdom*, the ECtHR observed:

> "[T]he Court is not persuaded that the acquisition of…communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient…[C]ommunications data, on the other

[12] *Klass v. Germany*, App. No. 5029/71, ECtHR, Judgment, 6 September 1978, § 41.
[13] *Zakharov v. Russia*, App. No. 47143/06, ECtHR (Grand Chamber), Judgment, 4 December 2015, §163.
[14] *Benedik v. Slovenia*, App. No. 62357/14, ECtHR, Judgment, 24 July 2018, *§*104.
[15] *Szabó and Vissy v. Hungary,* App no. 37138/14, ECtHR, Judgment, 12 January 2016, *§*53.
[16] See Witness Statement of Silke Holtmanns*, supra* note 3, §19.
[17] Privacy International, *"*How intrusive is communications data*?",* 21 August 2019, available at https://privacyinternational.org/long-read/3176/how-intrusive-communications-data (accessed 01/04/2020).

hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted."[18]

The ECtHR's *Big Brother Watch* ruling also reinforces prior rulings of the Court of Justice of the European Union ("**CJEU**"), which have similarly acknowledged the intrusiveness of intercepting communications data. In *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Watson* (*Tele2/Watson* case), the CJEU observed:

> "[Communications data] makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place."[19]

The EU Court then concluded that:

> "data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, 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".[20]

The rulings of both the ECtHR and the CJEU are further buttressed by the interpretation of the right to privacy articulated by international human rights expert bodies. In its most recent report

[18] *Big Brother Watch and Others v. The United Kingdom*, App. nos. 58170/13, 62322/14 and 24960/15, ECtHR, judgment, 13 September 2018, §356. Similarly, the Article 29 Data Protection Working Party (now the European Data Protection Supervisor) has warned that communications data "often yield information more easily than the actual content of our communications do". Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014, pp 4-5, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf (accessed 01/04/2020).

[19] *Tele2 Sverige AB v. Post- ochtelestyrelsen* (Case C-203/15) and *Secretary of State for the Home Department v. Watson* (Case C-698/15), Court of Justice of the European Union, Judgment, 21 December 2016, §98.

[20] *Id*. at §99. (citing *Digital Rights Ireland v. Minister for Communications,* Case C-293/12, Court of Justice of the European Union, Judgment, 8 April 2014, §27).

on "The Right to Privacy in the Digital Age", the Office of the High Commissioner for Human Rights ("**OHCHR**") declared that:

> "[t]he protection of the right to privacy is broad, extending not only to the substantive information contained in communications but equally to metadata as, when analysed and aggregated, such data 'may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication'".[21] Indeed, in a prior report, the OHCHR concluded that "any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used."[22]

Today, many people conduct major portions of their lives by accessing the internet through their mobile phones, which generates communications data as the phone communicates with the network. People use the internet to conduct daily activities, such as keeping records, arranging travel and managing financial transactions. They may also use the internet to conduct research, explore their sexuality, and seek medical advice and treatment. Communications data can reveal these activities, for example, by capturing web browsing history, which can indicate political affiliations, religious viewpoints or medical conditions. News sites visited, forums joined, items purchased, books read, movies watched and games played are all pieces of communications data that expose intimate details of who a person is and what they think. By intercepting such communications data, IMSI catchers enable the government to obtain an intrusive, deep and comprehensive view into a person's private life.

2.3. IMSI and IMEI data: Personal data

International human rights bodies have not yet had the opportunity to expound on the nature of the interference with the right to privacy when a government collects IMSI or IMEI data. However, these bodies have had opportunities to consider the intrusiveness when the government collects information that can similarly be used to identify a user or subscriber of a telecommunications service.

[21] The right to privacy in the digital age, UN Doc. No. A/HRC/39/29, *supra* note 10 §6, (quoting UN High Commissioner for Human Rights, the right to privacy in the digital age, UN Doc. No. A/HRC/27/37, 30 June 2014, §19, available at https://undocs.org/A/HRC/27/37, (accessed 01/04/2020)).

[22] The right to privacy in the digital age, UN Doc. No. A/HRC/27/37, *supra* note 22, §20.

One such example of such intrusiveness is government collection of Internet Protocol ("**IP**") addresses. An "IP address is a unique number assigned to every device on a network".[23] A static IP address is "a unique number" that "is permanently allocated to a particular network interface of a particular device".[24] By contrast, "a dynamic IP address is assigned to a device by the ISP [internet service provider] temporarily, typically each time the device connects to the internet".[25]

Like IMSI/IMEI data, an IP address can enable the government to identify the user of a particular service. Similarly, both categories of data are not readily available to the public, in that they cannot be cross-referenced in publicly available registries to determine a person's identity.

It is important to note that IP addresses can only form a floor for comparison to IMSI/IMEI data. Both dynamic and static IP addresses are an imperfect analogy because IMSI/IMEI data is a much more effective type of data for identifying a specific person. For example, one head of a household may be the subscriber to the internet service of that household, but other members of the household may have access to and use the computer to which the IP address is assigned, even if it is a static IP address. Dynamic addresses are an even less specific identifier in that they are only temporarily assigned. By contrast, because people so rarely lend their mobile phones (let alone their SIM cards) to others, the likelihood that IMSI/IMEI data is uniquely linked to a single person is much higher than for an IP address.

The ECtHR has held that government collection of a dynamic IP address can constitute an interference with the right to privacy.[26] In its judgment, the ECtHR emphasised that "private life is a broad term not susceptible to exhaustive definition" and also proceeded to articulate the nexus between privacy and the protection of personal data:

> "In the context of personal data, the Court has pointed out that the term 'private life' must not be interpreted restrictively. It has found that the broad interpretation corresponds with that of the 1981 Convention [for the Protection of Individuals with regard to Automatic Processing of Personal Data], the purpose of which is 'to secure in the territory of each Party for every individual...respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him' (Article 1). **Such personal data are defined as 'any information relating to an identified or identifiable individual'**.

[23] *Benedik v. Slovenia*, App. No. 62357/14, ECtHR, judgment, 24 April 2018, §96.
[24] *Id.*
[25] *Id.*
[26] *Id.* §96.

> It further follows from well-established case law that where there has been a compilation of data on a particular individual, the processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged."[27]

The ECtHR also emphasised that the particular context for collecting the dynamic IP address in this case was to identify the user behind particular online activities and noted that "there is a zone of interaction of a person with others which may fall within the scope of 'private life'" and that "[i]nformation on such activities engages the privacy aspect the moment it is linked to or attributed to an identified or identifiable individual".[28]

Finally, the ECtHR observed that the applicant in the case "could have reasonably expected privacy in relation to his identity", notwithstanding the fact "that he did not hide his dynamic IP address, assuming that it is possible to do so".[29]

For similar reasons, government collection of IMSI/IMEI data constitutes an interference with the right to privacy. IMSI/IMEI data is clearly a form of personal data and to a much higher degree of specificity than IP addresses (dynamic or static) relate to an identifiable individual. The government collection of IMSI/IMEI data through IMSI catchers is likely for the purpose of identifying mobile phone users. And finally, it is reasonable to presume that most individuals, when using their mobile phone throughout their day, maintain an expectation of privacy with respect to their identity.

This conclusion is further supported by the interpretation of the right to privacy articulated by international bodies. The UN General Assembly, in its resolutions on "The right to privacy in the digital age", has "[e]mphasiz[ed] that…the unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of

[27] *Id*. at §100, 102-03 (emphasis added). *Benedik* referred also to the CJEU case *Breyer v. Germany*, which provided a detailed exposition on why dynamic IP addresses may constitute a form of personal data subject to protection under the European Charter of Fundamental Rights. That judgment held that dynamic IP addresses can constitute a form of personal data where "the possibility to combine a dynamic IP address with…additional data…constitutes a means likely reasonably to be used to identify the data subject." *Breyer v. Germany*, Case C-582-14, Court of Justice of the European Union, judgment, 19 October 2016, §45.
[28] *Id*. §109.
[29] *Id*. §116.

expression and may contradict the tenets of a democratic society".[30] And the OHCHR has similarly emphasised that the right to privacy extends to the "generation and collection of data relating to a person's identity…as through those steps an individual loses some control over information that could put his or her privacy at risk".[31] It has also observed that government collection of "steadily increasing amounts of data related to the private lives of individuals" includes a "range and depth of…information" that is "vast", including "device identifiers, email addresses and phone numbers".[32]

2.4. Location tracking and monitoring

The collection of IMSI/IMEI data also interferes with the right to privacy by enabling the government to locate and track individuals. Some IMSI catchers can pinpoint a mobile phone down to approximately 10 feet.[33] Once a mobile phone has revealed its IMSI/IMEI, an IMSI catcher can determine its general location by measuring the strength of the signal from the phone. Moving the IMSI catcher around and measuring the strength of the signal from different locations permits a more precise triangulation of the phone's location.[34] It also enables the government to track the movements of a phone and therefore its user.[35]

The ECtHR has held that government collection of location data can constitute an interference with the right to privacy. In *Ben Faiza v. France*, the ECtHR found that the government's affixing of a GPS receiver to an applicant's vehicle interfered with his right to privacy because it can track the real-time movements of a person.[36] Importantly, it noted that one method by which the government may enable such tracking (in addition to the use of a GPS receiver) is by monitoring

[30] UN General Assembly resolution 73/179, the right to privacy in the digital age, UN Doc. No. A/RES/73/179, 17 December 2018, p. 3, available at https://undocs.org/en/A/RES/73/179 (accessed 06/04/2020); see also UN General Assembly resolution 71/199, the right to privacy in the digital age, UN Doc. No. A/RES/71/199, 19 December 2016, p. 3, available at https://undocs.org/en/A/RES/71/199 (accessed 06/04/2020); UN General Assembly resolution 69/166, the right to privacy in the digital age, UN Doc. No. A/RES/69/166, 18 December 2014, p. 2, available at http://undocs.org/en/RES/69/166 (accessed 06/04/2020).

[31] The right to privacy in the digital age, UN Doc. No. A/HRC/39/29, *supra* note 10, §7.

[32] *Id*. §12.

[33] Joseph Ooi, "IMSI Catchers and Mobile Security", School of Engineering and Applied Science, University of Pennsylvania, 29 April 2015, available at https://www.cis.upenn.edu/wp-content/uploads/2019/08/EAS499Honors-IMSICatchersandMobileSecurity-V18F.pdf p.18 (accessed 28/04/2020).

[34] See Privacy International, "Phone Monitoring", 22 February 2018, available at https://privacyinternational.org/explainer/1640/phone-monitoring (accessed 06/04/2020); Jennifer Valentino-DeVries, "How 'Stingray' Devices Work", *Wall St. Journal*, 21 September 2011, available at https://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/ (accessed 06/04/2020).

[35] Witness Statement of Silke Holtmanns, *supra* note 3, §37.

[36] *Ben Faiza v. France*, App. No. 31446/12, ECtHR, judgement, 8 February 2018; see also *Uzun v. Germany*, App. No. 35623/05, ECtHR, Judgment, 2 September 2010.

"*un terminal de télécommunication*" by exploiting the technology embedded within a mobile phone or tablet.[37]

The Article 29 Data Protection Working Party (now replaced by the European Data Protection Board under the EU General Data Protection Regulation) has also explained the privacy risks posed by the tracking of user location through mobile phones.[38] The Working Party has observed that "[t]he technology of smart mobile devices allows for the constant monitoring of location data" and that such "monitoring can be done secretively, without informing the owner".[39] In particular, the Party has emphasised that because "[m]ost people tend to keep their mobile devices very close to themselves, from their pocket or bag to the night table next to their bed", location tracking of a phone can permit "an intimate overview of habits and patterns of the owner of such a device and [the] build[ing] [of] extensive profiles". Moreover, that "pattern may also include special categories of data, if it for examples reveal[s] visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations".[40] The Working Party concluded that the processing of location data can therefore raise a variety of data protection concerns.

2.5. Indiscriminate collection of data

The use of IMSI catchers poses a particularly serious interference with the right to privacy because of the indiscriminate way they can collect IMSI and IMEI data. Surveillance targets and bystanders alike are unlikely to notice[41] or stop[42] their mobile devices from attempting to connect to the fake mobile phone tower. As a result, IMSI catchers enable the tracking of everyone in an area, for instance everyone who attends a political demonstration or a public event like a music festival. IMSI catchers can therefore interfere with the privacy rights of hundreds of people, including those who may not be the intended targets of surveillance.

[37] The Court also found in *Ben Faiza* that the government's collection of the list of cell towers pinged by the applicant's phone in order to track his movements also constituted an interference with the right to privacy.

[38] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN, 16 May 2011, p.7, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (accessed 31/03/20).

[39] *Id*. at p.7.

[40] *Id.*

[41] Unless a user has access to software which detects and warns against IMSI catchers. See for example SnoopSnitch, an IMSI catcher detection app for android devices, further information available at https://opensource.srlabs.de/projects/snoopsnitch/wiki (accessed 28/04/2020).

[42] Because by design, mobile phones seek to connect to mobile phone towers that give the highest signal strength, which is what IMSI catchers are frequently programmed to replicate.

IMSI catchers entice *all* mobile phones within their range to connect to them, therefore forcing *all* of those mobile phones to attempt to transmit their IMSI/IMEI data. Because IMSI catchers can capture the IMSI/IMEI data of *all* mobile phones within their range, they can also capture the location of *each* of those mobile phones. This process – *i.e.* whereby an IMSI catcher captures the IMSI/IMEI data of all phones within their range – can occur regardless of whether the government is using an IMSI catcher to target a particular person or to intentionally conduct indiscriminate surveillance.

IMSI catchers can be hand-held, mounted on police cars or even attached to drones or planes. David Anderson, the former UK Independent Reviewer of Terrorism, in his review of the investigatory powers of British intelligence agencies in 2015, specifically observed that "[r]eports suggest that [IMSI catchers] have been attached to aeroplanes, allowing collection over a wide area".[43] Similarly, it has been reported that U.S. law enforcement authorities have been using IMSI catcher technology attached to small planes since 2007.[44]
Depending on the range of the particular IMSI catcher, the number of individuals whose data is captured in any given operation could be in the hundreds, thousands, or potentially even tens of thousands.

European courts have previously found indiscriminate surveillance to violate the right to privacy. In *S and Marper v. United Kingdom*, the ECtHR held that the collection and retention of DNA and fingerprints of innocent people was contrary to the right to privacy.[45] In *MK v. France*, the ECtHR found a national digital fingerprint database to be unlawful for similar reasons.[46] In particular, the Court noted that "[t]he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention" and that the need for safeguards "is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes."[47]

In *Tele2/Watson*, the CJEU found the "general and indiscriminate retention of all traffic and location data of all subscribers and registered users" to violate the rights to privacy and data protection under the European Charter of Fundamental Rights. In its judgment, the CJEU

[43] David Anderson, Independent Reviewer of Terrorism Legislation, "A Question of Trust: Report of the Investigatory Powers Review", June 2015, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf (accessed 06/04/2020).
[44] Devlin Barrett, "Americans' Cellphones Targeted in Secret U.S. Spy Program", *The Wall Street Journal,* 13 November 2014, available at https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 (accessed 06/04/2020).
[45] S *and Marper v. United Kingdom,* App. Nos. 30562/04 and 30566/04, ECtHR, judgment, 4 December 2008.
[46] *M.K. v. France*, App. No. 19522/09, ECtHR, Judgment, 18 April 2013.
[47] *Id*. §35.

observed that such retention "is comprehensive in that it affects all persons using electronic communication services, even those persons [who] are not even indirectly, in a situation that is liable to give rise to criminal proceedings."[48]

In addition, European courts have identified that the absence of any requirement of reasonable suspicion will render government interferences with privacy unlawful. In *Zakharov v. Russia*, the ECtHR held that a government body authorising surveillance measures "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".[49] Similarly, in *Szabó and Vissy v. Hungary*, the ECtHR noted the requirement of "a sufficient factual basis for the application of secret intelligence gathering measures…on the basis of an individual suspicion regarding the target person" as critical for "the authorising authority to perform an appropriate proportionality test".[50] And in *Tele2/Watson*, the CJEU identified that one of the problematic aspects of indiscriminate retention of all traffic and location data was that it applied "even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences".[51]

3. IMSI catchers and freedom of expression

IMSI catchers primarily infringe on freedom of expression by removing peoples' ability to be otherwise anonymous. Being subjected to surveillance can cause people to alter their behaviour: they may refrain from seeking out different ideas, speaking out on certain issues, or questioning the status quo. This phenomenon is called the 'chilling effect' which is further elaborated in section 3.2. First, however, it is important to establish the relationship between privacy, anonymity and freedom of expression to better understand how the restriction of one can lead to limitations upon the other.

Remember - whole societies benefit from the exchange of ideas and peoples' ability to organise and petition for change, and we all suffer when people are less free to do so.

[48] *Tele2 Sverige*, *supra* note 20, §105; see also *Digital Rights Ireland v. Minister for Communications,* Case C-293/12, Court of Justice of the European Union, Judgment, 8 April 2014 §56-57.
[49] *Zakharov*, *supra* note 14, §260.
[50] *Szabó and Vissy*, *supra* note 16, §71.
[51] *Tele2 Sverige*, *supra* note 20, §105; see also *Digital Rights Ireland*, *supra* note 46, at §58.

3.1. How privacy and anonymity enable freedom of expression

By interfering with privacy in the ways already described, the use of IMSI catchers can also infringe on the freedom of expression. This is because privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other.[52]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has highlighted that: "[t]he right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression" because "States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy".[53] This builds from the idea that "privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively".[54] And so as a result, privacy enables individuals to thrive and develop in a way that does not compromise their autonomy.

While freedom of expression is an important right for everyone, there are particular groups of society that are placed in a more vulnerable position when their anonymity is taken away. IMEI and IMSI data obtained through IMSI catchers allows groups entitled to enhanced protections – including journalists - to be readily identified, which impedes anonymity. This matters because "in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources."[55]

[52] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. No. A/HRC/23/40, 17 April 2013, §79, available at https://undocs.org/A/HRC/23/40 (accessed 06/04/2020) ; see also UN General Assembly resolution 73/179, the right to privacy in the digital age, *supra* note 31, p.3 ("violations or abuses of the right to be free from unlawful or arbitrary interference with the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference").

[53] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. No. A/HRC/23/40, *supra* note 53, § 24, 79; see also UN General Assembly resolution 73/179, the right to privacy in the digital age, *supra* note 31, p.2 ("recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference").

[54] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, UN Doc. No. A/HRC/13/37, 28 December 2009, §33 available at https://undocs.org/A/HRC/13/37 (accessed 06/04/2020).

[55] UN General Assembly resolution 72/175, the safety of journalists and the issue of impunity, UN Doc. No. A/RES/72/175, 19 December 2017, available at https://undocs.org/en/A/RES/72/175 (accessed 07/04/2020).

Hence, the UN General Assembly Resolution on the safety of journalists "[c]alls upon States not to interfere with the use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law".[56]

3.2. How IMSI catchers induce 'chilling effect'

"[S]urveillance technologies have the capacity to chill projects of ethical self-development that are both core to liberty interests and essential to a functioning democracy."[57] The ECtHR has accepted the 'chilling effect' as a form of self-restraint: a chilling effect in the lawful exercise of a right.[58]

This idea has its roots in Foucauldian theory, inspired by a hypothetical panopticon prison. In a panoptic prison, cells were arranged so that each prisoner could be observed by a central watchman, but would never know with certainty whether they were being watched at any given time.[59] It was conceived that such an arrangement of power induces individuals to engage in conformist behaviour, which amounts to a new form of disciplinary control.[60] As such, similarities can be drawn with citizens subjected to newer forms of government surveillance: where practices (such as employing IMSI catchers) that lack foreseeability and transparency are akin to the watchman's ubiquitous gaze.

As explained in section 2.2., IMSI catchers intercept mobile users' communications data. This is significant because the ECtHR has recognised the "potential chilling effect that any perceived interference with the confidentiality of their communications, and particularly their sources, might have on the freedom of the press".[61] Whistle-blowers may be less inclined to co-operate with non-government organisations or the press to hold those in power accountable because of fear of retaliation. In turn, this can have a 'chilling effect' on public debate more broadly due to voices being silenced and stories being unpublished.

The UN Special Rapporteur on freedom of expression has also identified the vulnerable groups whose right to freedom of expression is disproportionately affected by the chilling effect of surveillance:

[56] *Id.*

[57] D. Gray and D. Citron, "The Right to Quantitative Privacy" (2013) 98 Minn L Rev p.69.

[58] B. Van der Sloot, "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities." in Gutwirth S., Leenes R., De Hert P. (eds) Data Protection on the Move. Law, Governance and Technology Series (vol 24. Springer, Dordrecht 2016) p.422.

[59] Jeremy Bentham "The Panopticon Writings" in Miran Bozovic (ed) (London: Verso 1995) p.29-95.

[60] Michel Foucault, Discipline and Punish: The Birth of the Prison (Paris: Gallimard 1975).

[61] *Big Brother Watch*, *supra* note 19, §495.

> "Unnecessary and disproportionate surveillance may undermine security online and access to information and ideas. Surveillance may create a chilling effect on the online expression of ordinary citizens, who may self-censor for fear of being constantly tracked. Surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children."[62]

As can be seen, the idea of the chilling effect has evolved in law since its original conception. However, what remains clear as warned by the UN Special Rapporteur on freedom of expression is that "even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse".[63]

3.3. How IMSI catchers impair the protection of journalistic communications and journalistic sources

IMSI catchers undermine specific, well-established rules regarding the importance of protecting journalistic communications and journalistic sources. Because IMSI catchers enable the tracking and monitoring of journalists' locations; as well as the monitoring and intercepting of journalists' communications (including phone calls and text messages), IMSI catchers can impair the confidentiality and protection of information given to journalists by their sources.

In *Goodwin v. United Kingdom,* the ECtHR stated that source protection for journalists is "one of the basic conditions of press freedom".[64] In *Weber and Saravia v. Germany*, the Court described the protection of journalistic sources as a "cornerstone of the freedom of the press",[65] whereby "without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result, the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be adversely affected".[66]

[62] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. No. A/HRC/32/38, 11 May 2016, §57, available at https://undocs.org/A/HRC/32/38 (accessed 07/04/2020).

[63] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. No. A/HRC/23/40, *supra* note 53, §52.

[64] *Goodwin v. the United Kingdom,* App no 17488/90, ECtHR, judgement, 27 March 1996, § 39.

[65] *Weber and Saravia v. Germany* App no. 54934/00, ECtHR, Decision on Admissibility, 29 June 2006, § 143.

[66] *Id.*

Without being granted the protection afforded by confidentiality, sources may be deterred from assisting the press in informing the public about matters of public interest. This restricts the press' ability to perform its "vital role as a "public watchdog"".[67] Hence, the ability for IMSI catchers to covertly identify the individual sources that a journalist meets, including those who are whistle-blowers by cross referencing IMEI and IMSI data, is a real cause for concern for press freedom, and as a consequence, freedom of expression.

3.4. IMSI catchers undermine a 'favourable environment' for journalists

The ECtHR, in *Dink v. Turkey,* held that "[S]tates are obliged to put in place an effective system of protection for authors and journalists as part of their broader obligation to create a favourable environment for participation in public debate by everyone and to enable the expression of opinions and ideas without fear."[68] This positive obligation for states to create a favourable environment for journalists co-exists with the ECtHR's general rule that when national authorities restrict the fundamental rights of private individuals, they are required "to choose the means that cause the least possible prejudice to the rights in question".[69]

Similarly, and in line with the CJEU *Tele2/Watson* judgement concerning indiscriminate data retention, the Advocate General maintained in his opinion in the ongoing *Privacy International* case[70] that within the fight against terrorism, resolving the issue is not a matter of *practical effectiveness* but of *legal effectiveness* within the framework of the rule of law.[71] Against this background, the indiscriminate way that IMSI catchers can interfere with *all* mobile devices within a given geographical location, including those belonging to protected groups such as journalists, has to be reconciled with the fact that should government officials wish to obtain IMSI/IMEI data from a specific target, authorised officials already have the capacity to do so by retrieving this data directly from mobile phone operators.

[67] A public watchdog in a democracy imparts information or ideas in the public interest. See also *Von Hannover v. Germany No.2* App nos. 40660/08 and 60641/08, ECtHR, judgement, 26 April 2004, § 110.
[68] *Dink v. Turkey*, App no.7124/09, ECtHR, judgement, 14 September 2010, §137.
[69] *Mouvement raëlien Suisse v. Switzerland*, App no. 16354/06, ECtHR, judgement, 13 January 2011, §75.
[70] *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, Case C-623/17, Court of Justice of the European Union, 5 January 2018.
[71] *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, Case C-623/17, Court of Justice of the European Union, Opinion of AG Campos Sánchez-Bordona, 15 January 2020, §39 (Quoting *La Quadrature du Net and Others* Cases C-511/18 and C-512/18, Court of Justice of the European Union, 15 January 2020, Opinion of AG Campos Sánchez-Bordona, §135).

4. IMSI catchers and freedom of assembly and association

IMSI catchers interfere with the right to freedom of assembly and association in many of the ways that we have seen under privacy and freedom of expression.

The resolution adopted by the Human Rights Council on "The Promotion and Protection of Human Rights in the Context of Peaceful Protests", "[r]ecognizes that peaceful protests can make a positive contribution to the development, strengthening and effectiveness of democratic systems and to democratic processes, including elections and referendums."[72] Moreover, the ECtHR, in *Gorzelik and Others v. Poland,* found that "the participation of citizens in the democratic process is to a large extent achieved through belonging to associations in which they may integrate with each other and pursue common objectives collectively."[73]

Given this context, our ongoing scrutiny is not unwarranted. It has already been seen how governments have in some circumstances used IMSI catchers to monitor[74] and intimidate[75] citizens exercising their right to peaceful assembly. Further, if we continually allow governments to escape scrutiny from their obscure use of IMSI catchers, then our enjoyment of these fundamental rights will continue to be threatened.

During protests and demonstrations, individuals often may not wish to be recognised, and in fact may rely on the anonymity of the crowd to protect them against retaliation. However, because the collection of IMSI and IMEI data de-anonymises people (see section 2.3.), individuals may be dissuaded from attending demonstrations if they are under surveillance. This chilling effect

[72] UN Human Rights Council, resolution 38/11, The promotion and protection of human rights in the context of peaceful protests, UN Doc no. A/HRC/RES/38/11, 16 July 2018, *preamble* available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/213/58/PDF/G1821358.pdf?OpenElement (accessed 06/04/2020).

[73] *Gorzelik and Others v. Poland*, App no. 44158/98, ECtHR, judgement, 17 February 2004, § 92.

[74] Fruzsina Eördögh, "Evidence of 'stingray' phone surveillance by police mounts in Chicago", *CS Monitor,* 22 December 2014, available at https://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-stingray-phone-surveillance-by-police-mounts-in-Chicago (accessed 07/04/2020).

[75] For example, in November 2013, Ukrainian protestors demonstrating against the government in Kiev's Maidan Nezalezhnosti and others in the vicinity of the protest received the following text message on their mobile phones: "Dear subscriber, you are registered as a participant in a mass disturbance." The mass delivery of the message suggested the Ukrainian government's use of an IMSI catcher to identify mobile phones and transmit such a message. Tyler Lopez, "How did Ukraine's Government Text Threats to Kiev's EuroMaidan Protesters?," *Slate*, 24 January 2014, available at http://www.slate.com/blogs/future_tense/2014/01/24/ukraine_texting_euromaidan_protesters_kiev_demonstrators_receive_threats.html. (accessed 07/04/2020).

(discussed in section 3.2.) threatens democratic participation as well as dissent, which as a result weakens democracy itself.

4.1. Direct interference with freedom of assembly and association

We explain in section 2.1 how IMSI catchers can be used to monitor and intercept ingoing and outgoing communications.

Beyond that, more advanced IMSI catchers can edit or reroute mobile communications, as well as block service. It has been recognised by the European Court of Human Rights that 'restrictions'[76] on the right to freedom of assembly must be interpreted as measures that take place before, during, or after a meeting.[77]

Therefore, when IMSI catchers block service through a process known as 'ramming', it directly interferes with the right to freedom of assembly and association. This is because mobile users are denied network coverage, which hinders the ability of individuals attending a gathering to communicate with one another or to organise further.[78]

The above example of direct interference will also be an infringement on the rights of journalists, and other human rights watchdogs, since such restrictions hamper these groups' ability to observe protests and to effectively report on them.

4.2. Indiscriminate surveillance of peaceful assembly and association

Section 2.5. addresses in detail how IMSI catchers can permit the indiscriminate monitoring of people's IMSI and IMEI data. Indiscriminate monitoring may interfere with our ability to exercise our freedom to peaceful assembly and association.

By their design, IMSI catchers are uniquely effective tools for conducting surveillance on all individuals within a geographic area, including individuals peacefully assembling or associating with others, because IMSI catchers can indiscriminately collect the IMSI and IMEI data of all mobile phones within their particular range.

[76] Within the meaning of paragraph 2 of Article 11(freedom of assembly and association) ECHR.
[77] *Ezelin v. France*, App no.11800/85, ECtHR, judgement, 26 April 1991, § 38.
[78] See Privacy International, Submission to the Office of the United Nations High Commissioner for Human Rights on the promotion and protection of human rights in the context of peaceful protests, October 2019, available at https://privacyinternational.org/sites/default/files/2019-12/PI%20OHCHR%20peaceful%20protest%20submission%20October%202019.pdf (accessed 07/04/2020).

The capacity to use communication technologies securely and privately is vital to the organisation and conduct of assemblies.[79] However, IMSI catchers' capture of uniquely identifying IMSI and IMEI data also allows the location and tracking of mobile phones and their users. This allows state agencies to readily identify all of the mobile phone users in that particular physical area. Thus, IMSI catchers permit the easy identification and collection of personal data of persons that are congregating for a peaceful purpose and associating with others.

This highlights the potential chilling effect (see section 3.2) inherent in the use of IMSI catchers, because individuals may be deterred from exercising their right to peaceful assembly as guaranteed by Article 21 CCPR and Article 11 ECHR if they are at risk of being surveilled. The indiscriminate nature of the interference means that no person attending a demonstration is guaranteed protection from their data being collected intentionally or otherwise. This fact alone may act as a deterrent in itself.

In the context of surveillance technology which chills the exercise of peaceful assembly and association, it should be reminded that States not only "have a negative obligation to abstain from unduly interfering with the rights of peaceful assembly and of association but also have a positive obligation to facilitate and protect these rights in accordance with international human rights standards."[80] The government use of IMSI catchers is at odds with this state obligation.

Data monitoring in the course of protests also raises particular concerns about the special category of data that is collected. The ECtHR in *Catt v. The United Kingdom "*[c]onsidered it significant that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection".[81] IMSI and IMEI data collected at the site of a demonstration has the potential to reveal personal details pertaining to an individual's political affiliations. Under these circumstances, governments must question whether there is a pressing social need to collect and retain citizens' personal data in a democratic society. The ECtHR further clarified that when the government examines "the question of whether there was a "pressing social need" to collect and retain…personal data", it recalls that the question for it to examine is "**not** whether there was a "pressing social need" for the police to establish and

[79] UN Human Rights Council, Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, Maina Kiai and Christof Heyns , UN Doc no. A/HRC/31/66, 4 February 2016, § 75.

[80] UN Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, UN Doc. No. A/HRC/41/41, 12 July 2019 §13 (quoting UN Doc. No. A/HRC/17/27, § 66; and UN Doc. No. A/HRC/29/25/Add.1.), available at https://undocs.org/A/HRC/41/41 (accessed 07/04/2020).

[81] *Catt v. The United Kingdom,* App no.43514/15, ECtHR, judgement, 24 January 2019, §112.

maintain such a database"[82] for the purpose of prevention of disorder or crime or otherwise, but to collect the special category data in the first place.

To support this finding, the ECtHR also in *Catt* referred to principle 2 on the collection of data in Recommendation R(87)15 to member states regulating the use of personal data in the police sector, which states that "the collection of data on individuals solely on the basis that they belong to particular movements or organisations which are not prescribed by law should be prohibited unless absolutely necessary or for the purposes of a particular inquiry".[83]

4.3. IMSI catchers undermining privacy infringes freedom of association and assembly

Section 2 discussed how IMSI catchers undermine the right to privacy. The main ways those interferences with privacy also infringe on the freedom of assembly and association is by:

- Undermining the security of mobile communications; and
- Collecting sensitive data on individuals exercising their rights to peaceful assembly and association (which can also have a chilling effect).

IMSI catchers are able to monitor and intercept the content of communications as well as communications data.[84] This type of interference, whether it is perceived or actual, undermines the security of communications that are necessary to exercise the right of assembly and of association. The importance of secure communications for peaceful assembly and association has been recognised by the UN General Assembly:

> in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking.[85]

Moreover, the interconnection between interference with the rights to privacy, freedom of expression, and freedom of peaceful assembly was recognised by the ECtHR in *Segerstedt-Wiberg and others v. Sweden*. It held

[82] *Id.* §116 emphasis added.
[83] *Id.* §124.
[84] See sections 2.1 and 2.2.
[85] UN General Assembly resolution 73/179, the right to privacy in the digital age, *supra* note 31.

> that the storage of personal data related to political opinion, affiliations and activities that is deemed unjustified for the purposes of Article 8 § 2 *ipso facto* constitutes an unjustified interference with the rights protected by Articles 10 and 11" which respectively protect the rights to freedom of expression and freedom of peaceful assembly.[86]

Therefore, when IMSI catchers gather data at the site of demonstrations and individuals attending have sensitive data revealed about their political opinion, they are subjected to an unjustified interference which should be prohibited.

The UN Special Rapporteur on the rights to freedom of peaceful assembly and of association challenges the use of surveillance techniques to conduct indiscriminate and untargeted surveillance of people exercising their right to peaceful assembly and association in both physical and digital spaces, and calls for its prohibition. The 2019 report on "The Exercise of the Rights to Freedom of Peaceful Assembly and of Association in the Digital Age" states that:

> Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision.[87]

IMSI catchers are fundamentally invasive tools, incapable of being exercised in a proportionate manner. They therefore have no place in spaces where people join together to exercise their most basic democratic rights.

[86] *Segerstedt-Wiberg and others v Sweden,* App no.7124/09. ECtHR, judgement, 6 June 2006, §107.

[87] Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, UN Doc. No. A/HRC/41/41, *supra* note 81, §57.

5. Conclusion

IMSI catchers, as with other forms of mass surveillance technology, are inherently incapable of being exercised in a manner that is proportionate. Due to the way they operate, IMSI catchers can interfere with a number of fundamental rights - most notably the right to privacy, freedom of expression, and freedom of assembly and association. Their obscure and unfettered use is therefore incompatible with international human rights standards which require that "any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights."[88]

Governments' intrusive and unregulated use of IMSI catchers violates the very essence of the right to privacy, and so should be prohibited. While technologies may be deployed under the guise of protecting democratic society, without adequate regulations and safeguards, those technologies threaten our most fundamental human rights, and thereby undermine democracy itself.

Whilst many governments use IMSI catchers to facilitate their surveillance activities, they are often doing so in secret and without a clear basis in law. Even in circumstances where governments conduct surveillance in connection with legitimate activities, such as gathering evidence in a criminal investigation or intelligence, they may never be able to demonstrate that their use of IMSI catchers is compatible with international human rights law.

There is a troubling lack of public debate surrounding government use of IMSI catchers in the UK and many other countries around the world. Civil society should be included in conversations about intrusive practices that interfere with their human rights on such a large scale. So that interested parties can assess state use of IMSI catchers in light of applicable international human rights law obligations.

[88] The right to privacy in the digital age, UN Doc. No. A/HRC/27/37, *supra* note 22, §23.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org