INTERVENTION SUBMITTED TO THE COLOMBIAN SUPREME COURT BY PRIVACY INTERNATIONAL

INTRODUCTION

1. Privacy International was founded in 1990. It is a UK charity working on the right to privacy at an international level. It focuses, in particular, on tackling the unlawful use of surveillance. It has litigated or intervened in cases implicating the right to privacy in the courts around the world, including those of the Unites States, the United Kingdom, and Europe, such as the European Court of Human Rights and the European Court of Justice.

2. Privacy International's primary aims are to raise awareness about threats to privacy, to monitor and report on surveillance methods and tactics, to work at national and international levels to ensure strong privacy protection, and to seek ways to protect privacy through the use of technology.

3. Privacy International has taken interest in Dejusticia's challenge to Law 1801 of 2016 ("Police Code") given the potential dangers posed to the right to privacy by the Police Code which limits the right to privacy (Articles 32, 139 and 237); imposes data retention powers (Article 95 and Article 237) and expands the use of surveillance cameras (Article 146). This is in the context of a regime that lacks sufficient safeguards.

4. This intervention does not provide an overview of all the international standards that are of relevance to the case before the court. On the contrary, this document focuses on the European and international human rights standards which Privacy International deems most applicable to the key issues in the case and seeks in this intervention to assist the Court by explaining the wider context and by emphasising the seriousness of the privacy interferences.

The scope of the right to private life

5. Article 32 of the Colombian Law 1801 of 2016 ("Police Code") sets out a definition of privacy for the purpose of the Police Code. This definition conditions the right to privacy on a person being located in an area that is exclusive and considered private. It excludes from the definition of private place, and thus from the definition of privacy, public spaces and public places.

6. Article 139 of the Police Code classifies the electromagnetic space as a public space. Thus, when read with Article 32, the electromagnetic spectrum does not fall within the definition of privacy.

7. Article 237 states data from video surveillance in public spaces is public. When read with Article 32 it thus falls outside the definition of privacy.

8. In submissions in advance of the consideration of the periodic report of Colombia, Human Rights Committee, 118th Session, 17 October – 04 November 2016 Privacy International[1] noted that:

> *"Article 32 contains a definition of privacy, which is unduly narrow. By defining the right to privacy as the right of people "to meet their needs and develop their activities in an area that is exclusive and therefore considered private", the provision seems to confuse the right to privacy with the right to unhindered development of personality as well as with the right to the inviolability of the home. Therefore, by linking the right to privacy with the existence of private physical spaces, it excludes from privacy protection any persons or assets (such as cars or electronic devices) placed in public places, including bars, restaurants, etc.*
>
> *Conversely Article 139 defines public space in a very broad way, including notably "the electromagnetic spectrum.*
>
> *The combined result of these definitions is of significant concern to the protection of privacy, particularly when considering that Article 237 states that: "(i) information, images and data of any nature captured and/or stored by video systems or technical means located in public place will be considered public and freely accessible; and (ii)*

[1] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/COL/INT_CCPR_CSS_COL_25208_E.pdf

video systems and technological means, of private or public property, located in the public space, common areas, places open to the public or that being private transcend to the public, will be permanently or temporarily linked to the network that for this purpose will be provided by the National Police." Thus these provisions could even mean that communications travelling through the electromagnetic spectrum would be excluded from privacy protection."

9. The right to privacy is set out in broad terms in:

    a. Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation. Any interference with the right to privacy can only be justified if it is in accordance with the law, has legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human rights.[2]

    b. Article 11 of the American Convention on Human Rights, which states:

    "1. Everyone has the right to have his honor respected and his dignity recognized.

    2. No one may be the object of arbitrary or abusive interference with his private life, his family life, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

    3. Everyone has the right to the protection of the law against such interference or attacks."

10. This right to privacy encompasses the importance of personal dignity and autonomy and the interaction a person has with others, both in private and in public. The right

[2] Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also Report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org.

to privacy is not contingent upon whether a person is in a public or private place – it exists in both and arises in variety of contexts including in the use of the electromagnetic spectrum[3].

11. The Human Rights Committee, in its concluding observations on Colombia[4], expressed concerns that

> *"32…el nuevo Código de Policía, que entrará en vigor en enero de 2017, prevea una definición muy amplia de lo que es espacio público, que incluye el espectro electromagnético, y que toda la información y los datos recolectados en los espacios públicos sean considerados públicos y de libre acceso (art. 17).*
>
> *…*
>
> *d) Velar por que la aplicación de la legislación que regule cuestiones que puedan tener consecuencias en el goce del derecho a la vida privada, en particular la Ley 1621 y el nuevo Código de Policía, sea totalmente conforme con las obligaciones que surgen del Pacto, en particular el artículo 17."*

12. Privacy International shares the concerns of the Human Rights Committee that the Police Codes overly narrow definition of privacy is not consistent with the international understanding of that right. In submissions in advance of the

[3] Privacy International raised the reference to 'monitoring the electromagnetic spectrum' in submission to the Human Rights Committee 116th Session, March 2016. https://www.privacyinternational.org/sites/default/files/HRC_colombia.pdf §2

Monitoring of electromagnetic spectrum constitutes an interference with the privacy of communications. It was noted in those submissions that 'Monitoring' the electromagnetic spectrum is not defined in the law (nor in the Colombian constitution).

Further, monitoring the electromagnetic spectrum could include filtering, analysing and monitoring emails, text messages and phone calls that carried upon the electromagnetic spectrum. Those acts constitute 'interception' of the communication and thereby interfere with the privacy of the person sending and receiving the information. 'Monitoring' the electromagnetic spectrum, thus, intrinsically involves an interference with the right to privacy.

Even if one contends that the means of 'monitoring' the electromagnetic spectrum without violating the privacy of communications exist, they pertain to an extremely narrow set of activities such as heat detection tools and direction-finding tools and antenna. All other forms of 'monitoring' the electro magnetic spectrum necessitate an interference with communication of a type that means that it is not possible to conclude anything other than that the monitoring has resulted in the communication being intercepted.

[4] http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/COL/CO/7&Lang=en

consideration of the periodic report of Colombia, Human Rights Committee, 118th Session, 17 October – 04 November 2016 Privacy International[5] noted that it was

> *"concerned over the practices of surveillance by Colombian intelligence and law enforcement agencies. National legislation governing surveillance is inadequate, unclear as to the powers, scope and capacity of state surveillance activities and thus it falls short of the required human rights standards to safeguard individuals from unlawful interference to the right to privacy."*

13. The submission further raised concern about the scope of surveillance under the Intelligence Law (Law no 1621 of 2013) in which intelligence and counter intelligence activities are regulated, including "monitoring the electromagnetic spectrum" which is a feature of the Police Code.

> *"The organisations reiterate their concerns about the scope of surveillance under the Intelligence Law (Law No 1621 of 2013) in which intelligence and counter intelligence activities are regulated, including "monitoring the electromagnetic specturm".*
>
> *The written replies of the Colombian government on this point (paragraphs 95 – 96) merely describe the scope of the law and the judgment of the Constitutional Court, without addressing the scope of monitoring, or providing any definition of what monitoring of the electromagnetic specturm consists of.*
>
> *To summarise the concerns of the organisations:*
>
> - *The purposes under which information can be obtained (Article 4) are over-broad, namely ensuring national security, sovereignty, territorial integrity, the security and defence of the nation, the protection of democratic institutions and the rights of Colombian residents and citizens and the protection of natural resources and economic interests of the nation;*[6]
>
> - *'Monitoring' the electromagnetic spectrum is not defined in the law (nor in the Colombian constitution). Without any definition provided, 'monitoring' the*

[5] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/COL/INT_CCPR_CSS_COL_25208_E.pdf

[6] UN Doc. CCPR/C/COL/Q/7, 26 April 2016.

electromagnetic spectrum could include filtering, analysing and monitoring e-mails, text messages and phone calls that are carried upon the electromagnetic spectrum. Those acts constitute 'interception' of the communication and thereby interfere with the privacy of the person sending and receiving the information;[7]

- *In fact the government accepts (in paragraph 95) that this 'monitoring' may include information that is not needed for the purposes of intelligence, but it fails to recognise that as a result, such 'monitoring' constitutes an interference with the individual's privacy that should be subject to the same strict test of legality, necessity and proportionality;*

- *The 2013 Intelligence Law only requires directors of the relevant security agencies to authorise the 'monitoring' of the electromagnetic spectrum."*

14. The European Court of Human Rights ("ECtHR") has developed significant jurisprudence on the scope of the right to privacy under Article 8 of the European Convention on Human Rights, whose wording is similar to Article 11 of the Inter American Convention. This jurisprudence is particularly relveant to this case because it demonstrates the right to privacy can be engaged even in public places.

15. Article 8 of the European Convention on Human Rights ("ECHR") provides:

> *"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

[7] Privacy International, 'Shadow State: Surveillance, Law and Order in Colombia', September 2015, p. 33, available at: https://privacyinternational.org/node/635.

16. The ECtHR, in applying Article 8 of the ECHR in the case of *Von Hannover v Germany* (Application no. 59320/00) 24 June 2004, which related to photos of the applicant taken exclusively in public places,[8] ruled:

> *"50. The Court reiterates that the concept of private life extends to aspects relating to personal identity, such as a person's name, or a person's picture.*
>
> *Furthermore, private life, in the Court's view, includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is therefore a zone of interaction of a person with others, even in the public context, which may fall within the scope of "private life".*
>
> *51. The Court has also indicated that, in certain circumstances, a person has a "legitimate expectation" of protection and respect for his or her private life. Accordingly, it has held in a case concerning the interception of telephone calls on business premises that the applicant "would have had a reasonable expectation of privacy for such calls"* (see *Halford v. The United Kingdom*, judgment on 25 June 1997).

17. Similarly, in *P.G. and J.H. v The United Kingdom* (Application no.44787/98) 25 September 2001, the ECtHR stated:

> *"56. Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. Article 8 also protects a right to identity and personal development and the right to establish and develop relationships with other human beings and the outside world. It may include activities of a professional or business nature. There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".*
>
> *57. There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. …*

[8] §19

18. The decision further notes that:

> "*Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. "*

19. The rapidly developing dimensions of data created by new technology permits the large-scale recording of individuals in public places in a way that represents a highly intrusive infringement with personal privacy. Techniques used include the use of facial recognition technology; body worn video; automated number plate recognition technology; social media monitoring; and use of unmanned aerial vehicles (a.k.a. drones). Data gathered can reveal location, individual opinions as well as information about a person's preferences, sexuality and health status.

20. The concerns raised by such public monitoring have been articulated in the Supreme Courts of the United States and the United Kingdom. In *United States v Jones*, 132 S Ct 945 (2012), a United States Supreme Court case considering monitoring of largely public movements by GPS technology Justice Sotomayor explained in her concluding opinion, at 956:

> "*Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."*

21. The issues were encapsulated by Lord Toulson of the Supreme Court of the United Kingdom in his dissenting judgment in *R (Catt) v Commissioner of Police of the Metropolis & Anor* [2015] UKSC 9, at §69:

> "*One might question why it really matters, if there is no risk of the police making inappropriate disclosure of the information to others. It matters because in modern society the state has very extensive powers of keeping records on its citizens. If a citizen's activities are lawful, they should be free from the state keeping a record of them unless, and then only for as long as, such a record really needs to be kept in the public interest.*"

The collection, retention and access to personal data

22. Article 95 of the Colombian Police Code establishes the obligation to register the International Mobile Equipment Identity (IMEI) number, a number that uniquely identifies a mobile phone[9], together with name, surname, address and contact telephone number.

23. The Court of Justice of the European Union ("CJEU"), in Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, held the collection, retention and use of metadata/communications data is an interference with the right to privacy. Such data constitutes personal data and its mandated retention and collection by the authorities raises significant concerns given that this personal data can be used to build profiles of individuals leading to further invasion of their privacy. The retention of IMEI data such as that required under Article 95 can be a crucial component of building such a profile.

24. In submissions in advance of the consideration of the periodic report of Colombia, Human Rights Committee, 118th Session, 17 October – 04 November 2016, Privacy International[10] on the issues of subscriber data noted:

> *"For criminal investigations, Decree 1704 (2012) provides that subscriber's information[11] and geo-localization[12] data must be kept for five years."*
>
> …
>
> *"Further, the Ministry of ICT has implemented a strategy to counter cellphone theft which involves the creation of a database that associates IMEI numbers with SIM cards and personal information such as ID number, name and address. The carriers*

[9] As noted in C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014 §16 '(d) data necessary to identify users' communication equipment or what purports to be their equipment' includes '(2) (iii) the International Mobile Equipment Identity (IMEI) of the calling party … (v) the IMEI of the called party'

[10] http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/COL/INT_CCPR_CSS_COL_25208_E.pdf

[11] Article 4 of Decree 1704 of 2012.

[12] Article 5 of Decree 1704 of 2012.

must check the user ID against several sources such as the National Archive of Identification, Civil Registry or financial databases.

Administrative, police and judicial authorities can access this information but there is not any provision on the reasons these authorities must provide to access the database or any oversight to the access which lays the ground for abuses of such a system and increases the risk of privacy violations."

25. In addition to the CJEU, a number of international bodies have expressed serious concern regarding such blanket retention of data. For instance, according to the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015):

> *"55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information."*

26. The UN Human Rights Committee has observed, in its Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016):

> *"42. [The Committee] is also concerned about the wide scope of the data retention regime under the [2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act]...*
>
> *43. The State Party should... consider revoking or limiting the requirement for mandatory retention of data by third parties..."*

27. The United Nations High Commissioner for Human Rights has said, in a Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014):

> *"26. Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on*

private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.

28. The CJEU also recently returned to the question of data retention in the joined cases of C-203/15 and C-696/15 *Tele2 Sverige and Watson* ECLI:EU:C:2016:970 ('***Watson***'). The Court held:

> *"1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*
>
> *2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."*

29. In considering the privacy invasive nature of subscriber data, the judgment highlighted that when combined with other data obtained by the authorities, it can help build a full profile of an individual, thereby significantly interfering with someone's privacy. Once obtained, subscribers' data can be used to tie individuals to

particular conversations, locations and times – all the government needs to do is to correlate an individual's name with a phone and then with other communications data already collected by the authorities:

> *"98. The data which providers of electronic communications services must therefore retain 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. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period.*
>
> *99. That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, 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. In particular, that data 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."*

30. In its judgment, the CJEU gave clear and unequivocal guidance as to data retention:

    a. Retention of data is only proper for the purposes of preventing and detecting serious crime (including terrorism), given the seriousness of the interference with privacy involved in data retention (§115, 119).

    b. General and indiscriminate retention of traffic and location data of subscribers and registered users is precluded (§112).

    c. Access to retained data can only be granted in relation to fighting crime, only to the data of indivduals suspected of planning, committing or having committed serious crime or being implicated in one way or another in such crime (§119).

d. There must be prior review of a request for access by a court or other independent authority, following a reasoned request, save in cases of urgency (§120).

e. There must be provisions for notification to persons whose data have been obtained, to enable their rights to be vindicated by complaint or legal proceedings, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities (§121).

31. Privacy International is concerned that Article 95 fails to meet these requirements.

CONCLUSION

32. Given the right to privacy is engaged when police and other authorities collect personal data and/or conduct surveillance in public places, the safeguards related to the limitations of privacy must apply. The International and European frameworks referenced herein provide an indication of the standards that must be met.

33. In this regard, Privacy International considers that Article 32, Article 95 (clause 8), aspects of Article 139, Article 146 (paragraph 2), and Article 237 (paragraphs 1 and 2) are potentially incompatible with the above internationally recognised human rights principles.