

NECESSARY & PROPORTIONATE

INTERNATIONAL PRINCIPLES
ON THE APPLICATION OF HUMAN RIGHTS
TO COMMUNICATIONS SURVEILLANCE



Credits

The International Principles on the Application of Human Rights to Communications Surveillance was cooperatively written by privacy organizations and experts worldwide including, but not limited to, Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comisión Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Reporter Without Borders, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International, and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. In addition, we also want to thank IP Justice, SHARE Foundation — SHARE Defense, IFEX Network and Instituto NUPEF for help connecting concerned groups together.

For more information, visit

necessaryandproportionate.org/text

Background History

More than 40 privacy and security experts participated in the drafting process of the Principles during the Brussels meeting in October 2012. After an initial broad consultation, which included a second meeting in Rio de Janeiro in December 2012, Access, EFF and Privacy International led a collaborative drafting process that drew on the expertise of human rights and digital rights experts around the world. The first version of the Principles was finalized on July 10, 2013 and was officially launched at the UN Human Rights Council in Geneva in September 2013. The resounding success and global adoption of the Principles by more than 400 organizations across the world necessitated a number of specific, primarily superficial, textual changes in the language of the Principles in order to ensure their consistent interpretation and application across jurisdictions. From March 2013 to May 2013, another consultation was conducted to ascertain and rectify those textual problems and update the Principles accordingly. The effect and the intention of the Principles were not altered by these changes. This version is the final product of those processes and is the authoritative version of the Principles.

NECESSARY & PROPORTIONATE

FINAL VERSION MAY 2014*

As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws, regulations, activities, powers, and authorities related to Communications Surveillance adhere to international human rights law and standards. This document attempts to clarify 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, States, and others 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 Communications Surveillance interferes with the right to privacy among a number of other human rights. As a result, it may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and 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 Communications Surveillance by States. 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 an individual's communications or use of electronic devices — the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make Communications Surveillance by States possible at an unprecedented scale.³ Meanwhile, conceptualisations of existing human

NECESSARY & PROPORTIONATE

rights law have not kept up with the modern and changing Communications Surveillance technologies and techniques of the State, the ability of the State to combine and organize information gained from different surveillance technologies and techniques, or the increased sensitivity of the information available to be accessed.

The frequency with which States are seeking access to both communications content and metadata is rising dramatically, without adequate scrutiny.⁴ Communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.⁵ Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, laws, regulations activities, powers, or authorities often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by States.

SCOPE OF APPLICATION

The Principles and the Preamble are holistic and self-referential – each principle and the preamble should be read and interpreted as one part of a larger framework that, taken together, accomplish a singular goal: ensuring that laws, policies, and practices related to Communications Surveillance adhere to international human rights laws and standards and adequately protect individual human rights such as privacy and freedom of expression. Thus, in order for States to actually meet their international human rights obligations in relation to Communications Surveillance, they must comply with each of the principles set out below.

These principles apply to surveillance conducted within a State or extraterritorially. The principles also apply regardless of the purpose for the surveillance — including enforcing law, protecting national security, gathering intelligence, or another governmental function. They also apply both to the State's obligation to respect and fulfil individuals' human rights, and also to the obligation to protect individuals' human rights from abuse by non-State actors, including business enterprises.⁶ Business enterprises bear responsibility for respecting individual privacy and other human rights, particularly given

NECESSARY & PROPORTIONATE

the key role they play in designing, developing, and disseminating technologies; enabling and providing communications; and in facilitating certain State surveillance activities. Nevertheless, these Principles articulate the duties and obligations of States when engaging in Communications Surveillance.

CHANGING TECHNOLOGY AND DEFINITIONS

“Communications surveillance” in the modern environment encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard 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 including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

“Protected Information” is 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. 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 and associations. 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, color, sexual orientation, national origins, or viewpoints; or enable the mapping of

NECESSARY & PROPORTIONATE

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 Protected Information should 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. Any Communication Surveillance is an interference with human rights and so international human rights law applies. 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 or invasive techniques used to accomplish Communications Surveillance have 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 full protection as Protected Information.⁹

The determination of whether the State may conduct Communications Surveillance with regard to Protected Information must be consistent with the following principles.

THE 13 PRINCIPLES



THE 13 PRINCIPLES

Legality

Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights 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 human rights 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 that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Necessity

Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are 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 is always 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 human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

1. there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;
2. there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;
3. other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and;
4. information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
5. any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
6. information is will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
7. that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

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 and independent from the authorities conducting Communications Surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used 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

Those whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstance:

NECESSARY & PROPORTIONATE

1. Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and
2. Authorisation to delay notification is granted by a Competent Judicial Authority; and
3. The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

The obligation to give notice rests with the State, but communications service providers should 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 laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. 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 not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for 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 all potentially relevant 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

NECESSARY & PROPORTIONATE

been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. 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 Communications 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.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 foreign service providers and States. 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 may 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 whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered 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 not be retained, but instead be destroyed or returned to those affected.

* The process of elaborating these Principles began in October 2012 at a meeting of more than 40 privacy and security experts in Brussels. After an initial broad consultation, which included a second meeting in Rio de Janeiro in December 2012, Access, EFF and Privacy International led a collaborative drafting process that drew on the expertise of human rights and digital rights experts across the world. The first version of the Principles was finalised on 10 July 2013, and officially launched at the UN Human Rights Council in Geneva in September 2013. The resounding success and global adoption of the Principles by more than 400 organisations across the world necessitated a number of specific, primarily superficial textual changes in the language of the Principles in order to ensure their consistent interpretation and application across jurisdictions. From March to May 2013, another consultation was conducted to ascertain and rectify those textual problems and update the Principles accordingly. The effect and the intention of the Principles was not altered by these changes. This version is the final product of those processes and is the authoritative version of the Principles.

ENDNOTES

- 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, Article 21 of the ASEAN Human Rights Declaration, 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. See also Frank La Rue, "Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression," 2013, A.HRC.23.40 EN.
- 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, metadata provides a window into 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 Perland'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.

NECESSARY & PROPORTIONATE

- 6 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16 2011, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf
- 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.iocco-uk.info/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.