Human Rights Committee Secretariat
Office of the United National High Commissioner for Human Rights
8-14 Avenue de la Paix
CH 1211 Geneva 10
Switzerland
Attention: Kate Fox/Sindu Thodiyil

February 14, 2014

I. Reporting Organization

This Shadow Report is submitted by Access, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), and Privacy International, as coordinators[1] of the coalition that drafted the International Principles on the Application of Human Rights to Communications Surveillance (The Principles).[2] The coalition, consisting of over 400 organizations continues to advocate for human rights protections in the changing digital surveillance landscape.

Many of the ICCPR's protections are endangered by mass surveillance, in particular, the rights to privacy (Article 17), freedom of expression (Article 19), and freedom of association (Article 22). We append to this submission the International Principles on the Application of Human Rights to Communications Surveillance ("The Principles") which consider how international human rights obligations, especially Article 17, apply to communications surveillance.

The Principles draw from existing international human rights law including the ICCPR, as well as the Universal Declaration of Human Rights (Article 12), United Nations Convention on Migrant Workers (Article 14), UN Convention of the Protection of the Child (Article 16); regional conventions including African Charter on the Rights and Welfare of the Child (Article 10), the American Convention on Human Rights (Article 11), the African Union Principles on Freedom of Expression (Article 4), the American Declaration of the Rights and Duties of Man (Article 5), the Arab Charter on Human Rights (Article 21), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8); Johannesburg Principles on National Security, Free Expression and Access to Information, and the Camden Principles on Freedom of Expression and Equality.

The Principles can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. With nearly 400 organizations and over 285,000 individuals endorsing the Principles, they speak to a growing global consensus that modern surveillance has gone too far and needs to be restrained.

II. Introduction

1The coordinators are: Access, the Electronic Frontier Foundation, Privacy International, the Centre for Internet and Society in Bangalore, and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC).

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

Since the release of the List of Issues, the public has learned much more about the scope and scale of surveillance conducted by the United States government.

The United States government's ongoing, indiscriminate surveillance of worldwide internet users, authorized by Executive Order 12333, PATRIOT Act Section 215, and FISA Amendments Act Section 702, is inconsistent with the rights enshrined in the ICCPR, including clear violations of the right to privacy under Article 17.

The aforementioned U.S. Government practices are also inconsistent with a number of the Principles, in particular, Legality, Necessity, Proportionality, Competent Judicial Authority, Transparency, Public Oversight, and Due Process.

III. Issue Summary

Executive Order 12333

Articles 17, 19, and 22 each place a legality requirements for restrictions on rights. Article 17 prohibits "arbitrary or unlawful interference" with privacy, Article 19 requires any restriction on expression be "provided by law," and Article 22 requires any restriction be "prescribed by law." It is widely believed that the U.S. government has interpreted Executive Order 12333 to authorize any surveillance activities that are not otherwise unlawful or unconstitutional. Traditionally, there has been very little public information about EO 12333, including the programs it authorized and any oversight thereof. According to recent reports, the NSA utilizes EO 12333 to collect, among other things, hundreds of thousands of contact lists from email and instant messaging services daily.[3] The US government avoids domestic legal constraints by operating these program overseas.

Furthermore, the Committee's General Comment 16 notes: ". . . relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis."[4] EO 12333 has never been approved by the legislature nor has the government identified the circumstances where it is utilized. The President's Review Group on Intelligence and Communications Technologies noted that EO 12333 has no requirement that the government meet any burden of proof before initiating surveillance.[5]

Measuring EO 12333 against the Principles reveals further shortcomings. Specifically, on legality, the Principles require a lawful interference be prescribed by a legislative act and individuals be granted notice of its application. Surveillance conducted under EO 12333 also fails to provide oversight or transparency as neither court nor legislative body oversees its operation and the public knows little-to-nothing about it.

PATRIOT Act Section 215

---

3 http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

4 http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument

5 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, 161, 266

Articles 19 and 22 require any restrictions on expression and association to be necessary. In the context of Article 22, restrictions must be "necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others." As noted by General Comment 16, surveillance must be conducted on a case-by-case basis, not bulk or widespread. Yet, the PATRIOT Act (Section 215) has been used to authorize bulk programs of questionable utility. Section 215 allows the government to collect "any tangible things . . . for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." The government interprets Section 215 to authorize NSA bulk collection of the metadata from millions of phone calls, if not every call, made in the US. However, the language of Section 215, which specifically requires the material be relevant to an "investigation," appears to be violated by bulk collection before relevance is proven or any particular investigation is initiated.

The necessity and proportionality of United States surveillance has been similarly called into question by recent reports on the effectiveness of bulk metadata collection under Section 215 of the PATRIOT Act.[6] A report by the New America Foundation found Section 215 played a role in initiating investigations in 1.8% of terrorist cases. In *Klayman v. Obama*, a federal judge expressed "serious doubt," given the evidence provided by the government, about the effectiveness of bulk metadata collection for cases involving "imminent threats of terrorism."[7] The Privacy and Civil Liberties Oversight Board (PCLOB) similarly concluded that "Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation." Ineffective programs that harm fundamental rights cannot be necessary or proportional.

Yet, metadata can be at least as intrusive of user privacy as the collection of content of communications, revealing, for example, relationships, medical information, and ideologies. As such, bulk metadata collection and other mass surveillance programs are particularly egregious violations of Article 17 of the ICCPR.

FISA Amendments Act Section 702

FISA Amendments Act (Section 702) programs suffer from a lack of legality, necessity, proportionality, and transparency. Section 702 authorizes "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." Under Section 702, the government creates lists of selectors, such as email addresses and telephone numbers, it believes relevant for national security investigations and which should provide 51% certainty the target is not a US-person. In the PRISM program, and potentially other similar programs, companies use lists of selectors to collect data from their servers. Not only does 702 authorize collection of a target's correspondence, but it has been interpreted to allow collection about the target as well.

---

6 http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0.pdf

7 http://www.nytimes.com/interactive/2013/12/17/us/politics/17nsa-ruling.html, 61-62

The lack of transparency limits public knowledge of the scope of collection under 702, though the authority has been at times used to collect a huge quantity of data. Legislation certainly does not "specify in detail the precise circumstances in which such interferences may be permitted," as outlined in General Comment 16. A tailored program, complying with the principles of necessity and proportionality would operate so that selectors are individually approved by the FISA Court based on actual evidence of their relevance to a national security interest, not only on their likelihood of returning data from non-US internet users.

FISA Court

Article 14 establishes due process as an element of civil and political rights by requiring a "fair and public hearing by a competent, independent and impartial tribunal established by law." The FISA Court (FISC) fails to ensure such protections, and fails to operate as an effective oversight body, in many respects. First, the independence of the FISC has been called into question. The court has rarely rejected a request for surveillance authorization. The Chief Justice of the Supreme Court appoints all FISC judges. Current Chief Justice John Roberts strongly favors judges with executive branch backgrounds.[8] The President's Review Group's recommended rotating appointment through the nine Supreme Court Justices so that they take turns appointing FISC judges. An impartial and independent institution should include judges with diverse backgrounds. Complaints have also been raised about the one-sided nature of the FISA Court. Generally, only the Department of Justice lawyers have access to the Court, unless a private party is challenging a FISA order or FISA judges request assistance from another attorney.

Relevant Question in List of Issues

> 1. Please clarify the following issues:
>
> (a) The State party's understanding of the scope of applicability of the Covenant with respect to individuals under its jurisdiction but outside its territory; in times of peace, as well as in times of armed conflict;
>
> 22. Please provide information on steps taken to ensure judicial oversight over National Security Agency surveillance of phone, email and fax communications both within and outside the State party. Please also specify what circumstances, as mentioned in section 206 of the USA Patriot Act, justify "roving" wiretaps.

U.S. Government Response

> 2. Issue 1(a). With respect to the scope of applicability of the ICCPR, the United States refers the Committee to ¶¶ 504 – 510 of its Fourth Periodic Report (CCPR/C/USA/4 and Corr. 1, hereinafter "2011 Report") [paragraph 505 reprinted below].
>
> 505. The United States in its prior appearances before the Committee has articulated the

8 http://www.nytimes.com/2013/07/26/us/politics/robertss-picks-reshaping-secret-surveillance-court.html?pagewanted=all&_r=0%20

> position that article 2(1) would apply only to individuals who were both within the territory of a State Party and within that State Party's jurisdiction. The United States is mindful that in General Comment 31 (2004) the Committee presented the view that "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 United States is also aware of the jurisprudence of the International Court of Justice ("ICJ"), which has found the ICCPR "applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory," as well as positions taken by other States Parties.

In General Comment 31, the Committee noted that "the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness . . . This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory." The extension of rights to individuals under effective control of a State Party is of particular importance given the global scope of U.S. surveillance. The Preamble of the Principles also notes their extraterritorial application. Regardless of where an internet user is located, surveillance is an interference with rights such as privacy and freedom of expression.

> 116. The FISC plays an important role in overseeing certain NSA collection activities conducted pursuant to FISA. It not only authorizes these activities, but it also plays a continuing and active role in ensuring that they are carried out appropriately. Moreover, if at any time the government discovers that an authority or approval granted by the FISC has been implemented in a manner that did not comply with the Court's authorization or approval, or with applicable law, the government must immediately notify the FISC and corrective measures must be taken.

As noted, FISC's oversight abilities are, in reality, limited. The FISA Courts effectiveness as an oversight body has been called into question by its own members. Chief Judge Walton called on the government to monitor its own compliance with FISA Court orders as the Court has little ability to effectively oversee the implementation of surveillance, though he expressed doubt about the government's compliance.[9] PCLOB,[10] the President's Review Group,[11] and a former FISA Court judge[12] have all recommended introducing an independent party into FISA Court to provide an alternative perspective, increasing the effectiveness of the Court.

> 119. The intelligence community is conducting court-authorized intelligence activities pursuant to a public statute with the knowledge and oversight of Congress. As described above, there is also extensive oversight by the executive branch, including DOJ and the

---

9 https://www.documentcloud.org/documents/785205-%C2%AD%E2%80%90pub-%C2%AD%E2%80%90march-%C2%AD%E2%80%902-%C2%AD%E2%80%902009-%C2%AD%E2%80%90order-%C2%AD%E2%80%90from-%C2%AD%E2%80%90fisc.html, 12

10 http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf, 17

11 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, 200

12 http://www.cbsnews.com/news/former-judge-admits-flaws-with-secret-fisa-court/

> Office of the Director of National Intelligence and relevant agency counsels and inspectors general. For example, activities authorized under Section 702 of FISA are subject to strict controls and procedures under oversight of the DOJ, the Office of the Director of National Intelligence, and the FISC, to ensure that they comply with the Constitution and the laws of the United States and appropriately protect privacy and civil liberties.

The existing oversight bodies have limited ability to function effectively. The United States Select Committee on Intelligence is one such oversight body, but last year the Director of National Intelligence James Clapper misled the Committee when asked about bulk data collection. Senator Wyden asked whether the US collects "any type of data at all on millions or hundreds of millions of Americans." Director Clapper responded "No Sir. Not wittingly."[13] The answer was provided shortly before the revelation of mass metadata collection under PATRIOT Act Section 215. None of the DOJ, Office of the Director of National Intelligence, counsels, or inspectors general are independent oversight bodies, which regularly report the public.

The U.S. government's surveillance activities and programs are also inconsistent with the Principle of transparency. Currently, the government does not release comprehensive statistics on the use of various surveillance authorities. The President's Review Group recommended "that legislation should be enacted requiring that detailed information about authorities . . . should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information." The government currently allows companies to release limited transparency reports, which are integral element of a transparent surveillance policy, but only a report by the government itself can provide a complete picture.

Recommended Questions

Additional questions could be asked to better contribute to the Human Rights Committee's understanding of the human rights impact of U.S. surveillance.

- What is the scope of surveillance under Section 702 and Executive Order 12333? What programs operate under each authority?
- What limitations are placed on the use of Section 702 and EO 12333 to protect the rights of non-US persons?
- Do any programs authorize the upstream collection of data?
- Are there any bulk surveillance programs other than those under Section 215?
- How does the FISA Court operate?

Suggested Recommendations

13 http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html

- Pass legislation that would end mass surveillance and introduce an independent advocate into the Foreign Intelligence Surveillance Court's processes.

- Refrain from the bulk collection under any authority. Instead, requests for foreign intelligence should be made if there are reasonable grounds to believe the information is relevant to a particular investigation and the order is limited in scope.

- Conduct regular studies of the NSA's surveillance authorities and programs to ensure necessity and proportionality and compliance with the ICCPR and the other international law.

- Recognize the intrusiveness of metadata surveillance.

- Increase protections for international users under Section 702 and EO 12333.

- Ensure greater transparency around surveillance powers and authorities. Transparency should be the default. Legal opinions, in particular, should be largely declassified.

- Ensure the FISA Court is properly advised on technical issues.

- Ensure the independence of the FISA Court by altering the method of selecting judges.

- Release comprehensive transparency reports, which include the total number of requests under specific authorities for specific types of data, and the specific number of individuals affected by each.

- Increase the oversight capabilities of PCLOB.

Appendix I

International Principles on the Application of Human Rights to Communications Surveillance

FINAL VERSION 10 JULY 2013

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

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

PREAMBLE

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

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

combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.

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

In order for States to actually meet their international human rights obligations in relation to communications surveillance, they must comply with the principles set out below. These principles apply to surveillance conducted within a State or extraterritorially. The principles also apply regardless of the purpose for the surveillance -- law enforcement, national security or any other regulatory purpose. They also apply both to the State's obligation to respect and fulfil individuals' rights, and also to the obligation to protect individuals' rights from abuse by non-State actors, including corporate entities.[6] The private sector bears equal responsibility for respecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and - where required - cooperating with State surveillance activities. Nevertheless, the scope of the present Principles is limited to the obligations of the State.

CHANGING TECHNOLOGY AND DEFINITIONS

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

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

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

When adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the

form as well as the scope and duration of the surveillance are relevant factors. Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.[9]

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

THE PRINCIPLES

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

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

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

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

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

sensitivity of the information and the severity of the infringement on the right to privacy.

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

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

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

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

COMPETENT JUDICIAL AUTHORITY: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. separate from the authorities conducting communications surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them.

DUE PROCESS: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,[10] except in cases of emergency when there is imminent risk of danger to

human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

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

1. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or
2. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

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

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

INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity,

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

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

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