International Principles on the Application of Human Rights to Communications Surveillance

Final version June 7 2013

As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. This document attempts to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These principles can provide civil society groups, industry, and States with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

Preamble

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law.[1] Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[2]

Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and information about communications, or "communications metadata," the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale. [3] Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.

The frequency with which States are seeking access to communications content and communications metadata -- information about an individual's communications or use of electronic devices -- is rising dramatically, without adequate scrutiny.[4] When accessed and analysed, communications metadata may create a profile of an individual's private life, including medical conditions, political and religious viewpoints, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone.[5]

Despite the vast potential for intrusion into an individual's private life, legislative and policy instruments often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by agencies, including how they are data-mined, shared, and retained.

In order for States to actually meet their international human rights obligations in relation to communications surveillance, they must comply with the principles set out below. These principles apply not only to the State's obligation to respect and fulfil individuals' rights, but also to the obligation to protect individuals' rights from abuse by non-State actors, including corporate entities. [6] The private sector bears equal responsibility for respecting and protecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and – where required – cooperating with State surveillance activities. Nevertheless, the scope of the present Principles is limited to the obligations of the State.

Changing technology and definitions

"Communications surveillance" in the modern environment encompasses the monitoring, interception, collection, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future. "Communications" include activities, interactions and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking information such as IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

Traditionally, the invasiveness of communications surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider.[7] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, colour, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time,[8] or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law.

In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State. Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require

people to be able to communicate free from the chilling effect of government surveillance. A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

When adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the form as well as the scope and duration of the surveillance are relevant factors. Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.[9]

The determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles.

The Principles

Legality: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

Legitimate Aim: Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Necessity: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

Adequacy: Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

Specifically, this requires that, if a State seeks access to protected information through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

a. there is a high degree of probability that a serious crime has been or will be committed;
b. evidence of such a crime would be obtained by accessing the protected information sought;
c. other available less invasive investigative techniques have been exhausted;
d. information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
e. information is accessed only by the specified authority and used for the purpose for which authorisation was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

a. other available less invasive investigative techniques have been considered;
b. information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
c. information is accessed only by the specified authority and used for the purpose for which was authorisation was given.

Competent Judicial Authority: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be (1) separate from the authorities conducting communications surveillance, (2) conversant in issues related to and competent to make judicial decisions about communications technologies and human rights, and (3) have adequate resources in exercising the functions assigned to them.

Due process: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,[10] except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

User notification: Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

a. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or
b. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
c. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed.

Upon the expiry of the delay, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

Transparency: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.[11] Oversight mechanisms should have the authority to access information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

Integrity of communications and systems: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.[12]

Safeguards for international cooperation: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States should not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

Safeguards against illegitimate access: States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

Signatories

- Access Now
- Association for Progressive Communications
- Article 19 (International)
- Bits of Freedom (Netherlands)
- Center for Internet & Society (India)
- Comision Colombiana de Juristas (Colombia)
- Derechos Digitales (Chile)
- Electronic Frontier Foundation (International)
- Open Media (Canada)
- Open Net (South Korea)
- Open Rights Group (United Kingdom)
- Privacy International (International)
- Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (Canada)
- Statewatch (UK)

---

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[2] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[3] Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, logs of nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts

[4] For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies who are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of

which were granted and executed. 2012 data available at http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586

[5] See as examples, a review of Sandy Petland's work, "Reality Mining", in MIT's Technology Review, 2008, available at http://www2.technologyreview.com/article/409598/tr10-reality-mining/ and also see Alberto Escudero-Pascual and Gus Hosein, "Questioning lawful access to traffic data", Communications of the ACM, Volume 47 Issue 3, March 2004, pages 77 - 82.

[6] Report of the United Nations Special Rapporteur on freedom of opinion and expression, Frank La Rue, 3 June 2013, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pd

[7]"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 medications they purchase to online retailers . . . 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." *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[8] "Short-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *United States v. Jones*, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

[9] "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." *U.S. v. Maynard*, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; *U.S. v. Jones*, 565 U.S. __, (2012), Alito, J., concurring. "Moreover, public 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." (*Rotaru v. Romania*, [2000] ECHR 28341/95, paras. 43-44.

[10] The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

[11] The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinise the types of requests, the extent of each access request,

the purpose of the requests, and the scrutiny applied to them.
See http://www.intelligencecommissioners.com/sections.asp?sectionID=2&type=top.

[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.