GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

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

Global Information Society Watch

2014

APC Hivos

Steering committee
Anriette Esterhuysen (APC)
Loe Schout (Hivos)

Coordinating committee
Monique Doppert (Hivos)
Valeria Betancourt (APC)
Mallory Knodel (APC)

Project coordinator
Roxana Bassi (APC)

Editor
Alan Finlay

Assistant editor, publication production
Lori Nordstrom (APC)

Proofreading
Valerie Dee
Stephanie Wildes

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration
Matías Bervejillo

Financial support provided by
Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch
Published by APC and Hivos
2014

ISSN: 2225-4625
ISBN: 978-92-95102-16-3
APC-201408-CIPP-R-EN-DIGITAL-207

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2014.

Table of contents

Thematic reports

Country reports

The myth of global online surveillance exempted from compliance with human rights

Alberto J. Cerda Silva
University of Chile Law School and ONG Derechos Digitales
www.derecho.uchile.cl, https://www.derechosdigitales.org

Introduction

Since mid-2013 there have been continuing revelations about the implementation by the United States (US) government of a series of programmes that constitute a system for global mass online surveillance. The initiative involves several agencies, primarily led by the National Security Agency (NSA), in close cooperation with companies that provide services through the internet. The system, which mostly targets foreigners and overseas communications, has affected private communications everywhere, from heads of state to ordinary web users.

These revelations about a system for global mass online surveillance have raised human rights concerns. Over time, these concerns have been rejected by suggesting that human rights have no application on the matter because they lack specific norms, have a narrow scope, or are irrelevant to non-state actors. These arguments have built a myth that online cross-border surveillance would be exempted from compliance with human rights law. This report challenges these misconceptions by, first, restating the full application of human rights law over global mass online surveillance and, second, calling attention to the current limitations of human rights law for achieving actual enforcement of human rights worldwide.

Human rights law on surveillance

Throughout the 1990s, there was a belief that the internet was a *laissez-faire* environment exempted from any governmental control, regulation and restriction. This misconception was fuelled by libertarian ideas that overstate the borderlessness, openness and virtual anonymity of the internet.[1] These features, however, rather than preventing any regulatory approach, merely challenge the efficiency of regulations, raising the difficulty of international harmonisation of regulations. Through the years, the internet has become an environment heavily regulated in which several layers of regulation and laws overlap, one of them being international human rights law. In fact, as some recent resolutions by the United Nations make clear, human rights are fully applicable to the online environment.[2]

Although human rights are wholly applicable to the internet, it has been suggested that online surveillance has no implications from a human rights viewpoint, since there is no specific rule on the matter in any international instruments on human rights. This argument, however, rests on a short-sighted and literal interpretation of the law. Those instruments, rather than dealing with specific risks, set forth general rules and principles that must be applied in numerous concrete circumstances. In the particular case of mass online surveillance, it raises concerns related to several rights, such as privacy, due process, protection of personal data, equal protection, and judicial protection, among others.

Ruling that surveillance has implications for human rights does not mean that surveillance should be outlawed, since its practice may be allowed in certain circumstances. On the contrary, it opens an analysis to determine if a given measure of surveillance is in compliance with human rights. In other words, human rights are not absolute and could be subject to certain limitations – and, some practices of surveillance that limit certain human rights could be permissible.

However, countries are not completely free to limit human rights; on the contrary, they must comply with certain rules established by international law on the matter.[3] First, limitations require

1 Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. https://projects.eff.org/~barlow/Declaration-Final.html

2 United Nations General Assembly, Resolution on the promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/20/L.13, 29 June 2012; United Nations Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age, UN Doc. A/RES/68/167 (21 January 2014); and United Nations General Assembly, The promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/26/L.24, (20 June 2014). See also the Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age, UN Doc. A/HRC/27/37, 30 June 2014.

3 Kiss, A. C. (1981). Permissible limitations on rights. In Louis Henkin (Ed.), *The International Bill of Rights: The Covenant on Civil and Political Rights*. New York: Columbia University Press, pp. 290-310.

an enabling law, that is, an act passed by the legislature.[4] Second, limitations must have a legitimate purpose. In fact, human rights could be subject to limitations for several reasons, including national security, public safety and order, as well as public health and morals. According to the Universal Declaration of Human Rights, limitations are permissible "for the purpose of securing due recognition and respect for the rights and freedoms of others."[5] Third, limitations must be proportional, that is, there must be certain balances between the imposed restriction and its attempted purpose.[6] And fourth, when adopting limitations, countries must establish appropriate safeguards to prevent the misuse and abuse of restrictions regarding human rights.

While the US has authorised the NSA's system for global mass online surveillance in domestic law, it fails to meet any other requirement set forth by international human rights law. First, although it seems justified on the grounds of legitimate purpose, international law proscribes any limitation that discriminates arbitrarily, such as those based on distinctions of religion, political or other opinion, and national or social origin, among others.[7] Second, the system does not meet the test of proportionality, since even if adequate for fulfilling its purpose, it is unnecessary because there are less severe means of achieving the intended objective, and it is disproportional because the detrimental effects on human rights of implementing a system for global mass online surveillance exceed its potential benefits. And third, the evidence has shown that the safeguards provided by law, mainly through judicial control in implementing policies, were neither sufficient nor appropriate, since they were completely overcome by the actual implementation of the system.

In sum, although a system for global mass online surveillance, similar to that implemented by the NSA, may be in compliance with a given country's domestic law, it certainly violates international human rights law by arbitrarily discriminating against its target population, by being unnecessary and disproportional, and by lacking appropriate safeguards.

Protection beyond citizenship and territory

Another misconception that has been used to justify mass online surveillance, especially overseas, involves narrowing the scope of human rights law by arguing that it does not provide protection to either foreigners or non-resident subjects. In the case of the NSA's initiative, this argument states that the US Constitution would only recognise the fundamental rights of citizens and, therefore, foreigners would be excluded from protection.[8] As a result, while domestic law provides for some safeguards in favour of nationals (which have proved deficient), they are virtually non-existent for alien citizens. Although this conception may be consistent with domestic law, it runs notoriously short on meeting international human rights law.

Limiting human rights protection to citizens also infringes human rights law. In fact, all international instruments on the matter recognise that these rights belong to everybody, disregarding their nationality or citizenship. As the Universal Declaration of Human Rights states, they are inalienable rights of "all members of the human family" that "human beings shall enjoy."[9] Excepting certain political rights that are attached to citizenship, such as voting and being elected, all other human rights belong to people without permissible exceptions based on being a citizen of a given country. On the contrary, international instruments on human rights law expressly forbid distinctions of any kind, not only based on race, colour, sex or language, but also on religion, political or other opinions, as well as national or social origin, among other statuses.[10]

Related to the argument that attempts to exempt compliance with human rights in the case of surveillance over foreigners, it has been argued that no government is required to guarantee rights other than those of people under its own jurisdiction and, therefore, there is no duty to respect human rights of people overseas. This narrow conception argues that one state cannot be compelled to promote, protect and respect human rights within other states, since this is a primary competence of the state that exercises jurisdiction over the territory. Additionally, this conception rests on

4 Inter-American Court of Human Rights, Advisory Opinion OC-6/86 of 9 May 1986, "Laws" in article 30 of the American Convention on Human Rights, para. 38.

5 Universal Declaration of Human Rights, Article 29 (2).

6 Barak, A. (2012). *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press.

7 American Declaration of the Rights and Duties of Man, articles I and II; Universal Declaration of Human Rights, articles 1 and 2; European Convention on Human Rights, article 14; International Covenant on Civil and Political Rights, article 2; International Covenant on Economic, Social and Cultural Rights, article 2; American Convention on Human Rights, article 1; Charter of Fundamental Rights of the European Union, article 21; and African Charter on Human and Peoples' Rights, article 2.

8 Cole, D. (2003). Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens?, *Thomas Jefferson Law Review*, 25, 367-388.

9 Universal Declaration of Human Rights, Preamble.

10 See note 7.

the literal interpretation of the word "territory", as the physical space under the exclusive control of a given state that forces compliance with human rights law. This argument is, however, deceptive and anachronistic.

Human rights law was created after the Second World War in order to develop binding international laws that would prevent a recurrence of the atrocities experienced. The law was not limited to violations committed by governments against their own nationals in their own territory, but also people from other jurisdictions, sometimes in territories that were not under exclusive control. It is true that a state may not be able to promote and protect human rights in other jurisdictions than its own, but it certainly can (and must) respect those rights by constraining its own officials from violating them on and off its territory. Moreover, in the case of a system of global online surveillance, it is not clear in which country's territory human rights violations take place.

However, the main problem with narrowing the scope of human rights to a physical territorial space is that, in a globalised world with noticeable improvements in transport and communications, one confronts an impermissible loophole from a teleological perspective that looks into the purpose of human rights law rather than the narrower wording of a human rights treaty. The extraterritorial application of human rights is the only one that provides meaning to human rights in the current state of affairs.[11] Even if limited, this extraterritorial effect of international human rights law has been upheld by international courts, as well as domestic courts, such as the United Kingdom courts that recently held liable its soldiers for human rights violations committed against civilians in Afghanistan. A teleological interpretation of human rights obligations is the only one that could make sense in a digital age, in which a violation of those rights could be committed remotely, between one country and another.

Non-state actors' responsibility

Another misconception about the human rights implications of surveillance argues that those rights are only enforceable against state actors, but not against non-state actors and, therefore, private actors spying on people are not subject to human rights scrutiny. This belief is anchored in the fact that international instruments on human rights set forth obligations only on state parties, since they have standing as legal entities before international law. In addition, this argument points out that, although human rights philosophy has been there for a while, international instruments crystallised them as a reaction against the experiences of totalitarian states that led to the horrors of the Second World War, in which governments infringed their own citizens' rights. In this view, preventing violations committed by private parties is not a matter of concern for international human rights law, but an issue left to the discretion of each country's domestic law. This argument is, however, misleading.

Although international instruments on human rights primarily set forth obligations on states, they have at the very least indirect effects on non-state actors, such as corporations involved in surveillance. In fact, those instruments demand that states not only respect but also promote and protect human rights.[12] Because of this, in addition to restraining states from violating human rights, international law imposes on states a duty to encourage and to safeguard those rights from infringing actions of third parties. As a matter of fact, case law by human rights courts has made explicit that the state is not only responsible for its own actions, but also for failing to protect those rights when violations are committed by non-state actors, such as paramilitary forces.[13] It follows, naturally, that since the state is internationally responsible for human rights, even if non-state actors violate them, the state has a duty to enforce those rights against infringing non-state actors in domestic law. Therefore, the state must take actions in order to prevent human rights violations by both state and non-state actors.

In order to comply with the obligation of ensuring that surveillance does not infringe on the right to privacy, as well as other human rights, countries have adopted diverse paths. Some countries have prevented illegal surveillance by: adopting laws that regulate in detail the processing of personal

11 United Nations Human Rights Committee, General Comment No. 31 [80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004), para. 10. See also: Moreno-Lax, V., & Costello, C. (2014). The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territory to Facticity, the Effectiveness Model. In S. Peers, T. Hervey, J. Kenner, & A. Ward (Eds.), *The EU Charter of Fundamental Rights: A Commentary*. Oxford: Hart Publishing, pp. 1657-1683; and Grabenwarter, C. (2014). *European Convention on Human Rights: Commentary*. Oxford: Beck/Hart.

12 United Nations Human Rights Committee, General Comment No. 31 [80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004), paras. 1-8.

13 Inter-American Court of Human Rights, Velasquez Rodriguez Case (Series C) No. 4, para. 172, 29 July 1988.

information by state and non-state actors; regulating the commercialisation of dual-use technology (i.e. goods that can be used for both legitimate and illegitimate purposes, such as spyware and communication intercepting devices); rejecting any evidence obtained that infracted on human rights, such as the illegal interception of communications; and punishing the most outrageous acts of intrusions on privacy. This legislative approach provides a certain level of legal certainty, but has some limitations, mainly the fact that it does not grant comprehensive protection.

Countries with a modern constitutional framework have adopted a different path for protecting human rights in domestic forums. They have incorporated international instruments on human rights into their domestic constitutions and made those rights enforceable against both state and non-state actors. This is the case in Latin American countries, in which there are a number of court decisions based on constitutional grounds that nullify data retention laws, grant privacy in online communications, prevent rights-abusive processing of personal data, and limit video surveillance to proportional circumstances. This constitutional protection of human rights grants comprehensiveness, although it is usually followed by legislative acts that detail concrete implications in more complex cases.

The internet has become crucial for our lives, and it will be even more important as more people connect, accessing more services, and for longer periods of time. The internet is, however, an environment essentially controlled by private actors: from entities that assign technical sources[14] to those that adopt technical standards, from those that provide the backbones and telecommunication services, to those that offer access and content. The fact that the internet is under private control should not be an excuse for preventing the realisation of human rights in the online environment and, therefore, states are required to promote and protect human rights against the abuse of non-state actors. This does not prevent the adoption of an international instrument on corporate human rights responsibility, particularly for cases in which a government cannot or does not want to enforce this through domestic remedies.[15]

The actual problem: Human rights enforcement

International human rights law provides rules applicable to a system for global mass online surveillance. What the case of the NSA shows, instead, is a different problem in current international law. There is a loophole in the enforcement of human rights with respect to those recalcitrant countries that fail to adjust their domestic laws and policy measures to human rights standards.[16] Domestic mechanisms of enforcement may help, if available, but they are insufficient when resolving issues based on mere parochial law standards, or a narrow-minded legal approach. There are certain mechanisms available in international forums, but they tend to be political rather than legal in nature. Unfortunately, in the case of the NSA, the US has not recognised the jurisdiction of any international courts. Therefore, it seems unfeasible that any legally binding decision on the matter of whether a system for global mass online surveillance violates international human rights law will be made.

14 Such as IP addresses and domain names.

15 United Nations General Assembly, Resolution on elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights, UN Doc. A/HRC/26/L.22/Rev.1, 25 June 2014.

16 Louis Henkin, International Human Rights Standards in National Law: The Jurisprudence of the United States, in Benedetto Conforti and Francesco Francioni (eds.), Enforcing International Human Rights in Domestic Courts (Martinus Nijhoff Publishers, 1997), pp. 189-205.