NECESSARY & PROPORTIONATE

International Principles
on
the Application of Human Rights Law
to
Communications Surveillance

Background and Supporting International Legal Analysis

May 2014

Table of Contents

INTRODUCTION 1

SCOPE: EXTRA-TERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES 2

DEFINITIONS: "PROTECTED INFORMATION" & "COMMUNICATIONS SURVEILLANCE" 7

PROTECTED INFORMATION 8

COMMUNICATIONS SURVEILLANCE 13

PRINCIPLE BY PRINCIPLE EXPLANATION 13

Principle 1: LEGALITY 14

Principle 2: LEGITIMATE AIM 18

Principles 3, 4, and 5: NECESSITY, ADEQUACY, & PROPORTIONALITY 20

Principles 6 and 7: COMPETENT JUDICIAL AUTHORITY & DUE PROCESS 22

Principle 8: USER-NOTIFICATION & THE RIGHT TO AN EFFECTIVE REMEDY 25

Principles 9 & 10: TRANSPARENCY & PUBLIC OVERSIGHT 27

Principle 11: INTEGRITY OF COMMUNICATIONS & SYSTEMS 28

Principle 12: SAFEGUARDS FOR INTERNATIONAL COOPERATION 29

Principle 13: SAFEGUARDS AGAINST ILLEGITIMATE ACCESS 31

INTRODUCTION

We live in an era where rapid developments in the economics and capabilities of digital surveillance prompt an array of challenges to many of our most dearly held human rights:

- How might we preserve privacy when governments around the world can, and often do, inexpensively and invisibly collect and analyse every citizen's interactions—even down to their address books, documents, and conversations—with family, friends, and colleagues?
- What freedom of association might remain when the second-by-second communications and physical locations of entire populations are harvested and stored from data emitted by mobile phones?
- How might true freedom of expression and opinion persist when every time we watch a challenging news item, read a controversial document, or browse a notorious author's work, a digital record is made—itself to be watched, read, and browsed by the machinery, algorithms, and agents of the state?

Above all, how will our human rights be preserved in the digital age when so many of our everyday actions, political activities, and communications now emit a continuous stream of revealing information, with few legal or technological constraints on monitoring, gathering, analysis, and use against us by the government?

These questions and ongoing concerns arising from surveillance techniques were the jumping off point for the drafting of the International Principles on the Application of Human Rights to Communication Surveillance that explain how international human rights law applies in the context of communication surveillance.[1] The principles are therefore firmly rooted in established international human rights law and jurisprudence. The more recent string of Snowden revelations have demonstrated precisely how far human rights can be eroded if technologically-driven challenges are not addressed.

The main purpose of what became the *13 Necessary and Proportionate Principles* (hereafter "the Principles")[2] was to provide civil society groups, states, the courts, legislative and regulatory bodies, industry, and others with a framework to evaluate whether current or proposed surveillance laws and practices around the world are compatible with human rights. In the post-Snowden era, the urgent need to revise and adopt national surveillance laws and practices that comply with the Principles and to ensure cross-border privacy protections has become clear.

---

[1] For more details about the consultation process, *see* Privacy International, *Towards International Principles on Communications Surveillance,* referencing a meeting of experts in Brussels in October 2012, 21 November 2012, available at: https://www.privacyinternational.org/blog/towards-international-principles-on-communications-surveillance. This was followed by a meeting organised by the Electronic Frontier Foundation in Rio de Janeiro, Brazil in December 2012, with the participation of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue: *see* UN Document A/HRC/23/40, at para. 10. Electronic Frontier Foundation, Privacy International, and Access launched a global consultation that ended in January 2013, and we, along with several NGOs, criminal attorneys, human rights advocates, and privacy advocates worked on revising the text until July 2013.

[2] The full text of the International Principles on the Application of Human Rights to Communication Surveillance is available at: https://en.necessaryandproportionate.org/text.

At the same time, one of the major concerns driving the Principles was to keep the application of the law up-to-date with the latest technological developments and to ensure that key protections built up over many years in the pre-digital era would remain strong. It is inevitable that established human rights law does not deal precisely with changes in technology over time. Our aim was to identify key principles that support robust protection of actual human rights in a digital age. For this reason, not all of the specific approaches we suggest have been formally or explicitly endorsed by international bodies for the protection of human rights.

The Principles have been signed by 400 organizations and 300,000 individuals throughout the world, and endorsed by the UK's Liberal Democratic Conference, as well as European, Canadian, and German Parliamentarians.[3] The Principles have been cited by the United States' President Review Group on Intelligence and Communications Technologies report,[4] the Inter-American Commission on Human Rights report,[5] and others.[6]

In this document, the Electronic Frontier Foundation and ARTICLE 19 explain the legal or conceptual basis for the specific Principles.[7] Our paper is divided into three parts. Part one addresses questions relating to the Principles' scope of application. Part two introduces key definitions and concepts, namely the concept of "protected information" in contrast with traditional categorical approaches to data protection and privacy and a definition of "communications surveillance." Part three explains the legal and conceptual basis of each Principle. It begins by setting out the basic human rights framework underpinning the rights to privacy, freedom of expression, and freedom of association. It then elaborates on the legal underpinning for each of the Principles with reference to the case law and views of a range of international human rights bodies and experts, such as UN special rapporteurs. We try to be clear about when our conclusions are based on firmly established law, and when we are suggesting new specific practices based on principles fundamental to human rights.

SCOPE: EXTRA-TERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES

One of the most disturbing aspects of the Snowden revelations was the extent of cooperation and intelligence-sharing between the NSA, GCHQ, and other Five Eyes partners, in which material gathered under one country's surveillance regime was readily shared with the others. Together, each of the Five Eyes (United States, United Kingdom, Canada, Australia, and New Zealand) are strategically located to spy on much of the world's

[3] The full list of signatories is available at: https://en.necessaryandproportionate.org/signatories.

[4] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World,* December 12, 2013, footnote 120, available at: http://whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[5] Annual Report of the Inter-American Commission on Human Rights, December 31, 2014, available at: http://www.oas.org/en/iachr/docs/annual/2013/informes/LE2013-eng.pdf.

[6] Necessary and Proportionate, News, available at: https://en.necessaryandproportionate.org/news.

[7] We are very grateful to everyone who has assisted us with the research and drafting of this document. In particular we thank Douwe Korff, Professor of International Human Rights Law, for preparing an earlier version of the paper and Cindy Cohn, Gabrielle Guillemin, Tamir Israel, Dr. Eric Metcalfe, and Katitza Rodriguez for their subsequent contribution. A word of special thanks also goes to Access, Privacy International, Asociación por los Derechos Civiles, Comisión Colombiana de Juristas, Fundación Karisma, Human Rights Information and Documentation System – HURIDOCS, The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, and Open Net Korea for reviewing and sharing background resources. While we attempted a broad consultation, we would especially welcome additional input from experts in the relevant African and Eastern European law, both national and regional bodies, which were not as strongly represented in this first version of the paper.

communications as they transit through or are stored in their various respective territories. The foreign intelligence agencies of these nations have constructed a web of inter-operability at the technical and operational levels that spans the global communications network. In addition, non-Five Eyes intelligence-sharing arrangements exist, as well as broader cooperation—between primarily law enforcement agencies—through more formalised arrangements, including the Mutual Legal Assistance Treaties (MLATs).

International cooperation between governments also raises questions as to how and when states may be liable under national and international law for their surveillance activities, which may have an impact far beyond their own borders. One issue is the extent to which states can be "extraterritorially" accountable for their human rights violations overseas, *e.g.* the surveillance of private communications in other countries. It is important to bear in mind, however, that current technology makes it possible for states to monitor a great deal of international traffic from within the confines of their own borders. It is therefore important to refer briefly to the issue of jurisdiction under international human rights law and the different ways that a state may be held responsible for its actions, even where the effects are felt beyond its borders.[8] Our discussion of Principle 12, below, provides further examination of this issue within the specific context of MLATs.

A core problem arises when overly narrow territorial limitations on human rights protections are relied upon, as these rapidly become meaningless when applied to highly integrated global communications networks. Historically, practical limitations heavily impeded the extent to which a government could operate to clandestinely access the communications of individuals in another country. Where this could occur, affected individuals could theoretically rely on the protections of their home state as such surveillance activities would necessarily require intrusion on another state's sovereignty and violation of its domestic laws. However, the nature of digital networks, which rely on borderless routing and storage for their efficiency and robustness, permits states to intercept vast amounts of foreign information from the comfort of their territorial homes. Accompanying this new technical capacity is a post-9/11 shift in focus that places all individuals—as opposed to foreign powers and states—at the focus of the formidable surveillance powers and resources of foreign intelligence agencies. The combination of these factors has led to a situation where the privacy rights of foreigners are frequently invaded to significant and substantial degrees by foreign intelligence agencies.[9] Finally, whereas foreign intelligence agencies are often provided with significant latitude to spy on

[8] For a more in-depth academic analysis and more extensive references to the case law of the Human Rights Committee and other sources, *see* Martin Scheinin & Mathias Vermeulen, "Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism," section 3.7 in *Denial of Extraterritorial Effect of Human Rights (Treaties)*, available at: http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf.

[9] For an example see: G. Greenwald & E. MacAskill, "Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data," The Guardian, June 11, 2013, available at: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining; The NSA is perhaps the clearest example of the scope and breadth at which a foreign intelligence agency can leverage interconnected networks to spy on individuals around the world. However, many of its Five Eyes partners are strategically located to supplement the NSA's reach with information transiting (or stored in) their own reach. For example, *see*: N. Hopkins, "Theresa May Warns Yahoo That Its Move to Dublin is a Security Worry," March 20, 2014, The Guardian, available at: http://www.theguardian.com/technology/2014/mar/20/theresa-may-yahoo-dublin-security-worry.

the communications of foreigners,[10] the highly integrated nature of communications networks has led many of these agencies to sweep up all data indiscriminately, citing difficulties between distinguishing foreign and domestic communications as a justification.[11]

In summary, governments may carry out surveillance both within and beyond their own borders. However, the domestic legal framework of most countries typically gives much greater protection to the privacy rights of citizens as opposed to non-citizens and non-residents. As a result, many governments routinely engage in bulk surveillance of international communications with very little regard for the privacy of those communications, possibly in the mistaken belief that their legal obligations only extend as far as their own citizens or residents. Even more problematically, it appears that countries seek intelligence-sharing arrangements with other countries in order to obtain surveillance material concerning their own citizens that they could not obtain under their domestic legal framework. However, as elaborated below, the enjoyment of fundamental rights is not limited to citizens of particular states but includes all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers, and other persons who may find themselves in a territory or subject to the jurisdiction of a State.[12] In addition, all persons are also equal before the law and consequently, they are entitled, without discrimination, to equal protection of the law.[13]

---

[10] Privacy International, "Eyes Wide Open", Version 1.0, 2013, available at: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf.

[11] *See, e.g*., S. Ackerman & J. Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ," The Guardian, February 28, 2014, available at: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo: "Programs like Optic Nerve, which collect information in bulk from largely anonymous user IDs, are unable to filter out information from UK or US citizens."; John Foster, Chief, Communications Security Establishment Canada (CSEC), Testimony to the Standing Senate Committee on National Security and Defence, 41st Parliament, 2nd Session, 2013-14, February 3, 2014, available at: http://www.parl.gc.ca/content/sen/committee/412/SECD/pdf/02issue.pdf, p. 2-71: "We will keep the metadata because as communications go over networks, foreign communications and Canadian are all mixed up together...When you collect metadata, it is impossible. It is all intermixed together, and good citizens and terrorists all are using the same networks. So when we collect it, we have no way of knowing at that point of disaggregating it until we look at it, and then we use it."

[12] UN Human Rights Committee (HRC), General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, 26 May 2004, CCPR/C/21/Rev.1/Add.13, available at: http://www.refworld.org/docid/478b26ae2.html [accessed 30 April 2014]

[13] For instance, pursuant to the Inter-American Convention on Human Rights, states must: "230. [A]bstain from engaging in actions or favouring practices that may in any way be aimed, directly or indirectly, at creating situations in which certain groups or persons are discriminated against or arbitrarily excluded, de iure or de facto, from enjoying or exercising the right to freedom of expression. Likewise, states must adopt affirmative measures (legislative, administrative, or in any other nature), in a condition of equality and non-discrimination, to reverse or change existing discriminatory situations that may compromise certain groups' effective enjoyment and exercise of the right to freedom of expression. This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained," See IACHR. Annual Report 2008. Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter III (Inter-American Legal Framework of the Right to Freedom of Expression). OEA/Ser.L/V/II.134 Doc. 5 rev. 1. 25 February 2009. para. 230, available at: http://cidh.oas.org/annualrep/2008eng/Annual%20Report%202008-%20RELE%20-%20version%20final.pdf. *See also* Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. OAS official records; OEA/Ser.L. OEA/Ser.L/V/II CIDH/RELE/INF.11/13, 31 December 2013, page 8, available at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.

In light of this, the Preamble to the Principles, in the Scope of Application section, expressly provides that the Principles "apply to surveillance conducted within a State or extraterritorially." This reflects the requirement under international human rights law that states must respect the rights of all persons without distinction or discrimination, either to "everyone within their territory or jurisdiction" or simply "within their jurisdiction" or "subject to their jurisdiction."[14]

It is important to be clear, however, that the obligation of states to respect the rights of persons within their "jurisdiction" is not limited to the rights of persons physically in their territory. In the case of *Bosphorus v. Ireland*,[15] for instance, the European Court of Human Rights held that the Irish government's decision to impound a plane in Dublin that belonged to a Turkish company was sufficient to bring the Turkish company within the jurisdiction of the Republic of Ireland for the purposes of the proceedings.

The same principle has also been applied in cases involving surveillance. In the 2008 case of *Liberty and others v. United Kingdom*,[16] two Irish NGOs had complained about the monitoring of their private communications by the British government by way of its Electronic Test Facility at Capenhurst in Cheshire, England—a facility able to monitor 10,000 simultaneous conversations between Ireland and Europe. In that case, the Grand Chamber of the ECHR found a violation of the Irish NGO's right to privacy under Article 8 ECHR notwithstanding that neither of the NGOs were physically present in the territory of the United Kingdom. In an earlier admissibility decision in *Weber and Savaria v. Germany*,[17] the ECHR was similarly prepared to consider the complaints of two residents of Uruguay against monitoring of their telecommunications by the German government.[18]

The common thread in each of these cases is that the surveillance in question was being carried out *within* the territory of the state in question, even if the subjects of the surveillance were not. The duty owed by the state under international human rights law to respect the rights of all persons within their territory or jurisdiction therefore *includes* persons physically outside the state but whose rights are interfered with by the state's actions within its borders.

It is also important to bear in mind that territorial jurisdiction may arise not only on the basis of the physical location of where the surveillance of the private communication took place, but also where the data was *processed*. In other words, even if the British

[14] International Covenant on Civil and Political Rights ("ICCPR"), Art. 2(1), United Nations General Assembly Resolution 2200A (XXI), Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, Rome, 4.XI.1950, ("European Convention on Human Rights" or "ECHR"), Art. 1; American Convention on Human Rights, OAS Treaty Series No. 36, November 22, 1969, ("IACHR"), Art. 1.1. The African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) ("ACH&PR") instead stipulates that "*The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Chapter and shall undertake to adopt legislative or other measures to give effect to them*" (Art. 1).

[15] (2005) 42 EHRR 1.

[16] (2009) 48 EHRR 1.

[17] No. 54934/00, 29 June 2006.

[18] The German government had argued that the application was incompatible *ratione personae* on the basis that the "monitoring of telecommunications made from abroad" was an "extraterritorial act" and therefore outside Germany's jurisdiction under Article 1 ECHR. The ECHR, however, declined to strike out the application on this basis (*see* para. 72 of the decision) although it did ultimately strike out the application on other grounds.

government had captured the private phone calls of the Irish NGOs from a facility located *outside* the United Kingdom, for example, its territorial jurisdiction would still be engaged if the data from the phone calls were processed by government agencies *inside* the UK.

Even if the surveillance was carried out by the state outside its own territory, however, it would still be responsible for violations of human rights in those places where it had authority or effective control. As the UN Human Rights Committee held in *Lopez Burgos v. Uruguay* and *Celiberti de Casariego v. Uruguay*:[19]

> States Parties are required by Article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State Party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.

The European Court of Human Rights has similarly held that:[20]

> ...In exceptional circumstances the acts of Contracting States performed outside their territory or which produce effects there ("extra-territorial act") may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention.

Some governments, most notably the US and Israel, have denied that their obligations under the ICCPR extend to responsibility for actions undertaken outside their territory.[21] In the context of the discussions on the Draft UN General Assembly Resolution on *Privacy in the Digital Age*—submitted in response to the Snowden revelations—a briefing note was leaked that confirmed that the USA continues to take the position that it is not under any legal duty to comply with Article 17 ICCPR (privacy) outside its own geographical territory. Indeed, it considered this to be a "redline" which it will not cross. Its very first instruction was that the US negotiators should:[22]

> Clarify that references to privacy rights are referring explicitly to States' obligations under ICCPR and *remove suggestion that such obligations apply extra-territorially.* [Emphasis added]

The position of the United States regarding the inapplicability of the Covenant to its extraterritorial activities was harshly criticised by the UN Human Rights Committee at its 110th session.[23] As the Committee remarked:

> "Would the delegation recognize that the United States' position on extraterritorial activities allowed the United States to commit violations everywhere except in their own territory? The non-applicability of the Covenant to extraterritorial activities led

[19] Case nos. 52/1979 and 56/1979, both of 29 July 1981, at §§ 12.3 and 10.3 respectively. *See also* the Committee's Concluding Observations on the reports by Israel in 1998 and 2003, mentioned in Scheinin and Vermeulen, o.c. (footnote 8, above), p. 37, footnote 81. *See also* General Comment 31, para. 10.

[20] ECHR, *Issa and Others v. Turkey*, judgment of 16 November 2004, final since 30 March 2005, para. 68.

[21] *See* 2006 Concluding Observations of the UNHRC on the USA report under the ICCPR; CCPR/C/USA/CO/3, para.10; and the 2011 report of the US to the UNHRC at CCPR/C/USA/4, para. 505.

[22] Right to Privacy in the Digital Age – U.S. Redlines, available at: http://columlynch.tumblr.com/post/67588682409/right-to-privacy-in-the-digital-age-u-s.

[23] Human Rights Committee considers report of the United States, 14 March 2014, available at: http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E.

> to impunity and rights violations. If all Statess were to share that interpretation, there would be no protection of rights at all."

As is clear from the discussion above, this retrograde US view of its obligations under the ICCPR is plainly at odds with international human rights law.[24] This was recognized by the United Nations General Assembly, which ultimately rejected the suggested US redlines and explicitly acknowledged in a recital that extra-territorial surveillance raises human rights concerns:

> Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights;[25]

Whether as a matter of extra-territorial jurisdiction or by way of a straightforward application of the principles of territorial jurisdiction, it is clear that states cannot evade their obligation to respect the privacy of communications by reference to either the nationality of the participants or their physical location. For this reason, the Principles make explicit the need of states to act in a non-discriminatory manner, without regard to such factors as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status.

DEFINITIONS: "PROTECTED INFORMATION" & "COMMUNICATIONS SURVEILLANCE"

The Principles address two core definitional issues that have raised specific challenges in the application of human rights protections to technologically advanced communications surveillance. The first relates to what types of information are protected. There has been a tendency in state surveillance practices to treat certain types of data as less worthy of protection, based on artificial analogies that predate the advent of digital networks in spite of the highly revealing and sensitive nature of the data. The Principles address this by defining "protected information" to include these categories of information and properly recognize the human rights implications that arise when they are interfered with. Secondly, technological developments have allowed state entities to monitor, analyze, collect, and store mass amounts of information indefinitely. Since these activities can be conducted without an individual "looking" at specific information directly, some have argued that no or limited privacy interests are engaged. However, these surveillance activities dramatically impact the privacy of individuals and, in effect, make significant amounts of information available that would not otherwise have been. Moreover, the legal premise for these distinctions is dubious. As such, the Principles define "communications surveillance" broadly to encompass a broad range of activity that implicates the privacy and expressive value inherent in communications networks.

---

[24] For more information, *see* Electronic Frontier Foundation and Human Rights Watch, "Joint Submission to the Human Rights Committee," 14 February 2014, available at: https://www.eff.org/files/2014/03/10/hrweffsubmission_on_privacy_us_ccpr_final.pdf.

[25] United Nations General Assembly, "The Right to Privacy in the Digital Age," November 2013, A/C.3/68/L.45, http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf.

PROTECTED INFORMATION

In just a few years, communications technology has undergone unprecedented changes, as has the use of those technologies by people around the world. At the same time, much of the existing legislation and case law dealing with safeguards against intrusive surveillance were developed several decades ago—in the days when telephone calls were still operated by pulse dialling and personal computers were a rarity.

Instead of maintaining out-dated concepts and categories from a pre-digital era, the Principles have been drafted to reflect the way in which data is now routinely stored and shared by both public and private bodies, and to provide a level of protection that matches the reality of the harms that can result when data is improperly accessed by the State.

In particular, 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.

While courts have recently begun resisting this approach, there has been a long-standing distinction in North American, European, and some Asian and Latin American laws between the "content" of a message (the actual message), the "communications data" or "metadata" (such as information about who sent a message to whom and when or where the message was sent),[26] and "subscriber data" (data regarding the owner of an account involved in a communication).[27] Following this distinction, North American, European, and some Asian

[26] "Communications data" (or "communications records") can further be broken down into different categories, *e.g.*, "subscriber data" and "traffic data." Note that "metadata" is more often used in US case law whereas Latin American, UK, and European law have more often referred to "communications data" (which has a statutory definition in the UK under section 21(4) of the Regulation of Investigatory Powers Act (RIPA)). However, the term "metadata" is now increasingly used in the UK and Europe as well: *see*, *e.g.*, Practice Direction 31B of the Civil Procedure Rules in England and Wales which defines metadata as "data about data;" or the INSPIRE Metadata Regulation (EC) No 1205/2008 of 3 December 2008. Sir David Omand, the former head of GCHQ, has publicly criticised the suggestion that "metadata," as it is used in US law, is equivalent to the definition of "communications data" under RIPA. However, in current proceedings before the Investigatory Powers Tribunal concerning PRISM and TEMPORA, the UK government has not suggested that there is any information covered by the term "metadata" which is not also covered by the statutory definition of "communications data."

[27] In Korea, for example, "communication data" or "metadata" thus defined will include "communications records" accessible by the police only through court approval under the Communications Secrecy Protection Act, and "communication data," available to the police within the service providers' discretion under the Telecommunications Business Act, is in fact the subscriber information provided upon enrolling into the telecommunication services. The Canadian *Criminal Code* prohibits the interception of private communications, which has been generally interpreted as applying to content, not metadata (or "transmission data"). Transmission information is constitutionally protected and typically requires some form of judicial authorization. The Canadian government attempted to introduce a new "subscriber information" category in legislation which would have obligated telecommunications companies to disclose such information upon request from various state agencies however this legislation failed to pass (M. Geist, "Lawful Access is Dead (For Now): Government Kills Bill C-30," 12 February 2013, available at:

and Latin American laws have traditionally afforded the *content* of a person's communication much greater protection from interference than any data relating to that communication. Unsurprisingly, this distinction was based on the traditional model of the postal service, which distinguishes between the information written on the envelope and the contents of the envelope (indeed, "envelope data" is a frequent synonym for "communications data" or "metadata"). This old-fashioned distinction is, however, frequently rendered meaningless by modern interception methods; unlike conventional postal mail; for example, the interception of e-mail involves making both the content and the metadata instantly accessible to the agency carrying out the interception. Moreover, metadata is now stored in digital formats by service providers and can be acquired *en masse* through production orders in ways that had no postal service equivalent.[28] Additionally, there is no "postal" comparator for the significant amount of anonymous online activity that can be linked to an individual when subscriber information is revealed to the state.[29]

These distinctions were adopted as a kind of rough proxy for privacy—the idea that merely knowing who a single envelope went to at a single point of time was not as revealing as the content of the letter. Yet, the increasing wealth of metadata, and the techniques for aggregating and analysing it, means that even "mere metadata" is capable of revealing far more about an individual's activities or thoughts than was the case thirty or forty years ago. This is due in part to the increasing amount and scope of data collected: In the early 1980s, for instance, when the European Court of Human Rights first heard a complaint about the use of phone metering[30] to collect details of a suspect's telephone calls, the only information that was recorded was the telephone numbers called and the length of the phone calls. In the present day, state agencies seek to collect not only the identities of the callers, but also their billing data, addresses, credit card details, the make and model of the phones used, and geo-location data of their physical movements. In the case of Internet browsing, a simple URL typed into an Internet browser (which would constitute "metadata"

---

http://www.michaelgeist.ca/content/view/6782/125/. United States law also recognized a "subscriber information" category in, for example, its National Security Letter regime, which authorizes the Federal Bureau of Investigations to compel communications providers to identify customers (disclose name, address, length of service, and billing info): D. Doyle, "National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background," Congressional Research Service, 3 January 2014, available at: https://www.fas.org/sgp/crs/intel/RS22406.pdf.

[28] For example the US National Security Agency has been collecting *all* metadata of *all* telephone calls from US telephone companies under regularly-renewed production orders issued by the Foreign Intelligence Surveillance Court (FISC). For a description of the program *see*: Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," 23 January 2014, pp. 8-10. In response to privacy concerns, President Obama recently announced the impending closure of the NSA metadata acquisition program: C. Savage, "Obama to Call for End to N.S.A.'s Bulk Data Collection," 24 March 2014, New York Times, available at: http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html; A comparable program encompassed the periodic production of all *Internet* metadata as well at an earlier point, but was discontinued in 2011: G. Greenwald & S. Ackerman, "NSA Collected US Email Records in Bulk for More than Two Years under Obama," 27 June 2013, The Guardian, available at: http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

[29] D. Gilbert, I.R. Kerr & J. McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunication Providers," [2006] 51 *Crim. L. Quart.* 469, available at: http://iankerr.ca/wp-content/uploads/2011/08/the_medium_and_the_message.pdf.

[30] The equivalent of a "pen register" in United States law or "number recorders" in some other jurisdictions.

rather than content in certain jurisdictions),[31] can easily be as revealing—and sometimes even more revealing—than the actual content of the webpage.[32] Likewise, identifying the owner of an IP address, mobile device identifier or an email's IP address, a mobile subscriber identifier (IMSE), or an email address can be highly revealing in an ecosystem where individuals leave their electronic footprints behind in all their digital interactions. In this way, metadata can be a "proxy for content."[33] In addition, people simply use communications technologies more often today than they did when most communications were via paper letters. Finally, and equally as important, the government's ability to gather much more of this data, over a longer period of time, and organise this data using modern surveillance techniques allows an intimate portrait of a person's life to be quickly and easily created from simple metadata.

The relative lack of protection afforded to a person's metadata historically is particularly evident under US constitutional law—although more recently courts in the United States and elsewhere are increasingly recognizing the inapplicability of this distinction to modern communications. Although the Fourth Amendment protects the *content* of a person's communications with others,[34] and while no definitive decision has yet been reached by the courts with regard to mass surveillance like that at issue in post-9/11 NSA practices, US courts have held that no Fourth Amendment protection applies to information that a person "voluntarily" shares with others (the so-called "third party doctrine"), including the details of their phone records held by the phone company:[35]

> Telephone users...typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbour any general expectation that the numbers they dial will remain secret.

---

[31] *See* Peter Sommer, *Can we separate "comms data" and "content"—and what will it cost?*, presentation at the 2012 "Scrambling for Safety" event, available at: http://www.scramblingforsafety.org/2012/sf2012_sommer_commsdata_content.pdf.

[32] Similarly, the Article 29 Working Party has said "*It is also particularly important to note that metadata often yield information more easily than the actual contents of our communications do,*" *see* Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014, WP215 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

[33] *See* Declaration of Professor Edward Felten, former Chief Technologist at the US Federal Trade Commission, in ongoing litigation brought in the US by the American Civil Liberties Union (ACLU) in relation to the Snowden revelations, available at: https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26 ACLU PI Brief - Declaration - Felten.pdf. *See also,* Amici Curiae Brief of Experts in Computer and Data Science in Support of Appellants and Reversal in ACLU v. Clapper, 2nd Circuit appeal, available at: https://www.eff.org/document/computer-scientists-amicus-aclu-v-clapper.

[34] *See*, *e.g.*, *Katz v. United States,* 389 U.S. 347 (1967), in which the US Supreme Court held that FBI monitoring of phone calls made from a phone booth amounted to a 'search' under the Fourth Amendment.

[35] *Smith v. Maryland*, 442 U.S. 735, 744 (1979**).** As described further below, while the constitutional protection is lacking in the U.S., some statutory protections exist under U.S. law for information in the hands of third parties, even metadata, such as the pen register/trap and trace statutes. They are insufficient under the "necessary and proportionate" principles, however, since the court issues an order based only on a showing of "relevance" to an investigation. *See* 8 U.S. Code 3123 (for prospective transactional data) and 18 U.S. Code 2703 (c), (d) (for stored information on the communications that already have taken place).

With each subsequent advance in communications technology, the conclusion of the US courts that there is no expectation of privacy in phone records has been extended to other forms of communications. In the 2008 case of *United States v. Forrester*, 512 F.3d 500, for instance, the Ninth Circuit Court of Appeals held that:

> e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.

In the recent Supreme Court case of *United States v. Jones*, 132 S. Ct. 949 (2012), however, Justice Sotomayor seemed to be willing to consider changing this approach. As she put it, with references to other cases:

> 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. *See Smith*, 442 U. S. at 749 ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."); *see also Katz*, 389 U. S. at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

This view has not yet been adopted by the Supreme Court, since the *Jones* case was decided on other grounds. It was, however, also recently questioned by the United States President's Review Group in its report on Intelligence Communications Technologies.[36]

As US courts have yet to recognize constitutional protections, metadata is currently protected primarily through legislative regimes such as the Pen Register Statute,[37] which affords such data less protection than "content." This, in turn, has inspired similar statutes in other countries, such as in Korea where acquisition of metadata is conditioned upon court approval.[38]

In contrast, the European Court of Human Rights has recognised communications data as "an integral element" of a private communication and therefore enjoys a degree of protection under the right to privacy under Article 8 of the European Convention on Human Rights (ECHR), albeit less than that afforded to the content of a communication.[39] Other kinds of personal data (including non-communications data) are also afforded protection under European data protection legislation[40] and Article 8 of the EU Charter of Fundamental

---

[36] President's Review Group, "Liberty and Security in a Changing World," December 2013 at page 121, citing the Principles, available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[37] 18 U.S. Code 3123 (for prospective transactional data) and 18 U.S. Code 2703 (c), (d) (for stored information on the communications that already have taken place).

[38] Korea's Communication Secrecy Protection Act, Article 13, available at: http://elaw.kiri.re.kr/en_service/lawPrint.do?hseq=21696.

[39] *See*, *e.g.*, *Malone v. United Kingdom* (1985) 7 EHRR 14 at para. 84.

[40] *See,* in particular, Article 29 Working Party, *Opinion 4/2007 on the concept of "personal data,"* 20 June 2007, WP136, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf. *See also* Article 29 Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and*

Rights specifically provides that everyone has the right to the protection of his or her personal data, which should, in principle, extend to metadata and subscriber information. Encouragingly, the Grand Chamber of the Court of Justice of the European Union very recently rejected the argument that "metadata" should attract less protection than the "content" of communications within the context of Article 7 of the EU Charter of Fundamental Rights.[41] At the same time, it is clear that the European law in this area also suffers from some serious problems: first, as noted above, the longstanding distinction between metadata or communications data, on the one hand, and the content of communications, on the other, is being eroded by technological changes; second, it is unclear to what extent the protections afforded to communications data under Article 8 ECHR, and that provided to other kinds of personal data under data protection legislation, overlap with one another. This is particularly problematic, given that European human rights law and EU data protection law are each capable of protecting the same information in very different ways, and are subject to very different exceptions.[42]

In light of these problems, it is clear that existing distinctions between metadata and content are no longer sound and that a fresh approach is necessary in order to protect individual privacy in a digital age. The Principles therefore proceed on the basis that all information relating to a person's private communications should be considered to be "protected information," and should accordingly be given the strongest legal protection. To the extent that it is necessary to provide further levels of protection in particular cases, this should depend on the nature of the intrusion in the particular context, rather than by reference to abstract categories and archaic definitions.

---

national security purposes, 10 April 2014*,* WP215, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

[41] *See*: *Digital Rights Ireland v. Ireland*, Joint Cases C-293/12 and C-594/12, 8 April 2014, paras. 25-31: "In such circumstances, even though, as is apparent..., the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter. The retention of data for the purpose of possible access to them by the competent national authorities...directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article. See also para. 37: "It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious.", referencing the Advocate General's Opinion on the matter (delivered December 12, 2013. Article 7 of the EU *Charter of Fundamental Rights* states that "Everyone has the right to respect for his or her private and family life, home and communication."

[42] Among other things, EU data protection law is subject to a broad "balancing" principle that enables the processing of (non-sensitive) personal data without consent and without a clear statutory basis provided the interests of the data subject do not "outweigh" the "legitimate interests" of the controller, save that what constitutes "sensitive" and "legitimate" interests are not clearly defined. In addition, there are broad exceptions enabling the processing of sensitive personal data where "necessary" to protect certain broader interests, including an outright exclusion for the purposes of "national security."

COMMUNICATIONS SURVEILLANCE

In the wake of the Snowden revelations, various governments have more aggressively sought to defend their activities by distinguishing between the automated collection and scanning of private communications, on the one hand, and the actual scrutiny of those communications by human beings, on the other. Some officials 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 is not "surveillance" for purposes of triggering legal protections.

International human rights law, however, makes clear that the collection and retention of communications data amounts to an interference with the right to privacy, whether or not the data is subsequently accessed or used by government officials. In *S and Marper v. United Kingdom,* for instance, the Grand Chamber of the European Court of Human Rights held that "the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data."[43] In *Digital Rights Ireland Ltd v. Minister for Communications,* the Grand Chamber of the Court of Justice of the European Union similarly held that the retention of communications data "for the purpose of possible access to them by the competent national authorities" constituted a "particularly serious interference" with the right to respect for private and family life, home, and communications under Article 7 of the EU Charter of Fundamental Rights.[44]

For these reasons, the Principles make clear that "Communications Surveillance" includes not only the actual reading of private communications by another human being, but also the full range of 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. Any suggestion by governments that automated collection or monitoring is not surveillance is, therefore, plainly at odds with the requirements of international human rights law. Nor should states be able to bypass privacy protections by reference to such arbitrary definitions.

PRINCIPLE BY PRINCIPLE EXPLANATION

The Principles are firmly rooted in well-established human rights law. In particular, they draw on the rights to privacy, freedom of opinion and expression, and freedom of association as guaranteed in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on

[43] *S and Marper v. United Kingdom* (2009) 48 EHRR 50 at para 121. The case concerned the "blanket and indiscriminate" retention of DNA samples from persons arrested but not charged or convicted.

[44] Joined Cases C 293/12 and C 594/12, 8 April 2014, paras. 29 and 39. The Grand Chamber of the CJEU also found that retention was an interference with the right to data protection under Article 8 of the Charter (*see* para. 36 of its judgment). In Case C-70/10, *Scarlet Extended SA v. SABAM* (2010), the CJEU similarly held that a filtering system proposed by rights-holders in order to combat copyright infringement was unlawful on the basis that it would require ISPs to engage in real-time "preventative monitoring" of customers' communications and would breach Article 15(1) of Directive 2000/31 and likely breach the rights to data protection and freedom of expression under Articles 8 and 11 of the EU Charter of Fundamental Rights.

Human Rights (ECHR), the European Charter on Fundamental Rights (EU Charter), and the Inter-American Convention on Human Rights (IACHR).[45]

While each of these rights is formulated in slightly different ways,[46] the structure of each article is usually divided into 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. Typically, the second paragraph provides that any restriction on the core right must comply with the following requirements:

- It must be provided "by law";
- It must not be "arbitrary";
- It must pursue one of the legitimate aims exhaustively listed in that paragraph; and
- It must be "necessary" to achieve the aim in question—which has been held to include requirements of adequacy and proportionality.

This "permissible limitations" test has been applied equally to the rights to privacy, freedom of expression, and freedom of association.[47] We explore the legal underpinning of each of these requirements in more detail under the heading of each corresponding Principle further below (Principles 1 to 5). We do so with reference to the specific context of surveillance where appropriate. We then explain our thinking and the legal basis behind the adoption of the remaining Principles (Principles 6 to 13). While we address them separately, the Principles expressly note that they are holistic and self-referential, meaning that each principle and the preamble should be read and interpreted as one part of a larger framework.

Principle 1: LEGALITY

General principles

The principle of legality is a fundamental aspect of all international human rights instruments and indeed the rule of law in general. It is a basic guarantee against the state's arbitrary exercise of its powers. For this reason, any restriction on human rights must be "provided" or "prescribed" by law.[48]

Under the ICCPR, the principle of legality is closely associated with the concept of "arbitrary interference." For instance, Article 17 stipulates that *"[n]o one shall be subjected to*

[45] *See* Articles 8-11 ECHR, Articles 12, 17, 18, 19, 21, and 22 ICCPR, and Articles 11, 12, 13, 15, and 16 IACHR.
[46] This is especially noticeable in relation to the right to privacy. For instance, Article 8 ECHR refers to the right to respect for private and family life, home and correspondence while Article 7 of the EU Charter refers to the right to respect for private and family life, home, and *communications*. For a more detailed analysis of the right to privacy under the ICCPR and other domestic and regional instruments, *see* UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/HRC/13/37, 28 December 2009, para. 11, available at: http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf.
[47] *See* UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Ibid.*, at paras. 16-18; *see also* UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/23/40, 17 April 2013, at paras. 28-29.
[48] *See* footnote 45, above. Other articles in the human rights treaties refer to "law," "lawfulness," or "legal" such as Article 5 ECHR (freedom from arbitrary arrest and detention), and Article 7 ECHR (no punishment without law).

arbitrary or unlawful interference with his privacy, family, or correspondence." The Human Rights Committee has interpreted "arbitrary interference" as follows:[49]

> The expression "arbitrary interference" is also relevant to the protection of the right provided for in Article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

In addition, the meaning of "law" implies certain minimum qualitative requirements of clarity, accessibility, and predictability. In particular, the Human Rights Committee has elaborated on the meaning of "law" for the purposes of Article 19 ICCPR (freedoms of opinion and expression) as follows:[50]

> 25. For the purposes of paragraph 3, a norm, to be characterized as a "law," must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.

The European Court of Human Rights has followed a similar approach in its jurisprudence. In particular, it has held that the expression "prescribed by law" implies the following requirements:[51]

> Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.

The same requirements apply in respect to the right to privacy under Article 17 ICCPR and Article 8 ECHR.[52]In particular, the European Court of Human Rights has clarified in the context of surveillance[53]:

---

[49] UN Human Rights Committee, General Comment No. 16 (1988) in Human Rights Instruments, Volume I, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies, HRI/GEN/1/Rev.9 (Vol. I) 2008, pp. 191-193, para. 4. See also UN Human Rights Committee, Toonen v Australia, Communication No. 488/1992, para. 8.3, U.N.Doc CCPR/C/50/D/488/1992 (1994) and Van Hulst v the Netherlands, Communication No. 903/1999, para. 7.6, U.N. Doc. CCPR/C/82/D/903/1999 (2004). In both communications, the Committee noted that reasonableness requires proportionality. More generally, *see* ACLU Privacy Rights In the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights, March 2014, available at: https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf.

[50] *See* UN Human Rights Committee, General Comment no. 34 on freedoms of opinion and expression (Article 19 ICCPR), available at: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[51] Judgment in the *Sunday Times vs. United Kingdom*, no. 6538/74; 26 April 1979, para. 49.

> [T]he law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

The European Court went on to explain:[54]

> [I]t would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

In other words, secret rules or secret guidelines or interpretations of the rules do not have the quality of "law."[55]A law that is not public is not law, for it is an essential component of the rule of law that the laws must be known and accessible to all. Similarly, laws or rules that are couched in terms of an unfettered power granted to the authorities fall afoul of the requirements of "law." The scope and manner of exercise of any discretion must therefore be indicated in the law itself or in published guidelines with "reasonable clarity," so that individuals can reasonably foresee how the law will be applied in practice. This all the more important given the inherent risks of arbitrariness in the exercise of power in secret.[56]

In the context of surveillance, this means that merely passing a law authorising mass surveillance at the national level does not make the surveillance "lawful" if that law fails to meet certain basic requirements of clarity and accessibility in the first place.

Minimum safeguards in the context of communication surveillance

The above requirements of clarity, accessibility, and precision take on a special meaning in the context of communication surveillance. This is because of the distinctive threat to the very essence of democracy posed by secret surveillance, as the European Court of Human Rights recognised as early as 1978.[57] The Court found that the "mere existence" of

---

[52] In relation to Article 17 ICCPR, *see* references in footnote 46 above. The European Court of Human Rights applied the principles developed under Article 10 ECHR (right to freedom of expression) in *Sunday Times* in the case of *Silver and others v. the United Kingdom,* nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983, paras. 85-86, which concerned the right to privacy of prisoners under Article 8 ECHR.

[53] *Malone v. the United Kingdom,* no. 8691/79, 2 August 1984, para. 67.

[54] *Ibid*., para. 68.

[55]*Silver and others v. the United Kingdom* cited above*,* paras. 85-86 and *Malone v. the United Kingdom,* cited above, para. 67.

[56] *Malone v. the United Kingdom*, para. 67.

[57] *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, paras. 42 and 49. In particular, the Court held "The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measure they deem appropriate." *See* also the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (OEA/Ser.L/V/II, CIDH/RELE/INF. 11/13, 31 December 2013), para 150: "As far as freedom of expression is concerned, the violation of the privacy of communications can give rise to a direct restriction when—for example—the right cannot be exercised anonymously as a consequence of the

legislation that allowed a system to secretly monitor communications gave rise to a "menace of surveillance" that amounted to an interference with the privacy of *all* those to whom the legislation may have been applied.[58] In view of these risks, the Court concluded that there must be adequate and effective guarantees against abuse laid down in law, and more specifically in statute.[59]

In particular, the European Court of Human Rights has identified the following minimum safeguards a surveillance law must meet in order to be compatible with Article 8 ECHR:[60]

- The offences and activities in relation to which surveillance may be ordered must be spelled out in a clear and precise manner;
- The law must clearly indicate which categories of people may be subjected to surveillance;
- There must be strict time limits on surveillance operations;
- Strict procedures must be in place for ordering the examination, use, and storage of the data obtained through surveillance;
- The law must lay down the precautions to be taken when communicating data to third parties;
- There must be strict rules on the destruction or erasure of surveillance data to prevent surveillance from remaining hidden after the fact;
- The bodies responsible for supervising the use of surveillance powers must be independent and responsible to, and be appointed by, Parliament rather than the Executive.

The same approach has been followed at the UN and Inter-American level. Specifically, the UN and OAS Special Rapporteurs on freedom of expression recently issued a Joint Declaration on surveillance programs in which they said:[61]

> [S]tates must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged.

---

surveillance activity. In addition, the mere existence of these types of programs leads to an indirect limitation that has a chilling effect on the exercise of freedom of expression."

[58] *Klass and Others v. Germany* cited above, para. 37.

[59] *See Weber & Savaria v. Germany*, no. 54934, 29 June 2006, para. 95.

[60] *See* in particular *Klass and Others v. Germany* cited above, *Liberty and Others v. the United Kingdom*, no. 58243/00,1 July 2008 and *Rotaru v. Romania,* no. 28341/95,[GC], 4 May 2000 concerning surveillance carried out by the intelligence agencies. For more details about the ECHR case law on surveillance, *see* Factsheet on the Protection of Personal Data, available at: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[61] *Joint Declaration on surveillance programs and their impact on freedom of expression*, issued by the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013, paras. 8 and 9, available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

> Given the importance of the exercise of these rights for a democratic system, the law must authorize access to communications and personal information only under the most exceptional circumstances defined by legislation. When national security is invoked as a reason for the surveillance of correspondence and personal information, the law must clearly specify the criteria to be used for determining the cases in which such surveillance is legitimate. Its application shall be authorized only in the event of a clear risk to protected interests and when the damage that may result would be greater than society's general interest in maintaining the right to privacy and the free circulation of ideas and information. The collection of this information shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.

Their views also reflect the recommendations of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin, who said in his 2009 report:[62]

> 69. Strong independent oversight mandates must be established to review policies and practices, in order to ensure that there is strong oversight of the use of intrusive surveillance techniques and the processing of personal information. Therefore there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorised through an independent body.

We return to the need for strong independent oversight in relation to Principles 6, 7, 9, and 10 further below.

Principle 2: LEGITIMATE AIM

Under international human rights law, any restriction on the rights to privacy, freedom of expression, and freedom of association must pursue at least one of the "legitimate aims," which are often exhaustively listed in the corresponding article at issue. These aims are extremely broadly phrased and include public safety, prevention of crime, protection of morals and of the rights of others, and national security.[63] Under Article 8 ECHR, this also includes "the economic well-being of the country." While Article 17 ICCPR does not explicitly stipulate that any restriction on the right to privacy must be necessary for a specified purpose, both the UN Special Rapporteur on Counter-Terrorism and the UN Special Rapporteur on Freedom of Expression have held that the "permissible limitations" test

[62] A/HRC/13/37, 28 December 2009, available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf.

[63] *See*, *e.g.*, Article 19 ICCPR (freedom of opinion and expression) refers to respect of the rights or reputations of others, [or] for the protection of national security or of public order, or of public health or morals; Article 8 ECHR (right to privacy) refers to "national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others," Article 13 IACHR (freedom of expression) refers to respect for the rights or reputation of others, the protection of national security, public order, or public health or morals.

under Article 19 among other articles of the ICCPR, was equally applicable to Article 17 ICCPR.[64]

Under European human rights law, states rarely encounter any difficulty in demonstrating that the restriction at issue pursues a legitimate aim. This is mainly because the Court tends to focus its analysis on the legislative framework for the exercise of surveillance powers rather than on a specific surveillance measure used in a particular case. It is also generally accepted by the Court that surveillance powers are necessary for the purposes of national security and law enforcement.[65] The need for surveillance measures to be more specifically "targeted" is an aspect that is more closely tied the question of the proportionality of the measure but, in practice, is rarely examined by the Court.[66]

By contrast, the UN Special Rapporteur on Freedom of Expression, Frank LaRue, expressed his concern in a recent report that "vague and unspecified" notions of "national security" in particular had been unduly used to justify interception and access to communications without adequate safeguards.[67] The Special Rapporteur went on to conclude:

> *60. The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists, or activists. It also acts to warrant often-unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.*[68]

Mindful of the potential for abuse inherent in such overly broad concepts, the Principles have sought to adopt a more stringent standard as to what constitutes a "legitimate aim" in relation to mass surveillance. For this reason, the "pressing and substantial objective" test applied in Canada and the "compelling government interest" test used in the United States were also discarded as being insufficiently rigorous.[69] Instead, the Principles reflect a higher standard imposed in Germany. In particular, the German Constitutional Court has ruled that deeply intrusive measures such as a search of a computer by law enforcement agencies cannot be justified merely by reference to some vaguely defined general interest. The German Constitutional Court held that such a measure had to be justified on the basis of evidence that there is "a concrete threat to an important legally-protected interest," such as a threat to the "life, limb or liberty of a person" or to "public goods, the endangering of

---

[64] *See* footnote 46 above.

[65] *See* for instance *Klass and others,* cited above, at para. 46.

[66] One rare exception is *Uzunv. Germany,* no. 35623/05, 2 September 2010; *see also Peck v. the United Kingdom,* no. 44647/98, 28 January 2003.

[67] A/HRC/23/40, report of 17 April 2013, at para. 58, available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[68] *Ibid.*

[69] *See*, e.g., in Canada: R. v. Oakes, [1986] 1 S.C.R. 103; R. v. Big M Drug Mart Ltd., [1985] 1 S.C.R. 295; In the United States: Austin v. Michigan Chamber of Commerce, 494 U.S. 652, 655 (1990). Boos v. Barry, 485 U.S. 312, 334 (1988) (plurality); see also Burson v. Freeman, 504 U.S. 191, 198 (1992) (plurality); Board of Airport Comm'rs v. Jews for Jesus, Inc., 482 U.S. 569, 573 (1987); Cornelius v. NAACP Legal Defense and Educ. Fund, Inc., 473 U.S. 788, 800 (1985); United States v. Grace, 461 U.S. 171, 177 (1983); Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

which threatens the very bases or existence of the state, or the fundamental prerequisites of human existence."[70]

Additionally, the Principles expressly prohibit discrimination in laws, including discrimination based on national or social origin, birth, or other status. This is, of course, a standard provision in international human rights law.[71] Here it, along with the extraterritorial application of the law discussed above, ensures that the protections of law reach all persons subject to surveillance regardless of their location or citizenship.

Principles 3, 4, and 5: NECESSITY, ADEQUACY, & PROPORTIONALITY

The principle that any interference with a qualified right such as the right to privacy or freedom of expression must be "necessary in a democratic society" is one of the cornerstones of human rights law. In general, it means that a state must not only demonstrate that its interference with a person's right meets a "pressing social need" but also that it is *proportionate*—or under Inter-American jurisprudence *adequate*[72]—to the legitimate aim pursued.[73]

In particular, the European Court of Human Rights has clarified that the term "necessary" is not synonymous with "indispensable." Nor is it as flexible as the terms "admissible," "ordinary," "useful," "reasonable," or "desirable."[74] Subject to the "margin of appreciation" doctrine, the European Court makes its assessment of the necessity and proportionality of a measure "in the light of all the circumstances." Nonetheless, certain measures, such as powers of secret surveillance, are more closely scrutinised.[75]

The Human Rights Committee follows a similar approach. In particular, the Committee explained in its General Comment on Article 12 ICCPR (freedom of movement):[76]

> Article 12, paragraph 3, clearly indicates that it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them. Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; *they must be the least intrusive instruments amongst those, which might achieve the desired result*; and they must be proportionate to the interest to be protected. [Emphasis added].

The same principles apply to the interpretation of Article 19 ICCPR[77] and Article 17 ICCPR.[78]

---

[70] *Dictum* in the Constitutional Court judgment of 27 February 2008 (1 BvR 370/07 and 1 BvR 595/07).

[71] *See*, *e.g.*, Article 2(1) ICCPR, Article 1.1 and 24 IACHR, Article 14 ECHR, Article 2 of International Convention for the Elimination of All Forms of Racial Discrimination, and Article 2 of the Convention to Eliminate All Forms of Discrimination Against Women. *See also*, *e.g.*, *Carson and others v. United Kingdom* (2010) 51 EHRR 13 in which the Grand Chamber of the European Court of Human Rights held that "other status" under Article 14 ECHR includes "country of residence" (paras. 70-71).

[72] Inter-American Court of Human Rights, *Case of Tristán Donoso v. Panama*, Preliminary Objection, Merits, Reparations and Costs. Judgment of January 27, 2009. Series C No. 193, para. 56.

[73] *Handyside v. the United Kingdom*, no. 5493/72, 7 December 1976, paras. 48 and 49.

[74] *Ibid.*, para. 48.

[75] *Klass v. Germany*, para. 42.

[76] General Comment No. 27, 1999, CCPR/C/21/Rev.1/Add.9, reproduced in *Human Rights Instruments, Volume I, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies*, HRI/GEN/1/Rev.9 (Vol. I) 2008, pp. 223 – 227, paras. 11 – 16.

[77] *See* General Comment no. 34 cited above, footnote 20, para. 34.

The Human Rights Committee also sometimes uses the word “appropriate” in its analysis. For instance, in relation to Article 19 ICCPR (freedom of expression), the Committee observed that restrictive measures “must be appropriate to achieve their protective function.”[79]

Similarly, as noted above, the Inter-American Court of Human Rights sometimes refers to the concept of “adequacy.” In particular, the Court has considered whether the measure at issue would be capable of contributing to the realization of the objective invoked for limiting the right at issue.[80]

Courts in several states have clarified that substantively, “adequacy” or “appropriateness” do not mean that the measures at issue have to be entirely successful. Instead, they impose a requirement analogous to the Canadian concept of “rationally connected,” although “appropriateness” is applied more rigorously. The measure must not just have some logical link to its intended objective, but should also be “effective” at achieving it. A measure which is inherently incapable of achieving the stated objective, or which is demonstrably grossly ineffective in achieving it, cannot ever be said to be “appropriate,” “necessary,” or “proportionate.”

This requirement of proportionality is particularly important in the context of mass surveillance, which is based on the indiscriminate collection and retention of communications and metadata without any form of targeting or reasonable suspicion. In *S and Marper*, for example, the Grand Chamber of the European Court of Human Rights held that the "blanket and indiscriminate" retention of DNA data amounted to a "disproportionate interference" with the private lives of those persons from which the data had been taken. The Grand Chamber placed particular weight on the fact that the material was "retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected."[81] In another case involving the use of search powers, the Grand Chamber found the absence of any requirement on the police to have "reasonable suspicion" that the person being searched was involved in criminality meant that the search power lacked "adequate legal safeguards against abuse" (paras. 86-87).[82] Most recently in its decision in *Digital Rights Ireland Ltd*,[83] the Grand Chamber of the Court of Justice of the European Union held that, although the retention of communications data under the Directive was for the legitimate aim of combating "serious crime," the blanket nature of the obligation entailed "an interference with the fundamental rights of practically the entire European population,"[84] including "persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[85]

---

[78] *See* references in footnote 46 above.
[79] *See* General Comment no. 34, *ibid*.
[80] Inter-American Court of Human Rights, *Case of Fontevecchia y D`Amico v. Argentina*, Merits, Reparations and Costs. Judgment of November 29, 2011. Series C No. 238, para 53.
[81] *S and Marper v. United Kingdom* (2009) 48 EHRR 50 at para 118. The UK government itself admitted that the retention of DNA data "was neither warranted by any degree of suspicion of the applicants’ involvement in a crime or propensity to crime nor directed at retaining records in respect of investigated alleged offences in the past" (para 94).
[82] *Gillan and Quinton v. United Kingdom* (2010) 50 EHRR 45 at paras. 86-87.
[83] Joined Cases C-293/12 and C-594/12, 8 April 2014.
[84] *Ibid*., para 56.
[85] *Ibid*., para 58.

By its very nature, mass surveillance does not involve any form of targeting or selection, let alone any requirement on the authorities to show reasonable suspicion or probable cause. Accordingly, mass surveillance is inevitably disproportionate as a matter of simple definition.[86] The Principles reflect the above international standards under the headings "necessity," "adequacy," and "proportionality."

As to targeted surveillance, the Principles discuss factors that must be established to a competent judicial authority prior to surveillance. The factors require careful limitations on the information accessed, as well as limits on use and retention. Importantly, as discussed further below, this provision requires the role of a Competent Judicial Authority.

Principles 6 and 7: COMPETENT JUDICIAL AUTHORITY & DUE PROCESS

Surveillance and prior judicial authorisation

As noted above, the Principles require that all decisions relating to Communications Surveillance be made by a competent judicial authority acting independently of the government and in accordance with due process of law. This reflects the core requirement of international human rights law that the use of lawful surveillance powers by public officials must not only be necessary and proportionate but also be attended by independently monitored strict safeguards against abuse.[87] As the European Court of Human Rights held in its 1979 decision in *Klass v. Germany:*[88]

> The rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

Although the Court in *Klass* agreed that "it is in principle desirable to entrust supervisory control to a judge," it did not go so far as to hold that prior judicial authorisation was required in every case so long as the relevant authorising body was "sufficiently independent" of "the authorities carrying out the surveillance" to "give an objective ruling" and was also vested "with sufficient powers and competence to exercise an effective and continuous control."[89] In subsequent cases, however, the Court has made clear the desirability of judicial authorisation for the use of lawful surveillance. In a case in 1999, for instance, the Court stated that:

> It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence.[90]

---

[86] Privacy International, Electronic Frontier Foundation, Access, APC, ARTICLE 19, Human Rights Watch et al, *OHCHR consultation in connection with General Assembly Resolution 68/167 "The right to privacy in the digital age,"* 1 April 2014, available at: https://www.eff.org/files/2014/04/17/ngo_submission_final_31.03.14.pdf.

[87] *See, e.g., Weber and Savaria v. Germany,* cited above at para 95, in which the Court identified various "minimum safeguards that should be set out in statute law in order to avoid 'abuses of power'" (para. 95).

[88] (1979-1980) 2 EHRR 214 at para. 55.

[89] *Klass v. Germany,* cited above, para. 56.

[90] *Kopp v. Switzerland* [1999] 27 EHRR 91, para. 74.

The Principles, however, reflect the view that prior judicial authorisation of surveillance powers is not merely desirable but *essential*. This is because neither of the other two branches of government is capable of providing the necessary degree of independence and objectivity to prevent the abuse of surveillance powers. The Court's view in *Klass*—that oversight by a parliamentary body might be sufficiently independent—no longer seems tenable, particularly in the wake of the 9/11 attacks in which legislators have shown themselves all too willing to sacrifice individual rights in the name of promoting security. In the case of the executive branch, the dangers are even more acute. In the UK, for instance, the same government ministers who are responsible for the activities of the intelligence services are also responsible for authorising interception warrants, and do so on the advice of those agencies—hardly a credible safeguard against abuse.

In addition, in August 2012, the South Korean Constitutional Court rejected the collection of individuals' subscriber data in the absence of prior judicial authorization on the basis that this amounted to "treating them as potential criminals."[91] This was followed by the Korean National Human Rights Commission, which decided in April 2014 that the lack of any requirement for prior judicial authorization for access to the collected data by police violates international human rights.[92] Also notable, among its recent recommendations relating to NSA surveillance, the UN Human Rights Committee recommended that the US government should provide "for judicial involvement in [the] authorization or monitoring of surveillance measures."[93] For these reasons, the Principles endorse the view that only a judge offers the sufficient guarantees of independence and impartiality to ensure that surveillance powers are exercised in a manner, which is both necessary and proportionate.

In practice, however, merely having a judge take surveillance decisions is not enough to protect fundamental rights. The Principles also make clear the importance of having judges who are conversant with both the relevant technologies and human rights principles so that they properly understand the nature of each surveillance request, and are able to assess its likely impact on individual privacy. Similarly, authorising judges must have sufficient resources to carry out the functions assigned to them, including *continuing* oversight of all surveillance activities, which have been authorised.

One of the key defects of existing models of prior judicial authorization is the fact that applications for surveillance are inevitably made ex parte without notice.[94] In practical terms, very few applications are refused and a major factor is undoubtedly the lack of any kind of adversarial challenge, because the interests of the person who is the proposed subject of surveillance are not effectively represented. In some jurisdictions, however, various mechanisms have been adopted in order to try and introduce an adversarial element into proceedings. One such example is the Queensland Public Interest Monitor, in which a lawyer is automatically appointed to represent the interests of the person affected

[91] *See* http://news.mt.co.kr/mtview.php?no=2014041611218282360 (Korean).

[92] *See* Constitutional Court's Decision 2010 Hunma 47, 252 (consolidated) announced August 28, 2012, and the subsequent decision of the Korean High Court in October 2012 (Seoul High Court, 2011Na19012, Chief Judge Kim Sang-Jun) which held a major portal liable for disclosing a blogger's identity to the police when no warrant was produced.

[93] UNHRC, Concluding Observations on the 4th U.S. report, 27 March 2014, available at: http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf, para. 22.

[94] For an analysis of the potential impact of such practices, see: K.S. Bankston, "Only the DOJ Knows: The Secret Law of Electronic Surveillance", (2007) 41 Univ. .S.F. L. Rev. 589, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2009442.

whenever an application is made for surveillance.[95] Other instances might involve the appointment of a special advocate (as used in public interest immunity proceedings in the UK and elsewhere) in order to represent the interests of the person who is unaware of the application.[96] These models are far from perfect, but they represent good faith attempts to square the circle in relation to effectively challenging covert surveillance decisions.

The other relevant principle in this context is that of Due Process, *i.e.* surveillance decisions must not only be made in accordance with the law, but in a manner compatible with the fundamental rights of the affected individual.[97] Prior judicial authorisation is an important safeguard in this respect, but many countries provide that surveillance powers may sometimes be used without judicial authorisation in times of emergency. The Principles therefore require that retroactive authorisation must be sought within a reasonably practicable time period, in order to prevent the abuse of emergency powers. They also require post-notification of surveillance decisions (*see* User Notification below) so that individuals will have the opportunity to challenge the legality, necessity, and proportionality of any surveillance decision affecting them. In the absence of an effective adversarial procedure for the authorisation of surveillance, states should also consider the introduction of suitable internal mechanisms to enable *ex parte* applications for surveillance to be properly challenged prior to authorisation being granted.[98]

Data sharing, judicial supervision, and prior authorization

Among the many problems caused by the mass collection and retention of private communications data is the lack of adequate controls on the onward sharing of such data by different government agencies as well as between different governments, as discussed above. A recent example is the way in which NSA data—supposedly gathered for the purpose of countering threats to national security—has instead been used for drug enforcement, regular law enforcement, and tax investigation purposes.[99] Indeed, these problems can arise even within different departments of the same agency, for example, the sharing of data between Canada's general compliance tax revenue branch and its criminal investigations wing—divisions that operate under very different legal restrictions reflecting the different standards, which are applicable in civil and criminal proceedings.

---

[95] *See* Eric Metcalfe, *Secret Evidence*, JUSTICE, June 2009, available at: http://www.justice.org.uk/data/files/resources/33/Secret-Evidence-10-June-2009.pdf at 177.

[96] *See* ibid at p173 for discussion of the Canadian SIRC model and p 231 for proposals to introduce public interest advocates. It is now increasingly common for UK Courts to appoint public interest immunity advocates: see e.g. *CM (Zimbabwe) v Secretary of State for the Home Department* [2013] EWCA Civ 1303. See most recently the report by the Congressional Research Service, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate,* 21 March 2014, available at: http://www.fas.org/sgp/crs/intel/R43451.pdf.

[97] *See,* e.g., the discussion of the need for prior judicial authorisation in the context of computer searches in the judgment of the Canadian Supreme Court in *R. v. Vu*, 2013 SCC 60, available at: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13327/index.do

[98] *See* section on User Notification below for further details.

[99] *See* Jennifer Stisa Granick & Christopher Jon Sprigman, *NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor*, 14 August, 2013, available at: http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/.

This problem of unrestricted data-sharing must be addressed, not only by appropriate data protection measures but also, where appropriate by way of judicial supervision of search warrants to enable the court to assess whether it is necessary and proportionate for the information sought to be shared with other public bodies. This is directly addressed in the proportionality principle as well.

Principle 8: USER-NOTIFICATION & THE RIGHT TO AN EFFECTIVE REMEDY

Under international human rights law, the principles of user-notification and transparency are best understood not only under the right to privacy but also as part of the right to an effective remedy and to a fair trial.[100] For it is fundamental to any effective system of justice that where there is a right, there must be a remedy (*ubi jus ibiremedium*).[101] It is impossible, however, for a person to effectively challenge a government's interference with his or her privacy without knowing whether he or she has been a victim in the first place. More generally, the absence of transparency concerning the operation of laws governing covert surveillance can prevent meaningful democratic scrutiny of those laws, effectively leaving intelligence agencies as lawmakers unto themselves.

Unfortunately, although European law requires user notification in the context of data protection in general,[102] the European Court of Human Rights has so far failed to find that user-notification is a necessary requirement in cases involving covert surveillance.[103] Indeed, in the 1979 case of *Klass v. Germany,* the Court acknowledged that the lack of any post-notification requirement means that surveillance decisions are effectively non-justiciable as far as the person affected is concerned:

> [T]he very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the

[100] The right to a fair trial is guaranteed under Article 10 UDHR, Article 6 ECHR, Article 8 IACHR, and Article 14 ICCPR. The right to an effective remedy is guaranteed under Article 8 UDHR, Article 15 IACHR, Article 13 ECHR, and Article 2.3 ICCPR. Under the EU Charter, both rights are protected under Article 47.

[101] *See*, *e.g.*, *Ashby v. White* (1703) 92 ER 126 per Lord Holt CJ: "it is a vain thing to imagine a right without a remedy, for want of right and want of remedy are reciprocal."

[102] *See*, in particular, Article 8 of the 1981 Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention No. 108) and Articles 10, 11, and 12, as well as 18 and 19 of the EC 1995 *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (Directive 95/46/EC). For an extensive discussion, linked to technological developments, *see* Douwe Korff, *Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, prepared for Douwe Korff & Ian Brown, *et al.*, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, study commissioned by the European Commission, 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.

[103] *See Klass v. Germany* (1979-80) 2 EHRR 214 at para. 58: "In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore...such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the 'interference' resulting from the contested legislation is in principle justified under Art 8(2)...the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the 'interference.'"

> individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights.

In a subsequent case in 2007, the Court suggested that "as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned,"[104] but stopped short of finding that notification was a necessary requirement of surveillance laws in general. In the 35 years since the Court's decision in *Klass*, however, it has become clear that there are no "adequate and equivalent safeguards" to effective user notification. In the UK, for example, the overwhelming majority of surveillance decisions under the Regulation of Investigatory Powers Act have been made without either prior judicial authorisation or effective judicial oversight on an ex post facto basis.[105] As a consequence of the Court's reasoning in *Klass*, many surveillance decisions have escaped both public scrutiny and effective judicial oversight.

The flawed approach taken by the European Court of Human Rights in *Klass* is, moreover, plainly at odds with the experience of those jurisdictions in which post-surveillance user notification requirements have operated for many years. In Canada, for example, the law limits the time of wiretapping surveillance and imposes an obligation to notify the person under surveillance within 90 days of the end of the surveillance, extendable to a maximum of three years at a time.[106] For this reason, the Principles stress the need for notification at the earliest possible opportunity, setting out an exhaustive list of circumstances which may justify delay—only when notification would seriously jeopardize the purpose for the surveillance or an imminent risk of danger to human life. They also require any delay to be determined by a Competent Judicial Authority, implying that sometimes notification may need to occur even before a risk to the purpose for which the surveillance was authorized is

[104] *Association for European Integration and Human Rights and Ekimdzhievv. Bulgaria*, 62540/00, 28 June 2007, para. 90. See also *Weber and Savariav. Germany,* where the Court reiterated that notification could constitute an important safeguard, though again not a necessary one.

[105] *See Freedom from Suspicion: Surveillance Reform for a Digital Age* (JUSTICE, October 2011).

[106] *See Criminal Code*, R.S.C., 1985, c. C-46, Part VI. Part VI has operated effectively for several decades, showing that individual notification requirements are practically workable. Moreover, the Canadian Supreme Court has recently taken steps towards recognizing individual notification obligations are a constitutional imperative under section 8 of the Canadian *Charter of Rights and Freedoms*, which guarantees the right to be free from unreasonable search and seizure: *R. v. Tse*, 2012 SCC 16, para. 11 (individual notice a constitutional requirement for wiretaps where there is no prior judicial authorization because of exigent circumstances); *R. v TELUS Communications Co.*, 2013 SCC 16, para. 30 ("a notice provision was necessary to meet the minimal constitutional standards of s. 8" protections against unreasonable search and seizure, but in obiter); *R. v. Chehil*, 2013 SCC 49, para. 58 ("after-the-fact notice of searches that are not subject to prior judicial authorization is an important safeguard against the abuse of such powers" referring to drug detection dogs 'sniffing' someone's suitcase). The United States 50 U.S.C section 2518(8)(d) requires notice for wiretaps "within reasonable time but not later than ninety days after the filing of an application for an order of approval." However none of these requirements have been applied to surveillance conducted under foreign intelligence authorities.

deemed to be "lifted."[107] This is done because investigations will often stretch indefinitely without any ongoing legitimacy. In fact, some wiretapping statutes expressly recognize this.

In practice, any system of user notification will inevitably be vulnerable to *ex parte* applications by government agencies to delay or prevent notification in particular cases. The nature of such applications means that the courts will be asked to determine the need for secrecy based on one-sided information presented by the authorities. In order for the principle of user notification to work effectively, therefore, it is incumbent upon legislatures to devise mechanisms to open up surveillance decisions to adversarial challenge as much as possible as discussed in the section on prior judicial authorisation above.

Finally, it is important to bear in mind that user notification and transparency serve different interests: the former is concerned with the provision of sufficient information about a surveillance decision to enable the affected individual to effectively challenge it or seek remedies; the latter is aimed at ensuring that the general public has sufficient information to assess whether the laws governing surveillance are working effectively, including whether there are sufficient safeguards for an individual's right to privacy. This is discussed in the following section.

The user notification principle thus requires notification with time to enable a challenge and only authorizes delay in narrow circumstances authorized by a Competent Judicial Authority, to ensure that delay is justified and no lengthier than strictly necessary to protect an investigation or to protect against a risk to human life.

Principles 9 & 10: TRANSPARENCY & PUBLIC OVERSIGHT

The principle of public oversight is closely related to, but distinct from, the question of remedies in individual cases; it relates to the importance of transparency to democracy in general. In a democracy, members of the public participate in the making of laws via their elected representatives. It is therefore essential that they have sufficient information as to how those laws are working in order to make informed decisions, whether at the ballot box or when deliberating with others over matters of public policy.[108] It is also essential in a democracy that public officials who have been entrusted with the power to conduct surveillance are subject to effective oversight, in order to ensure that those powers are being used lawfully rather than arbitrarily, and that they remain accountable to the public at large.[109]

The need to ensure democratic transparency is all the more important in circumstances where, for operational reasons, aspects of the system remain secret and are not subject to normal judicial oversight. As the European Court of Human Rights held in *Klass,* "powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic

[107] For instance, Korean Law, which allows the delaying of user notification upon Regional Chief Prosecutor's approval, will violate this Principle. Communications Secrecy Protection Act, Article 9-2 (5).
[108] *See* ARTICLE 19, *The Public's Right to Know: Principles on Freedom of Information Legislation,* June 1999.
[109] *See also Tshwane Principles on National Security and the Right to Information* for a discussion of the state's authority to withhold information from the public on national security grounds, available at: http://www.right2info.org/national-security/Tshwane_Principles.

institutions."[110] This gives rise to two core requirements: first, any system of laws governing surveillance must not only place firm restrictions on any discretion enjoyed by public officials, but the relevant law must also be "sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[111] Second, the laws must also provide sufficient safeguards to avoid the risk of abuse of power or arbitrariness.[112]

As the UN Human Rights Committee has also noted, it is important that the state does not just provide paper safeguards, but actually carries out ongoing checks to see if these safeguards work in practice. The manifest failure of such oversight in the US, the UK, and elsewhere, is one of the most salient features of the fallout from the Snowden revelations.[113] The reminder of the importance of properly functioning monitoring and oversight bodies by the Human Rights Committee is therefore important, and rightly reflected in the Principles.[114]

Public oversight also requires governments to release sufficient, clear, and precise information to the public to allow for a serious assessment of the necessity and proportionality of the use of surveillance powers in practice.[115] Opaque, meaningless statistics cannot serve this purpose. While some operational matters may have to remain secret, this should never, in a democratic society, lead to the unaccountable use of surveillance powers, outside public, democratic scrutiny.

Thus, the Principles contain relatively detailed requirements and require independent oversight. They also expressly forbid interference with service providers who seek to publish information as part of their own transparency efforts.

Principle 11: INTEGRITY OF COMMUNICATIONS & SYSTEMS

The right to privacy entails the right of persons to construct means of communicating with one another in a way that is secure from outside intrusion. The duty of governments to respect the privacy of communications also imposes a corresponding obligation on those governments to respect the integrity of any and all systems used to transmit private communications. Yet one of the most significant revelations this year has been the extent to which the NSA, the GCHQ, and others have apparently worked to undermine the global communications infrastructure, whether by obtaining private encryption keys for commercial services, installing backdoors into security tools, or undermining key

[110] *Klass*, para. 42. *See also* para. 49: "The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."
[111] *Malone v. United Kingdom* at para. 67.
[112] *Huvig v. France* (1990) 12 EHRR 528 at paras. 29-35.
[113] Cindy Cohn, Mark Jaycox, *NSA Spying: The Three Pillars of Government Trust Have Fallen*, 15 Aug 2013, available at: https://www.eff.org/deeplinks/2013/08/nsa-spying-three-pillars-government-trust-have-fallen.
[114] *See* also e.g. Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014, WP215, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf
[115] *See,* in particular, Principles 2 and 3 of the Right to Know Principles (footnote 109 above).

cryptographic standards relied upon by millions around the world.[116] In April 2013, the UN Special Rapporteur on Freedom of Expression noted, "the security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption."[117] Accordingly, he recommended that:

> Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys.

In this way, Principle 11 reflects the basic requirement that any interference with the privacy of communications must not only be lawful but also *proportionate.* Just as it would be unreasonable for governments to insist that all residents of houses should leave their doors unlocked just in case the police need to search a particular property, or to require all persons to install surveillance cameras in their houses on the basis that it might be useful to future prosecutions, it is equally disproportionate for governments to interfere with the integrity of everyone's communications in order to facilitate its investigations or to require the identification of users as a precondition for service provision or the retention of all customer data.[118] Notably, in its observations on the Fourth Periodic Report on the United States conducted as part of its Universal Period Review, the problems inherent in data retention regimes were recently recognized by the Human Rights Committee that the United States should, amongst other things, "refrain from imposing mandatory retention of data by third parties."[119] In this way, the inherent assumption behind such interference—that all communications are potentially criminal—runs contrary to the presumption of innocence, a core requirement of international human rights law.[120]

Principle 12: SAFEGUARDS FOR INTERNATIONAL COOPERATION

With increasing frequency, state surveillance activities of communications span territorial boundaries. In addition to the collaborative globe-spanning surveillance of communications networks conducted by many foreign intelligence agencies and discussed in more detail above, broader cooperation between governments also includes more formalised cooperation between law enforcement agencies, including through Mutual Legal Assistance Treaties (MLATs).

International cooperation between governments raises questions as to how and when states may be liable under national and international law for their surveillance activities,

---

[116] *See* Kurt Opsahl, Crucial Unanswered Questions about the NSA's BULLRUN Program, available at: https://www.eff.org/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program.

[117] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A.HRC/23/40, 17 April 2013), para. 79.

[118] 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.

[119] April 23, 2014, CCPR/C/USA/CO/4, para. 22.

[120] *See*, *e.g.*, Article 14(2) ICCPR and Article 6(2). In *S and Marper*, above, the Grand Chamber noted that while "it is true that the retention of the applicants' private data cannot be equated with the voicing of suspicions," the presumption was nonetheless relevant to the assessment of proportionality in that the perception of persons whose data was retained "that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed," (para. 122).

which may have an impact far beyond their own borders. One issue is the extent to which states can be "extraterritorially" accountable for their human rights violations overseas, *e.g.* the surveillance of private communications in other countries. It is important to bear in mind, however, that current technology makes it possible for states to monitor a great deal of international traffic from within the confines of their own borders. It is therefore important to refer briefly to the issue of jurisdiction under international human rights law and the different ways that a state may be held responsible for its actions, even where the effects are felt beyond its borders.[121]

One particular area of concern is the unsanctioned practice of states "pulling" data from servers in other countries, without the consent or knowledge of those governments. It appears from the Snowden revelations, for instance, that the US authorities may require US-based companies to produce such data from servers they own or operate in other countries and can also direct such companies to not inform either the authorities in the countries from which they pull the data, the entities whose data they are handing over, or indeed the data subjects, of such compulsory data disclosures.

Not only do such practices plainly breach the requirements of domestic data protection legislation of the countries from which data is pulled, but they also violate the fundamental principle of international law that a state "cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter."[122] As the International Law Commission said:[123]

> With regard to the jurisdiction to enforce, a State may not enforce its criminal law, that is, *investigate* crimes or arrest suspects, in the territory of another State without that other State's consent. [Emphasis added].

The proper channel for international cooperation in such matters is by way of Mutual Legal Assistance Treaties (MLATs). In this context, a provision in the Council of Europe *Cybercrime Convention* suggests that transnational data collection by law enforcement agencies might be possible with the consent, not of the target state, but with "the lawful and voluntary

---

[121] For a more in-depth academic analysis and more extensive references to the case law of the Human Rights Committee and other sources, *see* Martin Scheinin & Mathias Vermeulen, "Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism," section 3.7 in *Denial of Extraterritorial Effect of Human Rights (Treaties)*, available at: http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf.

[122] Ian Brownlie, *Principles of Public International Law*, 6th ed., 2006, at p. 306. The classic expression of the principle can be found in the award of the sole arbitrator in the *Palmas Island* case, Max Huber:
"*Sovereignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other state, the functions of a state. The development of the national organization of states during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the state in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations*."
Island of Palmas Case (*Netherlands/United States of America*), Award of 4 April 1928, UNRIAA, vol. II (1928), pp. 829-871, at p. 838, available at: http://legal.un.org/riaa/cases/vol_II/829-871.pdf.
See also the *Lotus judgment* of the Permanent Court of International Justice (the forerunner of the International Court of Justice), 7 September 1927, pp. 18-19, available at: http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

[123] 2006 Report of the International Law Commission, *Annex E* (footnote 83,above), para. 22, on p. 526, [emphasis added].

consent of the person who has the lawful authority to disclose the data to [the requesting LEA]" (Art. 32(b)) is highly contentious. At the very recent *Octopus Conference on Cooperation against Cybercrime* (Strasbourg, 4-6 December 2013), it was agreed to explore drafting a new protocol to either the *Cybercrime Convention* or the Council of Europe *Data Protection Convention* (or an entirely new, separate treaty) to address this issue.[124] This confirms that transnational access to data, and the "pulling" of data from other countries without the consent of such other countries, is still seen as clearly contrary to public international law and that the contentious *Cybercrime Convention* article, by itself, does not express such consent.

Principle 13: SAFEGUARDS AGAINST ILLEGITIMATE ACCESS

The final principle draws upon a range of international standards concerning the protection of privacy rights. First, the duty of governments to deter unlawful surveillance by way of criminal and civil sanctions reflects the requirements of international human rights law to protect individuals from breaches of their privacy, not only by the state but also by private individuals.[125] Second, the need for avenues of redress likewise reflects international standards concerning the right to an effective remedy for violations of human rights.[126]

Third, the need to provide effective protection for whistleblowers flows from several international instruments, including Article 19 ICCPR and the UN Convention against Corruption (2005).[127] Several UN experts have emphasized the importance of whistleblowers in revealing wrongdoing by public authorities as well as human rights violations. In particular, the UN Special Rapporteur on Freedom of Opinion and Expression has underscored numerous times that whistleblowing is an important aspect of the right to freedom of expression.[128] More specifically, the UN Special Rapporteur on the Promotion

[124] On the conference, *see* Council of Europe, Octopus Conference—Cooperation against Cybercrime, 4-6 December 2013, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp. At the time of writing (December 2013), the minutes and conclusions from the conference had not yet been released, but the need for a new protocol was broadly agreed at the concluding session, even though the nature of this protocol was still very unclear, other than the "consent" options in an earlier 2013 paper were insufficient (they referred to consent by the data subject/suspect, which it was agreed could not be assumed to have been given voluntarily; and to consent to others with "lawful authority" to disclose data [read: Internet and e-communications service providers], who it was agreed were not in a position to make the relevant judgment on disclosure). The matter is therefore to be addressed in further study.

[125] *See*, *e.g.*, the judgment of the European Convention on Human Rights in *CAS and CS v. Romania*, no. 26692/05, 20 March 2012, at para. 71: "positive obligations on the state are inherent in the right to effective respect for private life under Article 8; these obligations may involve the adoption of measures even in the sphere of the relations of individuals between themselves."

[126] *See*, *e.g.*, Article 2(3)(a) ICCPR, Article 13 ECHR.

[127] *See also* Article 10 ECHR. In the seminal case of *Guja v. Moldova* (no. 14277/04, 12 February 2008), the Grand Chamber of the ECHR held that signaling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection. The Court went on to hold that in examining any interference with a whistleblowers' right to freedom of expression, special regard should be had to the public interest involved in the disclosed information (para. 74) and the motive behind the actions of the reporting employee (para. 77).

[128] *See*, *e.g.*, UN Committee on Human Rights, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain, submitted in accordance with Commission resolution 1999/36 E/CN.4/2000/63. 18 January 2000; *see also* the Joint Statement of the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and

and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism has stated that whistleblowers are crucial to "break illegitimate rings of secrecy" inside those intelligence and security agencies that are committing human rights violations, and that in these cases, the public interest in disclosure outweighs the public interest in non-disclosure.[129] He has further stated that whistleblowers should be protected from legal reprisals and disciplinary actions when disclosing unauthorised information and mechanisms for their protection is necessary.[130] Several Principles, including the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information,*[131] and the *Tshwane Principles on National Security and the Right to Information*[132] further elaborate on the kinds of remedies and protections that whistleblowers should be afforded.[133]

Fourth, the requirement to make evidence inadmissible where it was obtained in a manner inconsistent with the Principles underlines the need to ensure that all government agencies act in accordance with fundamental rights, which is in turn a core requirement of the Rule of Law. In some countries, the exclusionary rule against the use of evidence illegally obtained is absolute; reflecting a fundamental constitutional principle, *see*, *e.g.*, the "fruit of the poisonous tree" doctrine under US law.[134] In other jurisdictions, the rule is not necessarily absolute in nature[135] but the unlawful means by which the evidence was obtained is always an important factor for the courts to take into account when determining whether the individual has received a fair hearing. [136]

Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 21 June 2013.

[129] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin, A/HRC/10/3, 4 February 2009, para. 61.

[130] *Ibid*. For further information and standards on whistleblowers, *see* ARTICLE 19, *USA must respect international standards on protection of whistleblowers,* available at: http://www.article19.org/resources.php/resource/37133/en/usa-must-respect-international-standards-on-protection-of-whistleblowers.

[131] In particular, the Johannesburg Principles provide that no person may be punished on national security grounds for disclosure of information if (i) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (ii) the public interest in knowing the information outweighs the harm from disclosure.

[132] The Tschwane Principles provide that the law should protect from retaliation those disclosing wrongdoing if, *inter alia,* whistleblower "reasonably believed that there was a significant risk that making the disclosure internally and/or to an independent oversight body would have resulted in the destruction or concealment of evidence, interference with a witness, or retaliation against the person or a third party" and "reasonably believed that the public interest in having the information revealed outweighed any harm to the public interest that would result from disclosure."

[133] US law is particularly weak in this regard, *see* Trevor Timm*, If Snowden Returned to US for Trial, All Whistleblower Evidence Would Likely Be Inadmissible, 23* December 2013, available at: https://huffingtonpost.com/trevor-timm/if-snowden-returned-to-us_b_4495027.html. Moreover, while the Intelligence Community Whistleblower Protection Act in 1998 establishes a procedure for internal reporting within the agencies and through the Inspector General to the congressional intelligence committees, it provides no remedy for reprisals that occur as a result.

[134] *See Silverthorne Lumber Co v. United States*, 251 U.S. 385 (1920).

[135] *See*, *e.g.*, the judgments of the European Court of Human Rights in *Schenk v. Switzerland* (1988) 13 EHRR 242 and *Chinoy v. United Kingdom*, no. 15199/89, 4 September 1991.

[136] *See*, *e.g.*, the judgment of the European Court of Human Rights in *Khan v. United Kingdom* (2000) 31 EHRR 45 at para. 34: "The question which must be answered is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair. This involves an examination of the 'unlawfulness' in question and, where violation of another Convention right is concerned, the nature of the violation found."

Fifth and last, the need to destroy or return material obtained as a result of surveillance reflects well-established data protection laws across a wide range of jurisdictions.