GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

A principled fight against surveillance

Katitza Rodríguez
Electronic Frontier Foundation
www.eff.org

Years before Edward Snowden leaked his first document, human rights lawyers and activists were concerned about a dramatic expansion in law enforcement and foreign intelligence agencies' efforts to spy on the digital world. It had become evident that legal protections had not kept pace with technological developments – that the state's practical ability to spy on the world had developed in a way that permitted it to bypass the functional limits that have historically checked its ability to spy. These concerns culminated in the International Principles on the Application of Human Rights to Communications Surveillance,[1] a set of principles intended to guide policy makers, activists and judges to better understand how new surveillance technologies have been eating away at our fundamental freedoms and how we might bring state spying back in line with human rights standards.

Over a year and a half in the making, the final version of the Principles appeared on 20 July 2013, in the first weeks of what we might call the Snowden era. An updated version was issued in May 2014. The Snowden revelations, once they started rolling in, affirmed the worst of our concerns. Intelligence services as well as law enforcement had taken it upon themselves to spy on us all, with little consideration for the societal effects. Lawmakers and even the executive had little comprehension of the capabilities of their own spymasters, and how our digital networks were being turned against all individuals everywhere. The need for the Principles was confirmed in spades, but the long and difficult job of applying them to existing practices was just beginning.

Since then, the Principles have, we hope, been a lodestar for those seeking solutions to the stark reality exposed by Snowden: that, slipping through the cracks of technological developments and outdated legal protections, our governments have adopted practices of mass surveillance that render many of our most fundamental rights effectively meaningless. The Principles have been signed by over 470 organisations and individual experts, and have played a central guiding role in a number of the rigorous debates on the need to limit states' increasingly expansive surveillance capacities. Their impact is already evident in, for example, the US president's Review Group on Intelligence and Communications Technologies report, the Inter-American Commission on Human Rights report[2] and the Office of the United Nations High Commissioner for Human Rights' recent report on the right to privacy in the digital age.[3] Their influence has also manifested in some of the administrative and legislative attempts to address surveillance problems post-Snowden. Perhaps most importantly, they have functioned as a rallying point for campaigning and advocacy initiatives around the world.

Below, we spell out some of the key features of the Principles. A more detailed explanation of the legal grounding for our conclusions in human rights jurisprudence can be found in a Legal Analysis and Background Materials document generated in support of the Principles.[4]

Core definitions in international human rights law

The Principles begin with defining two core concepts that spell out the "what" and the "how" of measured surveillance. The first concept focuses on the type of data to be protected, while the second one ensures that a broad range of surveillance activity constitutes an interference with privacy rights. Outdated definitions of these two terms have led to expansive surveillance practices, as wide swaths of sensitive data or surveillance activities have been deemed outside the scope of legal protections. These definitional changes are designed to re-focus privacy protections away from artificial examinations of the kind of data or method of interference, and back on the ultimate effect on the privacy of the individual.

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

2 www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf

3 www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

4 https://en.necessaryandproportionate.org/LegalAnalysis

Protected information

The Principles make clear that it is time to move beyond the fallacy that information *about* communications does not pose as serious a threat to privacy as the content of communications. Information about communications, also called metadata, subscriber information or non-content data, can include the location of your mobile phone, clickstream data,[5] search logs, or anonymous online activity. Individually, these can be just as invasive as reading your email or listening to your phone calls. When combined and analysed *en masse*, the picture painted by such data points can be far more revealing than the content of the communications they accompany. In spite of this reality, pre-internet age (in fact, postal service-based!) legal conceptions have persisted in some legal systems, offering less or, in some instances, no protection at all to information that is not classified as "content". What is important is not the kind of data that is collected, but its effect on the privacy of the individual.

As explained in the Legal Analysis and Background Materials which have been prepared for the Principles:

> The Principles use the term "protected information" to refer to information (including data) that *ought* to be fully and robustly protected, even if the information is not currently protected by law, is only partially protected by law, or is accorded lower levels of protection. The intention, however, is not to make a new category that itself will grow stale over time, but rather to ensure that the focus is and remains the capability of the information, alone or when combined with other information, to reveal private facts about a person or her correspondents. As such, the Principles adopt a singular and all-encompassing definition that includes any information relating to a person's communications that is not readily available to the general public.

This concern has been addressed by the latest report of the Office of the High Commissioner for Human Rights (OHCHR), which made clear that:

> From the perspective of the right to privacy, this distinction between [content and metadata] is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.

Given the revealing nature of metadata and content alike, states should be restrained from unchecked interference with any protected information: from revealing a speaker's identity if it is not public; from wantonly vacuuming up the websites or social media one has visited; from stockpiling information on all the people one has communicated with; and tracking the "when", "from where", and "for how long" of all our digital activities. In the pre-internet age, the much more limited amount and kind of "metadata" available to law enforcement was treated as less sensitive than content, but given current communications surveillance capabilities, this can no longer be the case.

Communication surveillance

Much of the expansive state surveillance practices confirmed during the past year depend on confusion over whether actual "surveillance" has occurred and thus whether human rights obligations even apply. Some have suggested that if information is merely collected and kept but not looked at by humans, no privacy invasion has occurred. Others argue that computers analysing all communications in real time for key words and other selectors does not amount to "surveillance" for purposes of triggering legal privacy protections. Still others seek to reduce privacy protections to "harmful uses" of information. Such legal variations can mean the difference between reasonable and carefully targeted investigations and a surveillance state built on the continuous mass surveillance of everyone.

In the digital age, where the most sensitive portions of our lives are constantly communicated over digital networks, it has never been more important to ensure the integrity of our communications. It means little whether the interference takes the form of real-time monitoring of internet transmission, hacking into individuals' mobile devices, or mass harvesting of stored data from third party providers. The mere recording of internet transactions – even if ultimately unviewed – can have serious chilling effects on the use of our most vital interactive medium. We have to ensure that all acts of communications surveillance are within the scope of human rights protections and, hence, are "necessary and proportionate".

On this front, the OHCHR report made clear that:

> [A]ny capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with

5 en.wikipedia.org/wiki/Clickstream

> privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.

To remedy this issue, the Principles define "communications surveillance" as encompassing the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects or arises from a person's communications in the past, present or future.

Scope of application

The Principles also address a long-standing problem arising from narrow interpretations adopted by some states regarding the extraterritorial application of their human rights obligations. Some have argued that the obligation to respect privacy and other human rights of individuals effectively stops at their national borders. In a world of highly integrated digital networks, where individual interactions and data routes defy any semblance of territorial correspondence, such distinctions are meaningless. The Principles therefore apply to surveillance conducted within a state *or* extraterritorially, and regardless of the purpose for the surveillance – including enforcing law, protecting national security, gathering intelligence, or another governmental function.

The OHCHR's report explicitly underscores the principle of non-discrimination:

> Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

In this regard, the OHCHR's report stresses the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."

The 13 Principles

The substantive Principles are firmly rooted in well-established human rights law. Generally, any limits on human rights should be necessary, proportionate and for a set of permissible purposes. These limits must be set out in law, and cannot be arbitrary.

Under international human rights law, each right is divided in two parts. The first paragraph sets out the core of the right, while the second paragraph sets out the circumstances in which that right may be restricted or limited. This second paragraph is usually called the "permissible limitations" test.

Regarding the right to privacy, the UN Special Rapporteur on Counter-Terrorism[6] and the UN Special Rapporteur on Freedom of Expression[7] have stated that the "permissible limitations" test under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), among other articles, is equally applicable to Article 17 of the ICCPR, which prohibits the arbitrary or unlawful interference with privacy rights.

The OHCHR report has neatly summarised these obligations with respect to Article 17 of the ICCPR:

> To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

6 UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/HRC/13/37.

7 UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/23/40.

Legality: No secret laws

The principle of legality is a fundamental aspect of all international human rights instruments and the rule of law. It is a basic guarantee against the state's arbitrary exercise of its powers. For this reason, any restriction on human rights must be prescribed by law. The meaning of "law" implies certain minimum qualitative requirements of clarity, accessibility and predictability. Laws limiting human rights cannot be secret or vague enough to permit arbitrary interference.

On that front, the OHCHR made clear that:

> To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.

The need to meaningfully and publicly explain rights-infringing practices – while important in all contexts – is key to any effective check on communications surveillance, as such practices tend to be surreptitious and difficult to uncover. Given the highly technical and rapidly evolving nature of communications surveillance, it is also incumbent that laws are interpreted publicly and not through secret processes effectively free from public scrutiny. The state must not adopt or implement a surveillance practice without public law defining its limits. Moreover, the law must meet a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of, and can foresee, its application. When citizens are unaware of a law, its interpretation, or the scope of its application, it is effectively secret. A secret law is not a legal limit on human rights.

In her landmark report, UN High Commissioner for Human Rights Navi Pillay made clear that:

> [S]ecret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight.

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.

Under international human rights law, any restriction on our fundamental freedoms must generally pursue a permissible purpose or "legitimate aim." These purposes or aims are often enumerated within the article itself. The Principles therefore require that communications surveillance only be undertaken in pursuit of a predominantly important legal interest. Such interests have been described by Germany's highest court as "the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence."

The OHCHR has similarly affirmed, in its 2014 report, that "any limitation to privacy rights reflected in article 17 of the ICCPR must be necessary for reaching a legitimate aim." The report elaborates:

> Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.

Finally, communications surveillance cannot be employed in a manner that discriminates on the basis of grounds such as race, colour, sex, language, religion or national origin, as such discrimination constitutes an illegitimate purpose.

Necessity, adequacy and proportionality

International human rights law makes clear that any interference with our fundamental freedoms must be "necessary in a democratic society". In its General Comments No. 27, the Human Rights Committee clearly indicates that it is not sufficient that such restrictions serve a legitimate aim, they must also be necessary to it.[8] Restrictive measures must also be adequate or appropriate to achieving their

8 Human Rights Committee, General Comment 27, Freedom of movement (Art. 12), UN Doc CCPR/C/21/Rev.1/Add.9 (1999). www1.umn.edu/humanrts/gencomm/hrcom27.htm

protective function. They must also be the least intrusive options amongst those which might be expected to achieve the desired result, and they must be proportionate to the interest to be protected. Finally, any restrictive measure which undermines the essence or core of a right is inherently disproportionate and a violation of that right.

Applying these foundational principles to the context of communications surveillance, the Principles affirm that:

Necessity: Often, a surveillance objective might be achieved using far less intrusive mechanisms. While it is by no means necessary to exhaust other options, it should be recognised that communications surveillance is inherently invasive and should not be a tool of first recourse.

Adequacy: It is not sufficient to show that a given surveillance practice is necessary for achieving a given objective; it must also be adequate and appropriate to it. As noted by the High Commissioner, at minimum, communications surveillance which interferes with privacy "must be shown to have some chance of achieving [its] goal."

Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights and poses a threat to the foundations of a democratic society. Communications surveillance for investigative purposes, in particular, should only occur once the state has convinced an objective third party – a judge – that a serious threat to a legitimate interest exists and that the communications mechanism in question will yield information that will assist with that serious threat.

No voluntary cooperation: Current digital networks and interactions entrust vast amounts of personal and sensitive data in the hands of a wide range of third party intermediaries, including internet service providers (ISPs), email providers, hosting companies and others. Through their discretionary decisions to comply (or not) with state surveillance requests, these intermediaries can dramatically impact on the privacy rights of all. Such voluntary sharing bypasses due process and poses a serious threat to the rule of law. The Necessary and Proportionate Principles therefore prohibit any state communications surveillance activities in the absence of judicial authorisation.

No repurposing: Contrary to many official statements, the modern reality is that state intelligence agencies are involved in a much broader scope of activities than simply those related to national security or counterterrorism. The Necessary and Proportionate Principles state that communications surveillance (including the collection of information or any interference with access to our data) must be proportionate to the objective they are intended to address. And equally importantly, even where surveillance is justified by one agency for one purpose, the Principles prohibit the unrestricted reuse of this information by other agencies for other purposes.

The OHCHR report also emphasises this point, noting that:

> The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resultant sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant [on Civil and Political Rights], because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.

Integrity of communications and systems

No law should impose security holes in our technology in order to facilitate surveillance. Undermining the security of hundreds of millions of innocent people in order to ensure surveillance capabilities against the very few bad guys is both overbroad and short-sighted, not least because malicious actors can use these exploits as readily as state agents. The assumption underlying such provisions – that no communication can be truly secure – is inherently dangerous, akin to throwing out the baby with the bathwater. It must be rejected.

The OHCHR report supports that conclusion, stating that:

> The enactment of statutory requirements for companies to make their networks "wiretap-ready" is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures.

Notification and right to an effective remedy

Notification must be the norm, not the exception. Individuals should be notified that access to their communications has been authorised with enough time and information to enable them to appeal the decision, except when doing so would endanger the investigation at issue. Individuals should also have access to the materials presented in support of the application for authorisation. The notification principle has become essential in fighting illegal or overreaching surveillance. Any delay in notification has to be based upon a showing to a court, and tied

to an actual danger to the investigation at issue or harm to a person.

Before the internet, the police would knock on a suspect's door, show their warrant, and provide the individual a reason for entering the suspect's home. The person searched could watch the search occur and see whether the information gathered went beyond the scope of the warrant. Electronic surveillance, however, is much more surreptitious. Data can be intercepted or acquired directly from a third party such as Facebook or Twitter without the individual knowing. Therefore, it is often impossible to know that one has been under surveillance, unless the evidence leads to criminal charges. As a result, the innocent are the least likely to discover that their privacy has been invaded. Indeed, new technologies have even enabled covert remote searches of personal computers and other devices.

The OHCHR report lays out four characteristics that effective remedies for surveillance-related privacy violations must display:

> Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored.

The 2014 OHCHR report continues, stressing the importance of a "prompt, thorough and impartial investigation"; a need for remedies to actually be "capable of ending ongoing violations"; and noting that "where human rights violations rise to the level of gross violations, [...] criminal prosecution will be required."

Safeguards for international cooperation

Privacy protections must be consistent across borders at home and abroad. Governments should not bypass national privacy protections by relying on secretive informal data-sharing agreements with foreign states or private international companies. Individuals should not be denied privacy rights simply because they live in another country from the one that is surveilling them. Where data is flowing across borders, the law of the jurisdiction with the greatest privacy protections should apply.

More to be done

The Necessary and Proportionate Principles provide a basic framework for governments to ensure the rule of law, oversight and safeguards. They also call for accountability, with penalties for unlawful access and strong and effective protections for whistleblowers. They are starting to serve as a model for reform around the world and we urge governments, companies, NGOs and activists to use them to structure necessary change.

But while the Principles are aimed at governments, government action is not the only way to combat surveillance overreach. All of the communications companies, internet and telecommunications alike, can help by securing their networks and limiting the information they collect and retain. Online service providers should collect the minimum amount of information for the minimum time that is necessary to perform their operations, and effectively obfuscate, aggregate and delete unneeded user information. This helps them in their compliance burdens as well: if they collect less data, there is less data to hand over to the government. Strong encryption should be adopted throughout the entire communications chain and, where possible, for data in storage.

It is clear that under the cloak of secrecy, malfunctioning oversight and the limited reach of outdated laws, the practice of digital surveillance in countries from the far North to the far South has overrun the bounds of human rights standards. We all hope to see activists around the world showing exactly where a country has crossed the line, and how its own policy makers and the international community might rein it back. We must call for surveillance reform to ensure that our national surveillance laws and practices comply with human rights standards and to ensure that cross-border privacy is in place and effectively enforced. Working together, legal plus technical efforts like deploying encryption, decentralisation of services and limiting information collected, can serve as a foundation for a new era of private and secure digital communications.