





OHCHR consultation in connection with General Assembly Resolution 68/167 "The right to privacy in the digital age"

Submitted by:

Privacy International

Access

Electronic Frontier Foundation

Article 19

Association for Progressive Communications

Human Rights Watch

World Wide Web Foundation

1 April 2014

Executive Summary

This submission is made by Privacy International, Access, the Electronic Frontier Foundation, along with Article 19, the Association for Progressive Communications, Human Rights Watch and the World Wide Web Foundation.

Submissions and recommendations cover five main themes: the meaning of interferences with the right to privacy in the context of communications surveillance, the out-dated distinction between communications data and content, the conceptualisation of mass surveillance as inherently disproportionate, the extra-territorial application of the right to privacy, and the need for legal frameworks to provide protections for the right to privacy without discriminating on the basis of nationality.

We make the following recommendations to OHCHR:

1. **The High Commissioner should explicitly recognise that any act of interception, collection, control, acquisition, or taking custody of communications amounts to an interference with the right to privacy that must be justified in accordance with the well-established requirements of international human rights law.**
2. **The High Commissioner should reiterate that collection of or access to communications data, to the extent it can even be considered separately from the content of communications, represents an equally serious interference with the right to privacy as interception of communications content.**
3. **The High Commissioner should emphasise that mass surveillance (or "bulk collection") is an inherently disproportionate interference with human rights.**
4. **The High Commissioner should reiterate that States owe human rights obligations to *all* individuals subject to their jurisdiction, at a minimum are required to respect the right to privacy of all persons whose communications they handle, and also have positive obligations to ensure and protect the individual's privacy when the act of conducting surveillance renders individuals within their effective control.**
5. **The High Commissioner should emphasise that the right to privacy is a universal right whose enjoyment does not depend on nationality or location, and caution against legal frameworks that purport to discriminate between nationals and non-nationals with respect to the privacy protections afforded.**

Introduction

6. This is a submission on behalf of Privacy International, Access, the Electronic Frontier Foundation, along with Article 19, the Association for Progressive Communications, Human Rights Watch and the World Wide Web Foundation, in our capacity as, respectively, the instigators of, and signatories to, the International Principles on the Application of Human Rights to Communications Surveillance ("the 13 Principles"). This submission responds to the call of the Office of the High Commissioner for Human Rights ("OHCHR") regarding the right to privacy in the digital age.

7. As a starting point, we wish to state in the strongest terms that very few measures are being taken at national levels to ensure respect for and protection of the right to privacy in the context of digital communications. Quite the opposite and, contrary to international law, measures are being taken to violate the right to privacy with increasing frequency. The national legal frameworks of many States fail to comply with international law and are inadequate to address these new forms of human rights violations. The result is gross and mass violations of the right to privacy by States, both individually and acting in concert with others.

8. In addition, very few States are being transparent about specific measures to ensure that procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, are compliant with international human rights law. States have shown continued reticence to disclose the nature and extent of the surveillance being conducted; most information in the public domain about the reach of State surveillance is due to the actions of human rights defenders, particularly whistleblowers, who have taken action to reveal human rights violations, often placing themselves at risk of persecution, including detention, as a result.

9. We submit for your consideration the 13 Principles[1] and call on you to use them as a guiding framework for your analysis of the right to privacy in the digital age. More than 400 organisations and 300,000 individuals have signed the 13 Principles. In addition, the Principles have also been endorsed by parliamentarians and political parties.[2]

10. In addition to presenting the 13 Principles, we wish to emphasise the following five issues addressed within them that we believe are central to the protection of the right to privacy in the digital age, and which we urge the OHCHR to address directly in its report:

    a. The recognition that interferences with the right to privacy in the context of communications surveillance occur at the point of collection, control or custody, not only at the point of access or viewing by a State agent.
    b. The reiteration that collection of or access to communications data (or metadata), to the extent it can even be considered separately from the content of communications,

[1] https://en.necessaryandproportionate.org/text

[2] Including the United Kingdom's Liberal Democrat Party (http://d3n8a8pro7vhmx.cloudfront.net/libdems/pages/4138/attachments/original/1392201564/Agenda___Directory__Spring_2014.pdf?1392201564 at pg. 64); other signatories by elected officials are available here: https://necessaryandproportionate.org/text#elected_officials_political_parties.

represents an equally serious interference with the right to privacy as interception of communications content.

c. The conceptualisation of mass surveillance (or "bulk collection") as an inherently disproportionate interference with human rights.
d. The application of extra-territorial human rights obligations in the context of communications surveillance.
e. An understanding of the right to privacy as a universal right, and of the need for legal frameworks that protect privacy without discriminating on the basis of nationality.

11. In addition to the issues articulated below, we wish to declare our support for further action to be taken by the Human Rights Council in order to affirm the centrality of the right to privacy and better guarantee its protection and promotion in the digital age, including the following:

    a. The establishment of a regionally-representative Commission of Inquiry to undertake a survey of laws, regulations and State practice with respect to intelligence practices and their compliance with international human rights law;
    b. The establishment of a dedicated special procedures mandate to the right to privacy in the digital age; and
    c. The issuance by the Human Rights Committee of a new General Comment on the right to privacy, to replace General Comment 16 (1988).

I- Collection of communications as a interference with the right to privacy

12. One of the most concerning debates that has emerged from various whistleblower revelations about global surveillance practices (such as those by Edward Snowden) has surrounded the mass interception of communications by intelligence services. Governments have been quick to attempt to colour the discourse around mass surveillance by rebranding their actions as "bulk collection"[3] of communications, asserting that such collection in itself is a benign measure that does not offend privacy rights. Rather than capacities to conduct mass interception, for example, the British Chair of the Intelligence and Security Committee, Sir Malcolm Rifkind, refers to "capacity… to take bulk data and process it by computers";[4] instead of the interception of emails on a global scale, US President Barack Obama similarly describes mass surveillance as "our bulk collection of signals intelligence."[5] Government attempts to substitute "bulk collection" for "mass surveillance" are aimed at suggesting that collection of communications in itself is not a violation of the right to privacy.[6] Collection, they argue, is conducted by a computer and thus does not endanger privacy rights; rather, they contend, the interference with the right only occurs when the communication is accessed and analysed by a duly authorised official or is otherwise selected

[3] http://www.pclob.gov/Library/Meetings%26Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Panel_I_Transcript.pdf, p 10.
[4] http://www.dw.de/rifkind-intelligence-depends-on-trust/a-17402345
[5] http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html
[6] For further on how language is being used to mislead, see Jameel Jaffer and Brett Max Kaufman, "How to Decode the True Meaning of What NSA Officials Say," *Slate*, 31 July 2013, available at http://www.slate.com/articles/news_and_politics/politics/2013/07/nsa_lexicon_how_james_clapper_and_other_u_s_officials_mislead_the_american.html

for further scrutiny after collection. In advancing this argument, these governments are seeking to justify their ever-expanding capacity to collect *all* communications globally by attempting to shift the relevant legal enquiry to a point after collection or monitoring.

13. It is essential that the OHCHR's report makes a strong statement that any articulation of the right to privacy in the digital age must acknowledge that any measure to collect, control or take custody of communications amounts to an interception, thus constituting an interference with privacy that must be justified in accordance with international human rights law.

Interception of communications as an interference with the right to privacy

14. Although little treaty-body jurisprudence exists to articulate the contours of the right to privacy in the context of communications surveillance, General Comment No. 16 firmly establishes that the interception of telephonic, telegraphic and other forms of communications amounts to an interference with the right to privacy, quite apart from the question of when or whether the communication is read or used by the State:

> "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."[7]

15. While the General Comment 16 was published before the public adoption of the internet and thus does not refer to digital communications, it can be fairly assumed that were the General Comment to be updated, digital communications would be added to the types of communications that should not be intercepted. The European Court of Human Rights ("ECtHR") has explicitly stated that e-mail communications, in addition to written, telephone and facsimile correspondence, are covered by the notions of "private life" and "correspondence" with the meaning of Article 8 of the European Convention on Human Rights.[8]

16. The ECtHR has a considerable body of jurisprudence establishing that interception of communications constitutes an interference with the right to privacy enshrined in Article 8.[9] Moreover, the Court has said that the mere existence of legislation permitting the interception of communications constitutes such an interference, as it first explained in *Klass v Germany* (1978):

> "Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, **in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services** and thereby

[7] CCPR General Comment No. 16: Article 17 (Right to Privacy), para. 8.
[8] Liberty & Ors v United Kingdom (2008) Application 58243/00, para. 56.
[9] See Malone v United Kingdom (1985) 7 EHRR 14 [64]; Weber v Germany (2008) 46 EHRR SE5 at [77]; and Kennedy v United Kingdom (2011) 52 EHRR 4 at [118]).

constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence."[10]

17. Importantly, the Court has also found that the interception and/or storage of a communication constitutes the interference, and that the subsequent use of the stored information has no bearing on that finding.[11] In *Amman v Switzerland* (2000) the ECtHR followed its judgment in *Leander v Sweden* (1987) that "[b]oth the storing and the release of [secret police-register information], which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life…".[12]

18. Equally, the Court has found that it does not matter whether the information gathered on an individual was sensitive nor whether the applicant had been inconvenienced in any way.[13] In *Amman* the Swiss government submitted that the establishment of a database of surveillance-derived information was not an interference with the right to privacy because it "contained no sensitive information about the applicant's private life".[14] The Court held:

> "[i]t is sufficient for it to find that data relating to the private life of an individual were stored by a public authority to conclude that… the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8, with the applicant's right to respect for his private life."[15]

19. In *Liberty and Others v United Kingdom* the ECtHR reiterated that the mere existence of powers "permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants".[16]

The legal meaning of interception

20. In its jurisprudence the ECtHR uses the term interception to refer to either targeted or mass surveillance of communications, from the recording or bugging of an individual's telephone communications and interference with postal mail,[17] to the mass monitoring or recording of public telecommunications, including telephone, facsimile and email communications.[18] In the vast majority of interception-related cases before the Court, the government parties have not disputed that the relevant activities constituted a form of interception of communications. As a result, the Court has not looked in depth at the technical mechanism of how interception is effected nor explicitly delineated what constitutes an interception. It has simply stated that any interception of communications will amount to an interference with Article 8.

---

[10] Klass v Germany (1978) application 5029/71, para 41 [emphasis added].
[11] Amann v Switzerland (2000) application 27798/95 para 69
[12] Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48
[13] Amann v Switzerland (2000) application 27798/95 para 70
[14] Amann v Switzerland (2000) application 27798/95 para 68
[15] Amann v Switzerland (2000) application 27798/95 para 70
[16] Liberty & Ors v United Kingdom (2008) Application 58243/00, para. 57.
[17] Malone v United Kingdom (1985) 7 EHRR 14
[18] Liberty & Ors v United Kingdom (2008) Application 58243/00

21. The term interception in the context of communications surveillance has long been understood to encompass as any act which involves the collection, control, acquisition, or taking custody of communications in the course of their transmission or while in storage. We submit that, as the technological mechanisms by which those acts are effected change, the term interception should continue to hold the same meaning. That is, any technology that enables a State to collect, control, acquire or take custody of communications is by its nature intercepting the communication. We explore the technical meaning of interception further below (at para 33).

22. Most national legislative frameworks regulating communications surveillance embrace such a definition of interception. While we do not purport to approve of these frameworks, an analysis of them provides a useful example of what is considered interception under domestic legal regimes, and highlights that recent moves to narrow the definition of interception to cover only access or analysis by a state agent are not in compliance with legal understandings of the term.

United Kingdom

23. In the United Kingdom, section 2 of the *Regulation of Investigatory Powers Act 2000* describes the meaning of 'interception' as follows:

> *(2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he—*
>
> *(a) so modifies or interferes with the system, or its operation,*
>
> *(b) so monitors transmissions made by means of the system, or*
>
> *(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,*
>
> *as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.*
> *[…]*
> *(7) For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.*
> *(8) For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.*

24. The key elements are thus as follows:

    a. During the time at which a communication is **being transmitted** by means of a telecommunications system (**including times when it is stored** in a manner that enables the intended recipient to collect or access it)
    b. A person **intercepts the communication**

c. To **make some or all of the content of the communication available** to a person other than the sender or intended recipient, **including by diverting or recording** the contents so as to make them subsequently available
d. And in doing so either modifies or interferes with the system or its operation, monitors transmissions made by means of the systems, or monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system.

It is clear that it is not only the diversion of communications that constitutes their interception, but any measures to monitor, record or collect them. Equally, the act of interception does not depend on contemporaneous access or analysis, but rather includes the recording of communications for later access or analysis. This is borne out by a later provision of the legislation that provides for separate threshold to enable "intercepted material" to be "*read, looked at or listened to by the persons to whom it becomes available*" (section 16(1)). This provision adds further weight to the contention that material collected via an action of interception should be considered "intercepted material" whether or not it has been viewed, accessed or analysed.

25. Accordingly, acts that constitute interception – and thus interfere with the right to privacy – will include any measure to divert, record, collect, monitor or store communications during the course of their transmission, and will span a broad spectrum from targeted to massive or indiscriminate interception. Some examples of the types of interference with communications that would thus constitute interception in accordance with the British definition are:

    a. The placing of a tap on a **telephone cable** servicing an individual residence and the recording of all phone calls coming in and out of the residence for analysis by a law enforcement officer;
    b. The diversion of all **postal mail** being sent to a certain address or set of addresses;
    c. The recording of all digital transmissions being sent to and from a certain **IP address** or set of IP addresses;
    d. The monitoring of all digital transmissions sent to and from a particular **mobile phone number** or set of mobile phone numbers; or
    e. The collection of all digital transmissions that pass through a **certain cable, cell tower, or cable landing station**.

United States

26. Under the law of the United States, 'intercept' is defined in 18 U.S.C. § 2510 ("the Wiretap Act") to mean *"the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."*

27. The jurisprudence of US courts has established that communications are 'intercepted' only if acquired contemporaneously with transmission.[19] In contrast to the United Kingdom, US law affords different and separate protections to stored communications in 18 U.S.C. Chapter 121 ("the Stored Communications Act").

[19]See *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 (D.N.J. 2001) (holding a key logger device on a personal computer will not intercept communications if it is configured such that keystrokes are not recorded when the computer's modem is in use).

28. However, under US law interception does not necessitate contemporaneous access, analysis or listening.[20] Rather, an interception occurs at the time that the contents of a communication are "captured or redirected in any way".[21] **Even when the communications are never accessed, analysed or listened to, an interception – and interference with privacy – will still have occurred.[22]** In addition, the act of interception can occur in multiple places: in the instance of a tapped phone, for example, the interception occurs where the tapped phone and second phone in the communication are located, and where the law enforcement officers first overheard the call.[23]

Other jurisdictions

29. The South African *Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002* adopts similar wording to the US Wiretap Act, providing in section 1 that:

> *"intercept" means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication and includes the—*
>
> *(a) monitoring of any such communication by means of a monitoring device;*
>
> *(b) viewing, examination or inspection of the contents of any indirect communication;*
>
> *(c) diversion of any indirect communication from its intended destination to any other destination,*
>
> *and "interception" has a corresponding meaning.*

30. In Australia, interception is defined in the *Telecommunications (Interception and Access) Act 1979,* which stipulates at section 6(1)

> *Interception "consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication".*

The meaning of the term "passing over a telecommunications system" was amended by the *Telecommunications (Interception) Amendment Act 2006* to clarify whether a particular communication is passing over, or is a stored communication:

> *5F (1) For the purposes of this Act, a communication:*
>
> *(a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and*
>
> *(b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.*

---

[20] *In re State Police Litigation,* 888 F.Supp. 1235 (D.Conn. 1995)

[21] *U.S. v. Rodriguez,* 968 F.2d 130 (2d Cir. 1992)

[22] *George v. Carusone,* 849 F. Supp. 159, 163 (D. Conn. 1994).

[23] United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992); United States v. Denman, 100 F.3d 399, 403 (5th Cir. 1996)"

31. In South Africa and Australia, it is clear that interception includes collection and recording for subsequent analysis and access, in addition to contemporaneous listening and analysis.

The technical act of "interception"

32. Drawing on the definitions contained in domestic legislation, as well of the jurisprudence of the European Court, it is clear that "interception" in the context of surveillance is broader than its ordinary meaning; it is not restricted to the cutting off of communications, but rather includes all acts of monitoring, copying, diverting, duplicating and storing communications in the course of their transmission. In the context of surveillance, a communication can still reach its destination even if it is intercepted in the course of its transmission.

33. From a legal viewpoint, collection and recording of communications amounts to interception of communications. This is equally true from a technical viewpoint. Any measures to copy, divert, record, duplicate, acquire, collect or store all or part of a communication necessitate a technical act that touches upon communication in the course of its transmission. In technical terms it makes no difference whether the communication is read, looked at or listened to by a human; the interception is effected at the moment at which a communication is engaged with sufficiently to enable its collection and retention for analysis, either contemporaneously or subsequently.

34. Traditionally, telephony required a dedicated physical link (circuit) to be set up between two callers in order to enable them to communicate, and the role of the telephone system was to set up that unique circuit for the call via a series of switches. Traditional forms of interception involved placing a tap on that physical link to intercept – collect and record, but not prohibit from reaching their destination – the communications between the two callers. However, a large majority of the world's internet, as well as mobile and fixed telephony, communications are now conducted via internet protocol (IP). With IP-based communications, a large number of simultaneous communications travel through links, with each individual communication being split into small chunks, or packets. Each of these packets will contain different parts of the message, as well as information identifying the originator and intended recipient. A single communication, once split up into different packets, may traverse entirely separate links. These packets are comprised of different layers, and can contain different information at different layers within the packet; so, in the case of a Facebook message, the information about which individuals the message is between is buried deep within the packet.

35. The internet provides a superhighway for all of these packets to travel to and from their destination. Packets will choose the fastest and cheapest route to their destination, but not necessarily the most direct route. Each of the packets travelling across the global communications infrastructure will be related to different types of communications and represent different kinds of interactions amongst different kinds of entities. For example, one packet found on the internet might be a voice call directly between users, while another is part of a large, ongoing conversation between two large e-mail service providers in which hundreds of different e-mails between different pairs of users are gradually being delivered; meanwhile, another is part of a web browsing session in which a user is downloading a large image from a popular web site. All of these are "IP packets", and there are still many other kinds besides these.

36. At its most basic level, interception of IP-based communications could involve the handling, duplication or storage (for either a brief or long period of time) of every packet that flows through a certain link. At the point of interception, the packet is opened and an inspection of some layers or every layer within the packet takes place, in order to analyse whether the packet contains something of interest. Each packet can then be duplicated, categorised, logged, copied and stored. The process is conducted instantaneously such that the packets are not necessarily delayed in their transmission, nor are they prevented from reaching their destination.

37. This process clearly amounts to an interference with the communication. If we take the analogy of traditional interception of postal mail, interception of IP-based communications is akin to an inspection and recording of both the address of every single piece of mail that passes through a certain post office, as well as the opening, inspection and potentially duplication of the contents of that piece of mail, prior to the forwarding on of the mail to its intended destination. **Just like with postal interception, the interception of digital communications is effected at the moment at which a communication is engaged with sufficiently to enable its collection and retention for analysis, either contemporaneously or subsequently.**

II- Access to communications data as an interference with the right to privacy

38. Advancements in modern technologies, expanding internet access, the spread of mobile and digital devices, the declining costs of data storage, increased cross-border transfer of data, and the digitisation of public and private services have drastically altered the landscape of privacy and data protection. The amount of data that exists in the digital realm today is around ten times that which existed less than a decade ago.[24] The speed and frequency with which it is emitted and transmitted grows dramatically each year. The types of data available and accessible have also expanded, particularly as the open data paradigm gains influence. Importantly the means and modalities of analysing data have advanced to a level that has facilitated access to and scrutiny of previously incoherent, disparate or meaningless types and amounts of data to produce incredibly revelatory analyses.

39. The way we communicate and use modes of communication has also changed considerably. While recognising that access to the internet remains a serious issue for a large portion of the world, for a great number of us the major portions of our lives are lived, to a large extent, online. We use the internet to talk, learn, shop, find employment, read books, watch movies, conduct financial transactions, organise travel, keep records, conduct research, impart ideas, diagnose health conditions, and learn and express our political views. Our mobile and digital devices are ubiquitous extensions of our personal and professional lives, seamlessly integrated into every aspect of our personal behaviours and relationships. They enable us to collect and catalogue a disparate range of media, information and tools. They have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, correspondence files, fixed-line telephones, and personal computers. Increasingly, they are also replacing our formal identification documents, our bank and credit cards.

[24] Helbing, Dirk, and Stefano Balietti. "From Social Data Mining to Forecasting Socio-Economic Crises." *Arxiv* (2011) 1-66. 26 Jul 2011 http://arxiv.org/pdf/1012.0178v5.pdf.

40. Use of the internet via mobile and digital devices enables the creation of additional personal data about communications, known as communications data or metadata. This type of data can include personal information about individuals, their locations, travels and online activities, and logs and related information *about* the e-mails and messages they send or receive, even apart from the content of those messages themselves. Communications data are storable, accessible and searchable, and access to and analysis of the data can be hugely revelatory and, as described further below, highly invasive. The historical distinction between data about an individual's communications and the content of his or her communications has become insignificant.

41. Put together, such personal and communications data can reveal an individual's identity, relationships, location and activity, as well as a vast array of diverse information about their web browsing activities, medical conditions, political and religious viewpoints and/or affiliation, interactions and interests. Access to and analysis of such data allows deep, intrusive and comprehensive view into a person's private life. Even seemingly innocuous transactional records, when analysed and matched with other personal data, can be extremely revelatory.[25]

42. Given the value of personal and communications data, particularly when multiple such datasets are combined and analysed, States are increasingly looking to access and analyse such data as a means of surveillance. The Snowden revelations have illustrated the extent of State access to communications data held by phone and internet companies. Intelligence and law enforcement authorities are also increasingly accessing other sources of communications data through means such as, for example, searching and monitoring publicly available information through social media sites like Facebook and Twitter, and infiltrating groups and tracking members of those sites, as well as data collected in physical spaces, such as mass license plates collections. Other forms of personal data are also being collected and retained by the State, including, most notably, the DNA and biometric data of suspects, arrestees, witnesses, victims and convicted persons. Personal data that are publicly available are also a common source of information for intelligence and law enforcement authorities. Such data might include, for example, newspaper articles, blogs, radio programmes or decisions by public authorities.

The nature of the interference with the right to privacy

Personal data, including publicly available data

43. There is well-established case law in the ECtHR that speaks to the principle that systematic State collection of personal data, even when publicly available, amounts to an interference with Article 8. *Segerstedt-Wiberg v Sweden*[26] concerned the collection and retention of information on the political activities of the applicants by the security police. The Court considered that, even though much of the information was publicly available, because it had been systematically collected and

[25] Jonathan Mayer & Patrick Mutchler, MetaPhone: Jonathan Mayer & Patrick Mutchler, MetaPhone: The Sensitivity of Telephone Metadata (Mar. 12, 2013), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata; Declaration of Edward W. Felten, *ACLU v. Clapper*, No. 13-cv-03994 (WHP) (SDNY Aug. 23, 2013), ECF No. 27, available at: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.

[26] (2007) 44 EHHR 2

stored in police files the applicants' Article 8 right had been interfered with.[27] The Court built on its decision in *Rotaru v. Romania* (2000),[28] in which it stated that:

> "[p]ublic information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention."[29]

44. In *S and Marper v United Kingdom* (2009) this Court expanded on this principle and provided a summary of the operation of Article 8 in the context of the acquisition and processing of personal data. The Court opined as follows:

> "The Court recalls that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8. Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family. Information about the person's health is an important element of private life. The Court furthermore considers that an individual's ethnic identity must be regarded as another such. Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world. The concept of private life moreover includes elements relating to a person's right to their image" (citations omitted).[30]

45. The Court went on to conclude:

> "The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding. However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained" (citations omitted).[31]

46. This reasoning was most recently applied by the British Court of Appeal in *Catt v ACPO* [2012], in which the Court considered the retention in a database of written and photographic reports about the applicant's attendance at demonstrations and protests. The Court held that "[t]he systematic collection, processing and retention of a searchable database of personal information, even of a relatively routine kind, involves a significant interference with the right to respect for private

---

[27] At [72]-[73].
[28] *Rotaru v. Romania* (2000) Application 28341/95
[29] *Rotaru v. Romania* (2000) Application 28341/95 paras 43-44.
[30] *S and Marper v United Kingdom* (2009) 48 EHRR 50 para 66.
[31] *S and Marper v United Kingdom* (2009) para 67.

life".[32] In the case of publicly available information, the test is not solely, or even predominantly, concerned with whether the individual had a reasonable expectation of privacy, but rather the factor of particular importance is whether data have been subject to systematic processing and entry on a database capable of being searched in a way that enables the authorities to recover information by reference to a particular person.[33]

47. A similar approach to the analysis of personal data, even publicly available information, has been developed by the United States Supreme Court in *United States v Jones* (2012) in considering the use of GPS tracking technology.[34] The Court held that the attachment of a GPS device to a vehicle, and the use of that device to monitor the vehicle's movements, constituted a search in contravention of the Fourth Amendment to the US Constitution. While the Court's decision turned on the corollary issue of trespass on the vehicle, the concurring opinions of the Court considered at length the effect of new technologies, and. The Court suggested that advancements in capabilities that allow the collection and processing of personal data over a period of time may necessitate a departure from the long-standing legal precept that communications data enjoys a lower level of legal protection. Justice Sotomayor 's comments are apposite:

> "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. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." United States v. Cuevas-Perez, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. […]
>
> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., Smith, 442 U. S., at 742; United States v. Miller, 425 U. S. 435, 443 (1976). **This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.** People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and mediations they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable,"

[32] *Catt v ACPO* [2012] EWHC 1471 para 44.
[33] *Catt v ACPO* [2012] EWHC 1471 para 30.
[34] *United States v Jones* 132 S. Ct. 945 (2012)

> post, at 10, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[35]

Communications data

48. There has been increasing judicial recognition in Council of Europe member states of the value and sensitivity of communications data and the intrusive nature of its collection and processing. The European data retention directive 2006/24, mandating the retention of data generated or processed in the provision of communications services and networks for six to 24 months, is currently the subject of referrals in the European Court of Justice ("ECJ") by both the Irish High Court and the Austrian Constitutional Court. The Romanian and German Constitutional Courts have both declared legislation implementing the directive unconstitutional.[36] The recently published opinion of the Advocate General to the ECJ, Cruz Villalón, suggests the Court may find the directive in contravention of the European Convention on Human Rights. Mr Villalón criticised multiple elements of the directive and stated, in strong terms:

> "…the fact remains that the collection and, above all, the retention, in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitute a permanent threat throughout the data retention period of to the right of citizens of the Union to confidentiality in their private lives…"[37]

49. As data becomes more and more revelatory, either in isolation or when paired with other data, it is no longer appropriate to subject communication data to lower thresholds or consider its collection and processing a less invasive practice than interception of content. Communications data can now reveal equally sensitive information as communications content.[38]

50. The changing nature of communications data and the information that its collection and processing reveals by virtue of advancements in technologies must result in a change in

---

[35] *United States v Jones* 132 S. Ct. 945 (2012) at pp. 3-4 [emphasis added].

[36] Curtea Constitutionala a Romaniei, Decision No. 1258 of 8 October 2009, German Federal Constitutional Court Vorratsdatenspeicherung decision 1 BvR 256/08, 2 March 2010

[37] Opinion of Advocate General Cruz Lillalon, delivered on 12 Decmber 2013, in the case of Digital Rights Ireland v Ireland (Request for a preliminary ruling from the High Court of Ireland) and Kartner Landesregierung and Others (Request for a preliminary ruling from the Verfassungsgerichtshof (Austria)), para 72.

[38] For more information about the revelatory nature of metadata, see Jonathan Mayer and Patrick Mutchler, "MetaPhone: The NSA's Got Your Number," *Web Policy*, available at http://webpolicy.org/2013/12/23/metaphone-the-nsas-got-your-number/

perception of it as akin to communications content in nature and worth. **As such, if the mere existence of legislation enabling surveillance of communications content constitutes an interference with the right to privacy,[39] so too must the existence of legislation enabling the acquisition, processing, and analysis of communications data for the purposes of surveillance**.

III- Mass surveillance as inherently disproportionate

51. Mass surveillance (sometimes erroneously labelled "bulk collection") suggests the interception of communications content or access to communications data on a large and indiscriminate scale, either through generalised blanket surveillance of whole cables, networks or devices, or the wholesale requisition of data from a third party. It is to be contrasted against targeted interception in which the State agency effecting interception is required to identify a particular individual, residence, IP address or device upon which surveillance is to be carried out, or, in the case of access to communications data, to specify the individuals or accounts to which the data pertains.

52. Mass surveillance of digital communications can be achieved – and is being achieved by, among others, the United States and United Kingdom – by placing a tap on one or more of the undersea cables that carry 99 per cent of the world's communications. These cables are owned for the most part by private companies, who are allegedly paid by governments to facilitate massive interception of all of the digital communications that flow through them.[40] In conducting fibre optic cable interception – what the NSA sometimes calls "upstream" collection – States can collect and read any the content of any unencrypted communication flowing through that cable. These include phone calls, voice-over-IP calls, messages, emails, photos, ss and Facebook posts. They can then apply a range of analysis techniques and filters to that information – from voice, text and facial recognition, to the mapping of networks and relationships, behavioural analysis, and emotion detection. The most comprehensive example of mass surveillance systems are the recently revealed progammes being undertaken by the US and UK signals intelligence agencies, but mass interception systems are also available for purchase, and we know they were part of the infrastructure in pre-revolutionary Tunisia and Libya. Some of the promotional material published by companies that make these technologies attests to the fact that they enable "country-wide monitoring" of "all calls and messages"; "mass capture of entire countrywide wireline telecommunications networks"; interception of "more than 100,000 simultaneous voice channels" and the capturing of "up to one billion intercepts a day and storing in excess of 5000 terrabytes of information.[41]

53. A recently reported disclosure concerns an NSA mass surveillance programme called MYSTIC, by which enables the US to conduct mass surveillance of all phone calls (content and metadata) from an unidentified country.[42] According to the leaked documents, collection systems recorded and

[39] *Weber and Saravia v Germany* (2006) Application 54934/00

[40] http://www.guardian.co.uk/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

[41] Privacy International's Surveillance Industry Index collates the promotional material of more than 300 surveillance companies selling these types of technologies: https://www.privacyinternational.org/sii/

[42] http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html

continue to record, “every single” conversation nationwide, storing billions of them in a 30-day rolling buffer that clears the oldest calls as new ones arrive.

54. From a human rights perspective, mass surveillance on this scale can never be said to be proportionate. It involves the interference with a fundamental human right on an indiscriminate basis.

55. The ECtHR cases on interception have not yielded any considerable jurisprudence on what constitutes proportionality in the context of surveillance. In the context of bulk collection and retention of DNA records in *S and Marper v the United Kingdom* (2008)[43] the Court remarked:

> “In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed (see paragraph 35 above); in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.
>
> The Court acknowledges that the level of interference with the applicants' right to private life may be different for each of the three different categories of personal data retained. The retention of cellular samples is particularly intrusive given the wealth of genetic and health information contained therein. However, such an indiscriminate and open-ended retention regime as the one in issue calls for careful scrutiny regardless of these differences.
> […]
> In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society...”

The decision in *S and Marper* demonstrates that **an indiscriminate measure, even where it can be shown to meet a legitimate aim, is unlikely to meet the proportionality aspect of being ‘necessary in a democratic society’**.[44]

[43] Application 30562/04 and 30566/04, at paras 119-125.
[44] See also in this regard Campbell v United Kingdom Appl. No. 3578/05 (ECtHR 27 March 2008)

56. The jurisprudence of the ECtHR suggests that the following factors have a bearing upon whether the proportionality criteria is satisfied:

    a. **Scope** - Is the scope of the interference sufficiently limited?
    b. **Safeguards** - What measures are in place to safeguard fundamental rights?
    c. **Nature of the interference** – What type of information is being collected and what is the nature of the activity subjected to the measure? In *Dudgeon v United Kingdom*,[45] the ECtHR placed significance on the particularly sensitive nature of the activity being affected as well as the circumstances in which the measure was deployed.
    d. The **severity of the pressing social need** and **associated harm or detriment** to or effect on the public.

57. An assessment of mass surveillance measures in light of these criteria reveals the following:

    a. **Mass surveillance is inherently disproportionate** – Mass surveillance operations enable the scooping up of communications pertaining to individuals on the basis of location, nationality, or communications services used, rather than on the basis of individualised suspicion or the detection or prevention of a particular offence. The fundamental premise of this communications (signals) intelligence gathering is the collation of excessive amounts of information from which patterns or correlations might be drawn, rather than the pursuit or investigation of particular activities. Such a scope is necessarily so broad as to obliterate any precision or targeted calculation of the individual impacts of measures.
    b. **Mass surveillance is also inherently disproportionate regardless of technical or procedural safeguards** – It is difficult to imagine what safeguards would need to be put in place to prevent against abuse of a system that enables the mass collection and storage of intimate and sensitive information on whole populations. The very quantity and nature of the information being collected renders such a system inherently unsafe. Even if judicial authorization were to be required for each act of mass surveillance – which, in most countries, it is not – and such surveillance could be independently audited, the very collection of such valuable information in itself raises huge issues of safety and security that would be extremely difficult to overcome with legal safeguards. In addition, the "minimisation" procedures used by States such as the US, which they claim safeguard the communications of certain categories of persons, are shrouded in secrecy.
    c. **Mass surveillance interferes with virtually all aspects of our everyday lives** – Given that almost all activities – communication between individuals, financial transactions, accessing health care services, to name just a few – are now conducted online, via computers or on mobile phones, and thus subject to mass collection techniques such as tapping into the undersea cables or at Internet switches, mass surveillance interferes with any and all activities, even those of an extremely sensitive nature.
    d. **No compelling evidence has ever been put forward to justify the need for mass surveillance** – While the protection of national security and the prevention of crime

[45] Dudgeon v United Kingdom Appl. No. 7525/76 (ECtHR 22 October 1981)

and disorder are undoubtedly pressing social needs, it is difficult to assess the severity of those needs – particularly under the umbrella of national security – given the aura of secrecy accorded to surveillance in the context of national security and terrorism-related measures. It is impossible for the public to know or assess the pressing nature of the need without greater transparency and accountability by governments about the usefulness of surveillance measures in actually addressing national security and terrorism concerns.

e. **Mass surveillance has a correlative chilling effect on freedom of expression and freedom of association** – The destructive impact of mass surveillance on general well-being cannot be underestimated. These impacts include not only the violation of privacy rights, but extend to broader societal impacts on the ability to freely form and express ideas and opinions, to associate and organise, and to disagree with dominant political ideologies and demand change to the status quo. It is well-accepted that people are much less likely to express themselves and share information if they know or suspect that the government is monitoring their interactions with others. By undermining people's confidence in the privacy and security of their online communications, mass surveillance seriously impedes the free flow of information and ideas online. Mass surveillance chills not only free speech, but innovation, creation and imagination. As the UN Special Rapporteur on Freedom of Expression concluded in his report of 17 April 2013, 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. [46] The UN Special Rapporteur also warned that without strong legal protections in place, journalists, human rights defenders, political activists and whistleblowers risk being subjected to arbitrary surveillance activities. [47] The European Court of Human Rights recognized as much in *Segerstedt-Wiberg and Others v Sweden* (no. 62332/00, 6 June 2006, paras. 107), where it found that the Swedish government's collection and storage of personal data related to political opinion, affiliations and activities was an unjustified interference with the rights to freedom of expression and association.

IV- State obligations to respect privacy of all individuals subject to jurisdiction

58. **States owe human rights obligations to *all* individuals subject to their jurisdiction.**[48] This extends not only to the territory of the State, but to anyone within the power and effective control of the State, even if they are outside the territory.[49]

[46] See UN Special Rapporteur on Freedom of Expression, report of 17 April 2013 (A/HRC/23/40), para. 79.
[47] Ibid., paras. 51 and 79
[48] ICCPR, Article 2: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction…"; ECHR, Article 1: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention;" American Convention on Human Rights, Article 1: "The States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination for reasons of race, color, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition."
[49] Human Rights Committee General Comment 31, para 10.

59. The right to privacy, extending as it does to the privacy of communications, is distinct from many other rights in the sense that its realization can occur remotely from the physical location of the individual. When an individual sends a letter, email or a text-message, or makes a phone call, that communication leaves their physical proximity and travels to its destination. In the course of its transmission the communication may pass through multiple other States and, therefore, multiple jurisdictions. Yet the right to privacy of the communication remains intact, subject only to the permissible limitations set out under human rights law.[50]

60. The obligation to "respect and to ensure to all individuals within its territory and subject to its jurisdiction" of Article 2.1 of the International Covenant on Civil and Political Rights has been interpreted by the Human Rights Committee[51] and the International Court of Justice[52] as entailing a disjunctive rather than conjunctive condition: a State Party is obligated with respect to "all individuals within its territory and all individuals subject to its jurisdiction." Although a conjunctive interpretation is possible,[53] such that obligations only accrue to persons both within the territory and the jurisdiction of a State Party, many countries and many scholars have rejected this narrow interpretation as fundamentally incompatible with the object and purpose of the treaty.[54] The question remains, then, what it means for an individual to be subject to a State Party's jurisdiction such that the state owes an obligation.

61. "Jurisdiction" with respect to State obligations under human rights instruments is commonly interpreted to refer to a State's power, authority, or "effective control" over an area or an individual.[55] While the ECtHR has with difficulty tried to rationalise decisions by focusing variously

---

[50] A comprehensive account of the permissible limitations on the right to privacy is presented in the report of the UN Special Rapporteur on the freedom of expression and opinion of 17 April 2013 (A/HRC/23/40).

[51] See Human Rights Committee, General Comment No. 31: Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) para. 10.

[52] *See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ Rep. 136, paras. 108, 111.

[53] The conjunctive interpretation is maintained by the United States and Israel. Although the United States maintained this interpretation at its latest periodic review under the ICCPR, it should be noted that its former Department of State Legal Advisor, Harold Koh, apparently argued this position was without compelling historical or legal foundation and should be changed. See Memorandum Opinion on the Geographic Scope of the International Covenant On Civil and Political Rights from Harold Hongju Koh, former Legal Adviser of the Department of State, to the Office of the Legal Adviser, October 19, 2010 (hereinafter "Koh memo"), http://www.nytimes.com/interactive/2014/03/07/world/state-department-iccpr.html?_r=0 (accessed March 27, 2014). Professor Ryan Goodman also points out that the United States, in its 2013 Department of Defense Operational Law Handbook, explicitly acknowledges that customary international human rights law binds the United States military in extraterritorial operations, and that among those customary rules is prohibition of "consistent patterns of gross violations" of internationally recognized human rights. See Ryan Goodman, "International Law and Mass Foreign Surveillance: A Response to Ben Wittes and Ashley Deeks," accessible at http://justsecurity.org/2014/03/26/international-law-mass-foreign-surveillance-response-ben-wittes-ashley-deeks/.

[54] See, e.g. Thomas Buergenthal, *To Respect and to Ensure: State Obligations and Permissible Derogations, in* THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS (Louis Henkin ed., 1981) and Milanovic, draft essay (articulating the "Auschwitz Rule" that a human rights treaty whose purpose is to establish universal norms and protections should not be read in a way as to be inapplicable to an atrocity that motivated its very creation, i.e. a German death camp in occupied Polish territory).

[55] See Human Rights Committee, General Comment No. 31, para. 10; Wall decision; see also Loizidou v. Turkey, App. No. 15318/89, Judgment (preliminary objections), 23 February 1995, para. 62 (European Convention on Human Rights applies when as a consequence of military activity a Contracting Party exercises effective control of an area outside its territory).

on the physical or juristic control of the territory on which the human victim is found (the prison containing the prisoner, or the contested territory on which a person is killed),[56] the Human Rights Committee has taken a somewhat different approach. In Lopez-Burgos[57], the Committee stressed that "jurisdiction" was not pinned to the status of the location of an alleged violation, but rather to a *relationship* between the state and an individual in respect of an alleged violation, so that Uruguay was not free of responsibility for its agents abducting an individual on the territory of Argentina.

62. Manfred Nowak, the former Special Rapporteur on Torture, has written in support of this view of jurisdiction that centres on the relation of the state and the individual with respect to a Covenant right. In a recent letter,[58] he contends that a correct interpretation of "effective control" over a person "must take the **specific right at issue** into account". While physical custody of an individual may be a necessary condition for the commission of torture, it is not necessary for all human rights violations, as demonstrated by the ECtHR rulings in *Issa v Turkey*[59] and *Al-Skeini v United Kingdom*, both concerning extraterritorial violations of the right to life. As an illustration, he posits the condition of a woman, held by a foreign power in house arrest in her country. If she were then tortured, existing law would firmly support she was in the "effective control" of that foreign state. And so she would be if the foreign state confined her in her home in which it installed listening devices, violating not only her freedom of movement but her privacy as well. However, if she were not confined, but nevertheless had her house secretly bugged by a foreign power, her right to a private life would still be in the "effective control" of the foreign power.[60]

63. Martin Scheinin also writes in support of this view,[61] citing the cases of *Sophie Vidal Martins v Uruguay* (57/1979), where the Human Rights Committee found a violation on the part of Uruguay for refusing to issue a passport to its citizen in Mexico, thereby preventing her from leaving that country, and *Gueye et al. v France* (196/1985), where France was found to impermissibly discriminate in legislation that accorded veterans of its military who were French living in France a higher pension than to Senegalese veterans of its military who were living in Senegal. In both cases, the control over territory or physical custody of the individual was immaterial, and the ability of the state to control enjoyment of the individual's right was key.

---

[56] Cf. Banković and Others v. Belgium and Others [GC] (dec.),, App. No. 52207/99, 12 December 2001 and Al-Skeini and others v. United Kingdom [GC], App. No. 55721/07, 7 July 2011.

[57] Lopez-Burgos v. Uruguay, Communication No. R.12/52, UN Doc. Supp. No. 40 (A/36/40) at 176 (1981), paras. 12.1-12.3

[58] See Letter to the Editor from Manfred Nowak, What does extraterritorial application of human rights treaties mean in practice?, *Just Security*, March 11, 2014, http://justsecurity.org/2014/03/11/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/ (accessed March 27, 2014)

[59] Issa v. Turkey, App. No. 31821/96, 16 November 2004.

[60] This example also points to a peculiar and complicating characteristic of surveillance as a human rights violation; it not only can be conducted remotely, it can be conducted invisibly and non-exclusively, so that the State on whose territory the individual victim resides may be unaware and so unable to protect its resident, or may even be simultaneously conducting surveillance with or without knowledge of one or more foreign States' surveillance. This problem of invisibility and non-exclusiveness underscores the importance of finding "effective control" with respect to any State that has control of an individual's right to privacy of communications.

[61] See Letter to the Editor from Martin Scheinin, former member of the Human Rights Committee, *Just Security*, March 10, 2014, http://justsecurity.org/2014/03/10/letter-editor-martin-scheinin/ (accessed March 27, 2014)

64. This approach to understanding "effective control" was recently reiterated by the Human Rights Committee in its March 26, 2014 concluding observations on the fourth periodic review of United States compliance with the ICCPR, where it urged the United States to "acknowledge the extraterritorial application of the Covenant under certain circumstances," and in particular to "take all necessary measures to ensure that its surveillance activities, **both within and outside** the United States, conform to its obligations under the Covenant, including article 17" and to take measures to ensure that any interference with privacy "complies with the principles of legality, proportionality and necessity **regardless of the nationality or location** of individuals whose communications are under direct surveillance" (emphasis added). [62]

65. Yet a third type of reading of Article 2.1 has been put forward,[63] whereby the obligation to "respect" rights is considered more generally applicable to individuals whose rights are at stake, but the obligation to "ensure" is read as restricted to only those within the "territory and jurisdiction" of the State Party. This interpretation recognizes the universality of both human rights and the universal obligation of States to respect them,[64] in the sense of negative duties of non-interference, and at the same time acknowledges the practical and legal limits on any given State's ability to positively ensure rights to persons living under a different sovereign.

66. The extension of these principles to the protection of privacy in the context of communications surveillance by a foreign State does not require a new normative framework. Any State that can engage in extraterritorial surveillance over foreigners outside its territory is a) required to at a minimum "respect" the right to privacy, that is, to conduct surveillance in accord with the right as delimited in international law, and b) is capable of exerting "effective control" over those persons' access to the right to privacy, and should thereby be required to apply the Covenant to its actions.

67. Given the invasive nature of the mechanisms by which surveillance of global communications networks is effective – the exploitation of the very infrastructure that makes up the internet – it is evident that the measures taken by States to achieve surveillance of foreigners communications allow them "effective control" of the privacy rights of all individuals whose communications pass within their reach.

68. With the advent of the internet and new digital forms of communication, now most digital communications take the fastest and cheapest route to their destination, rather than the most direct. This infrastructure means that the sender has no ability to choose, nor immediate knowledge of, the route that their communication will take. Even when a digital communication is

---

[62] It should be noted that different writers have different formulations. Harold Koh, for example, argues in his memorandum, "A state incurs obligations to respect Covenant rights - i.e., is itself obligated not to violate those rights through its own actions or the actions of its agents - in those circumstances where a state exercises authority or effective control over the person or context at issue" while confining the obligation to ensure to situations where there is not only control over the person or context, but territory as well. Marko Milanovic, in contrast, casts the obligation to respect as universal and unqualified, and the obligation to ensure as requiring control of an "area" because otherwise proactive measures are beyond its power.

[63] See Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," and Koh memo. Note that these authors, and others who endorse this interpretive strategy, do not agree on the precise contours and conditions of the obligation to ensure, but that's beyond the scope of this memorandum

[64] See, e.g. UN Charter art. 55(c); UDHR preamble (member states pledge to achieve "the promotion of universal respect for and observance of human rights and fundamental freedoms").

being sent to a recipient within the same country as the sender, the communication may travel around the world to reach its destination. Upstream fibre optic cable interception, which compromises the cables that carry 99 per cent of the world's communications; mass collection of communications data held by the world's largest internet companies; the hacking of networks and devices, the compromising of encryption standards and tools, and the exploitation of applications and programmes; each of these measures enables the States conducting them such total power over the affected individuals' communications so as to render such States in "effective control" of the person's enjoyment of the right to privacy. We note, moreover, that many acts of surveillance do not take place outside a given State's territory, but by intercepting communications as they flow through its territory.

69. We therefore urge the High Commissioner to conclude that **a State conducting extraterritorial surveillance on any person is required at minimum to respect the right to privacy**, and conform its actions accordingly, regardless of the location or nationality of the individual whose communications are invaded. Depending on the degree of control it exercises over the location, individual or context, **a State may also have positive obligations to ensure and protect the individual's privacy, by regulating or legislating appropriately, or by restraining the actions of third parties.**

V- Ensuring enjoyment of the right to privacy without discrimination

56. The patchwork of secret spying programmes and intelligence-sharing agreements implemented by parties to the Five Eyes arrangement (the US, UK, Canada, Australia and New Zealand) constitutes an integrated global surveillance arrangement that covers the majority of the worlds' communications. At the heart of this arrangement are carefully constructed legal frameworks (Appendix 1 to this submission) that provide differing levels of protections for internal versus external communications, or those relating to nationals versus non-nationals. These discriminatory frameworks attempt to circumvent national constitutional or human rights protections governing interferences with the right to privacy of communications that, States purport, apply only to nationals or those within their territorial jurisdiction.

57. It is evident that the legal frameworks of the Five Eyes States currently distinguish between the obligations owed to nationals or those within the States' territories, and non-nationals and those outside. In doing so, these legal frameworks infringe upon the rights of all individuals within the respective States' jurisdiction to enjoy human rights protections equally and without discrimination.

58. In human rights law, discrimination constitutes any distinction, exclusion, restriction or preference, or other differential treatment based on any ground, including national or social origin, or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment, or exercise by all persons, on an equal footing, of all rights and freedoms.[65] The Human Rights Committee has deemed nationality a ground of "other status" with

[65] General Comment No. 20 of the Committee on Economic Social and Cultural Rights, 10 June 2009.

respect of article 2(1) of the ICCPR in *Gueye and ors v France*.[66] The ECtHR has also recognised that "country of residence" is an aspect of personal status for the purposes of Article 14 ECHR.[67]

59. It is both irrational and contrary to the spirit and purpose of international human rights norms to suppose that the privacy of a person's communications could be accorded different legal weight according to their nationality or residence. An equivalent distinction on the basis of ethnicity or gender would be deemed to be manifestly incompatible with human rights law; why then should States be able to purport to offer varying protections based on an individual's nationality or location? If an individual within a State's jurisdiction is granted lower or diminished human rights protections – or indeed is deprived of such protections – solely on the basis of their nationality or location, this will not only lead to a violation of the right they seek to enjoy, but will amount to an interference with their right to be free from discrimination.

60. Individuals have a legitimate expectation that their human rights will be respected not only by the State upon whose territory they stand, but by the State within whose territory their rights are interfered with. The current legal frameworks of the Five Eyes States purport to discriminate between the rights and obligations owed to nationals or those physically within their territory, and those outside of it, or non-nationals.

Conclusion – procedural steps

70. In addition to the issues articulated above, we wish to declare our support for further action to be taken by the Human Rights Council in order to affirm the centrality of the right to privacy and better guarantee its protection and promotion in the digital age, including the following:

    a. The establishment of a regionally-representative Commission of Inquiry to undertake a survey of laws, regulations and State practice with respect to intelligence practices and their compliance with international human rights law;
    b. The establishment of a dedicated special procedures mandate to the right to privacy in the digital age; and
    c. The issuance by the Human Rights Committee of a new General Comment on the right to privacy, to replace General Comment 16 (1988).

66 Gueye and Others v. France (Comm. No. 196/1985)
67 *Carson v the United Kingdom* (no. 42184/05), 16 March 2010, paras. 70-71

Appendix 1: Discriminatory legal frameworks of the Five Eyes States

61. Each of the Five Eyes members (United States, United Kingdom, Australia, New Zealand and Canada) have complex legal frameworks governing the interception, monitoring and retention of communications content and data. This paper does not attempt to comprehensively outline such frameworks, and only excerpts some relevant provisions to illustrate the obfuscatory nature of legal frameworks that enable the rights of non-nationals or those outside the territory to be diminished.

United States

62. FISA section 1881a (also known as Section 702 of FISA Amendments Act) is entitled "Procedures for targeting certain persons outside the United States other than United States persons" and applies generally to collections occurring inside the US.

63. Section 1881(a) ss (a) provides:
    a. the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be *located outside the United States* to acquire foreign intelligence information.

64. An authorisation pursuant to FISA section 1881(a) permits "foreign intelligence information" to be obtained both by directly intercepting communications during transmission and by making a request to an electronic service provider that stores the information to make it available to the authorities.

65. Executive Order 12333[68] authorizes surveillance conducted by the US primarily outside the United States, although there are indications that the government maintains that some amount of US-based surveillance can also occur under this authority. The US government asserts that programmes conducted under the authority of EO 12333 do not require judicial approval or oversight of any type. While EO 12333 contains some restrictions on actions concerning US persons, and instructs the intelligence agencies to provide further restrictions, EO 12333 notably contains no collection, retention or use limitations regarding non-US persons.

66. Under both FISA section 1881a and Executive Order 12333, what can be acquired is defined very broadly. FISA section 1881a authorizes the collection of information for the purpose of obtaining "foreign intelligence information" which is defined to include information about terrorism, weapons of mass destruction and counterintelligence - categories of information that arguably could be important for national security. But it also allows for the collection of information that merely "relates to" the "conduct of foreign affairs of the United States."[69] What can be obtained under Executive Order 12333 is even broader. It is defined as "foreign intelligence" which means information "relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists" – allowing for

68 http://www.archives.gov/federal-register/codification/executive-order/12333.html
[69] 50 U.S.C. Section 1801(e).

the collection of information merely about "foreign persons."[70]

United Kingdom

56. The Regulation of Investigatory Powers Act 2000 *distinguishes between "internal" and "external" surveillance.* Where the communication is internal (i.e. neither sent nor received outside the British Islands, see RIPA s 20), a warrant to permit lawful interception must describe one person as the "interception subject" (s 8(1)(a)) or identify a "single set of premises" for which the interception is to take place (s 8(1)(b)). The warrant must set out "the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted" (s 8(2)).

57. Where the communication is "external", that is either sent or received outside the British Islands, RIPA s 8(1) and 8(2) do not apply. There is no need to identify any particular person who is to be subject of the interception or a particular address that will be targeted.

New Zealand

58. The Government Security Communications Bureau is permitted to conduct interception by applying for an interception warrant under s15A of the Government Communications Security Bureau Act 2003 (amended 2013). However, s14 of the Act (as amended) states that in performing the function of intelligence gathering and analysis, the GSCB cannot "authorise or do anything for the purpose of intercepting the private communications of a person who is *a New Zealand citizen or a permanent resident of New Zealand*, unless (and to the extent that) the person comes within the definition of foreign person or foreign organisation....".

59. However, this limitation does not apply to its other two functions – i.e. surveillance of New Zealanders related to cyber-security and assisting other agencies (such as the Police).

Australia

60. Under the *Intelligence Services Act 2001*, the Australian intelligence agencies can conduct any activity connected with their functions[71] provided they have the authorisation of the relevant Minister (s8).
61. However, *where there is an Australian person involved* the Minister must be satisfied of the following before making an authorisation (s9):
    a. any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned; and
    b. there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and
    c. there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

[70] Executive Order 12333, Section 3.5(e), http://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf

71 Which include to obtain foreign intelligence (ASIS), to obtain intelligence relevant to security (ASIO), to obtain foreign intelligence using the electrical, magnetic or acoustic energy (ASD), or to obtain geospatial and imagery intelligence via electromagnetic spectrum (DIGO)

62. In addition, the Minister must (s9(1A))
    a. be satisfied that the Australian person mentioned in that subparagraph is, or is likely to be, involved in one or more of the following activities:
        i. activities that present a significant risk to a person's safety;
        ii. acting for, or on behalf of, a foreign power;
        iii. activities that are, or are likely to be, a threat to security;
        iv. activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
        v. committing a serious crime by moving money, goods or people;
        vi. committing a serious crime by using or transferring intellectual property;
        vii. committing a serious crime by transmitting data or signals by means of guided and/or unguided electromagnetic energy; and
    b. if the Australian person is, or is likely to be, involved in an activity or activities that are, or are likely to be, a threat to security (whether or not covered by another subparagraph of paragraph (a) in addition to subparagraph (a)(iii))—obtain the agreement of the Minister responsible for administering the *Australian Security Intelligence Organisation Act 1979*.
63. There are *separate Rules to Protect the Privacy of Australians* for each of the intelligence agencies, stating that where it is not clear whether a person is an Australian, it is presumed that a person within Australia is Australian and outside of Australia is not Australian (Rule 1.1). Where an intelligence agency does retain intelligence information concerning an Australian person, the agency must ensure the information is protected by security safeguards, and access to the information is only to be provided to persons who require it (Rule 2.2).

<u>Canada</u>

64. The *National Defence Act* pertains to the Communications Security Establishment Canada (CSEC) and establishes that the mandate of CSEC is (s273.64 (1))
    a. to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
    b. to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;

    […]

    Para (2) of the section provides that activities
    a. shall not be directed at Canadians or any person in Canada; and
    b. shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.