access

MAY 2015

UNIVERSAL IMPLEMENTATION GUIDE FOR THE INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE

A PRODUCT OF ACCESS

accessnow.org

Table of Contents

The primary authors of this Guide are Amie Stepanovich and Drew Mitnick. Access and the authors would like to thank the following individuals for their valuable input, assistance, and feedback in the preparation of this guide:

Walid Al-Saqaf
Kevin Bankston
Roxana Bass
Jochai Ben-Avie
Brittany Benowitz
Deborah Brown
Jack Bussell
Fabiola Carrion
Alberto Cerda
Cindy Cohn
Hanni Fakhoury
Tomaso Falchetta
Mike Godwin
Natalie Green
Elonnai Hickok
Arne Hintz
Martin Husovec
Tamir Israel
Zeke Johnson
Lee Kaspar
Priya Kumar
Joy Liddicoat
Susan Morgan
Carly Nyst
K.S. Park
Alexandrine Pirlot de Corbion
Katitza Rodriguez
Naureen Shah
Sarah St. Vincent
Amos Toh
Francisco Vera
Timothy Wagstaffe
Kate Westmoreland
Cynthia Wong

We would also like to thank current Access staff who contributed substantial time to the completion of this document: Brett Solomon, Peter Micek, Raegan MacDonald, Estelle Masse, Javier Pallero, Michael Carbone, and Rian Wanstreet.

The Principles in Short

The International Principles on the Application of Human Rights to Communications Surveillance provide a framework for assessing human rights obligations and duties when conducting communications surveillance.

LEGALITY

Any limitation on the right to privacy must be prescribed by law.

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.

NECESSITY

Laws permitting Communications Surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a Legitimate Aim.

ADEQUACY

Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific Legitimate Aim identified and effective in doing so.

PROPORTIONALITY

Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

COMPETENT JUDICIAL AUTHORITY

Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent.

DUE PROCESS

States must 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.

USER NOTIFICATION

Individuals should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation.

TRANSPARENCY

States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities.

PUBLIC OVERSIGHT

States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

States should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.

SAFEGUARDS FOR INTERNATIONAL COOPERATION

Mutual Legal Assistance Treaties (MLATs) 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 should apply.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS

States should enact legislation criminalising illegal Communications Surveillance by public and private actors.

Preface

1. Introduction

The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") provide a framework for assessing human rights obligations and duties in the commission of communications surveillance. Access, the Electronic Frontier Foundation, and Privacy International led a broad consultation process to develop the Principles, which were launched in July 2013. The Principles have been endorsed by more than 400 civil society organisations, and referenced in debates on legislative reform in several countries and regions.[1]

This Implementation Guide provides more detail on how to apply the Principles in practice. It considers each stage of the process of a government application to access an individual's online information and gives examples and checklists for government agents, judges, and lawyers who are involved in processing applications to access User Data. The Guide is divided into five sections:

- Government Application for Information;
- Judicial Consideration;
- The Search;
- Appeals and Remedies; and
- International Cooperation.

The full text of the Principles is available in Appendix A. Appendix B provides a helpful checklist of the considerations that we examine herein. Appendices C and D serve as case studies to provide additional information on what surveillance conducted which protects human rights may resemble.

2. Legal framework on privacy and surveillance

Privacy is one of our most important rights — not only is it inherently valuable, it is also essential for the protection and promotion of other fundamental rights such as the freedoms of expression, movement, assembly, thought, and religion.[2] The right to privacy is recognized in international conventions and reflected in many countries' national

[1] *See, e.g.*, Report and Recommendations of the President's Review Group on Information and Communications Technology, *Liberty and Security in a Changing World*, Dec. 12, 2013, fn. 120, available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; Annual Report of the Inter-American Commission on Human Rights, Dec. 31, 2013, *available at* http://www.oas.org/en/iachr/docs/annual/2013/informes/LE2013-eng.pdf.

[2] *See* Frank La Rue, *Report of the Special Rapporteur to the on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/23/40 (April 17, 2013), avaliable at *http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf*.

constitutions and domestic laws.[3] Under international law, the right to privacy is framed as the right not to be "subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence."[4]

Following up on a December 2013 resolution by the United Nations General Assembly, the Office of the High Commissioner published a report on "the Right to Privacy in the Digital Age" in July 2014.[5] The Report, which repeatedly cites to the Principles, noted, "there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice."[6] In December 2014, a new UN General Assembly Resolution called upon States to review procedures, practices, and legislation to ensure that the right to privacy was upheld in commission of communications surveillance and asked for the Human Rights Council to consider establishing a special procedure on the right to privacy — such a procedure was adopted in March 2015 and a special rapporteur on the right to privacy was established.[7]

The right to privacy implicates certain necessary procedural and substantive safeguards.[8] The OHCHR report concluded that international law provides a "clear and universal framework for the promotion and protection of the right to privacy," but also found that many states evinced "a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight."[9]

---

[3] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Nov. 4, 1950, 213 U.N.T.S. 2889 [hereinafter ECHR]; American Convention on Human Rights art.11, Nov. 21, 1969, 1144 U.N.T.S. 143 [hereinafter ACHR]; *see, e.g.*, The Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act 2011 (Jamaica), s.13(3)(k); Constitution of the Federative Republic of Brazil, art. 5; Constitution of the Republic of South Africa, s.14.

[4] ICCPR art. 17. Article 11(2) of the ACHR states that "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation." Article 8 of the ECHR provides more direct guidance about the nature of permissible interferences; *see also Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, U.N. Doc. A/HRC/13/37, para. 17 (Dec. 28, 2009), available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf ("The permissible limitations test, as expressed in the general comment, includes, inter alia, the following elements: (a) Any restrictions must be provided by the law (paras. 11-12); (b) The essence of a human right is not subject to restrictions (para. 13); (c) Restrictions must be necessary in a democratic society (para. 11); (d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13); (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14); (f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14-15); (g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18)." (internal citations omitted)); UN Human Rights Committee (HRC), *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, Nov. 2, 1999, CCPR/C/21/Rev.1/Add.9, *available at http://www.refworld.org/docid/45139c394.html*.

[5] *The Right to Privacy in the Digital Age*, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Jan. 21, 2014); *The Right to Privacy in the Digital Age: Rep. of the Office of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/27/37 (June 30, 2014), available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[6] *Id.* at 5.

[7] *The Right to Privacy in the Digital Age*, G.A. Res. 69/166, U.N. Doc. A/RES/66/166 (Feb. 10, 2015); *Human Rights Council Agenda Item 3, The Right to Privacy in the Digital Age*, 28th Sess., A/HRC/28/L.27 (Mar. 24, 2015) [final pending].

[8] ICCPR art. 17, Declaring both a substantive right to privacy and procedural rights under the law.

[9] *Supra*, note 5, at 16.

Applying these concepts to real world situations has always been difficult. Modern technologies have compounded these challenges by making surveillance cheaper and easier while further blurring the privacy rights to be protected. Further complicating matters, laws, regulations, and formal procedures often move too slowly to keep pace with the newest technologies.

In June 2013, UN Special Rapporteur Frank La Rue issued a very timely report on government Communications Surveillance. Mr. La Rue concluded that, despite the clear existence of rights in international human rights law,[10] these laws and procedures are not sufficiently nuanced to provide clear guidance to individuals and governments when applying them in individual cases. The Principles started to fill this gap, and this Implementation Guide is intended to accompany the Principles and continue where they left off. It draws on existing human rights jurisprudence and explains how obligations apply to electronic Communications Surveillance for law enforcement, national security, or any other regulatory purpose. This Implementation Guide provides details on how to put the Principles into practice.

3. The Principles approach

Discussions about surveillance and access to user information are often fragmented and based on artificial and outdated distinctions. Whether or not they should, separate dialogues often occur in the contexts of national security and local criminal contexts. The Principles bridge this divide by focusing on the impact of surveillance on the user, rather than the nature of the information or the motivation of the government agent. They set out standards to protect users' rights, regardless of whether the government seeks access for law enforcement, national security, or intelligence-gathering purposes.

The Principles recognize that increasingly individuals trust more and more of their information in the hands of third parties, a process that often involves storage and transfers across multiple jurisdictions. However, this does not necessarily mean that individuals expect that their most personal information could or should be considered public or that government could be granted unfettered access to it. In fact, recent events demonstrate just how vast the discrepancy is between how users and governments interpret personal expectations of privacy. These users are now mobilizing to demand that government laws and practices be accountable and respect human rights.[11] The systematic violation of human rights undermines true national security and jeopardizes international peace and security.[12]

[10] La Rue, supra note 2.

[11] *See, e.g.*, Stop Watching Us (Sept. 17, 2014), StopWatching.US.

[12] UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, Sept. 28, 1984, E/CN.4/1985/4, *available at* http://www.refworld.org docid/4672bc122.html; see also OTI report by Danielle Kehl.

Terminology in this Guide

Account

is a record or collection of records created due to the interaction between a Target and another entity, which may be a user, organisation, network, company, or any other party.

Adjudicator

is an official of a Judicial Authority with authority to act with the force of law.

Application to Conduct Communications Surveillance or Application

is a document filed with a Judicial Authority seeking authority to conduct Communications Surveillance.

Communication

is any imparting, receipt, or exchange of information or data between a user and any other entity or entities, which may be any other user, organisation, network, company, or any other party. The Communication includes both the content as well as any metadata concerning that Communication, including but not limited to subscriber information, the identity of the parties to any communications, biometric information, location information, IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

Communications Surveillance

encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing, or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.

Court Order for Communications Surveillance or Court Order

is a document issued by a Judicial Authority authorising the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing, or similar actions taken with regard to information that includes, reflects, arises from, or is about a person's communications in the past, present, or future.

Device

means any piece of mechanical hardware used by a Target to collect, transmit, store, or communicate information or to facilitate the collection, transmission, storage, or communication of information.

Emergency Circumstances
are those in which there is an imminent risk or danger to human life and for which standards are defined explicitly in public law.

Formal International Channel
is a process for the exchange of User Data between jurisdictions. Any Formal International Channel provides clear guidance on which laws apply in situations involving multiple jurisdictions, clearly defines Protected Information, requires judicial authorisation for any access to Protected Information, applies a higher evidence threshold for more sensitive information, and provides clear guidance on sharing information under Emergency Circumstances.

Government Agent
means an agent, instrumentality, employee, contractor, or other person working on behalf of a government to conduct Communications Surveillance, and includes but is not limited to law enforcement agents, prosecutors, and national security officers.

Judicial Authority
is a competent and impartial government entity responsible for making determinations related to Communications Surveillance which is separate and independent from authorities legislating or conducting Communications Surveillance.

Legitimate Aim
is a predominantly important legal interest that is necessary in a democratic society, the primary purpose of which is not to infringe on any internationally recognized human right and the fulfillment of which does not discriminate on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, sexual orientation, or other status.

Necessary Information
is User Data that a Government Agent has identified as relevant to a Legitimate Aim and the Communications Surveillance of which represents the least intrusive means by which to investigate or pursue the Legitimate Aim.

Notice of Intent to Use Emergency Procedures
is advance, written notice of a plan to conduct Communications Surveillance when Emergency Circumstances exist which pre-empt the standard process to conduct Communications Surveillance. The notice must be provided to the same Judicial Authority which will receive and review the associated Application to Conduct Communications Surveillance.

Protected Information

is User Data that includes, reflects, arises from, or is about a user's communications and that is not readily available and easily accessible to the general public. This Implementation Guide applies exclusively and comprehensively to Protected Information.

Providers

refers to both content providers and service providers — companies and organisations that provide access to the Internet and related services. While these entities typically fall under separate legal regimes, the sensitive user information that they collect and store means they should safeguard user rights similarly against Communications Surveillance. "Providers" include:

- telecommunications carriers (e.g. America M6vil, Vodafone);
- information service providers (e.g. Comcast, Orange);
- interactive computer service providers (e.g. Google, Baidu);
- information content providers (e.g. BuzzFeed, BBC);
- applications and over-the-top service providers (e.g. Zynga, WhatsApp)

Repository

a record or collection of records created to store, process, or manage data by, for, or about a Target but is not necessarily generated by the Target's direct activity or communications.

Request for Assistance

is a written application for mutual legal assistance made pursuant to a Formal International Channel.

Request for Search or Request

is a written notice that a Judicial Authority has approved a Court Order for Communications Surveillance and identifying the specific Communications Surveillance that has been authorised. The Request for Search should include the identity of the Adjudicator having entered the Court Order and the requesting Government Agent, and all information on all available means of redress, remedy, or appeal.

Search

is Communications Surveillance according to a Court Order to Conduct Communications Surveillance or pursuant to the terms of a Notice of Intent to Use Emergency Procedures.

Target

is a User or other specific and identifiable entity identified as possessing Necessary Information and therefore subject to an Application to Conduct Communications Surveillance and any resulting Communications Surveillance authorised under a Court Order. A non-individual may be a Target in its own capacity but not for the purpose of obtaining access to its customers, users, or other individuals who are properly Targets in their own capacity.

User

is any single individual.

User Data

includes information or data to, from, created by, or about a User.

access

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

accessnow.org

Government Application for Information

1. Authority to make an application

Applications to Conduct Communications Surveillance must be made in accordance with the law.

Relevant principle(s): Legality

The ability for a Government Agent to conduct Communications Surveillance must be authorised by publicly available and discernable law that complies with international human rights laws. Such law must have been promulgated in a public forum and subject to open debate, and cannot be altered or otherwise construed by any secret document or opinion.[13] Government Agents must abide strictly by these provisions.

Implementing example:
General Comment 16 of the United Nations Human Rights Committee interpreting Article 17 states, "[t]he term 'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[14] "[R]elevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis."[15]

2. Necessity of a search

Communications Surveillance should only be requested when there is no less intrusive means that can be used.

Relevant principle(s): Necessity, Adequacy, and Proportionality

In order to conduct a Search to obtain Protected Information, a Government Agent must clearly demonstrate that Communications Surveillance is the least intrusive means that can be used to obtain Necessary Information in order to achieve an identified Legitimate Aim.

In order to do this, the Government Agent must specifically determine the scope of the Necessary Information. It is not enough that the Communications Surveillance is related to

[13] According to international standards, in developing Communications Surveillance laws, "[e]verybody should be informed and consulted in the process of law drafting" with limited exceptions. Provided information should clearly explain the issues addressed issues and extra precautions should be taken to ensure civil society involvement. *Transparency and Public Participation in Law Making Processes*, pg. 6-7, Organization for Security and Co-Operation in Europe, Oct. 2010, available at http://www.ecnl.org/dindocuments/381_Transparency%20in%20Law%20Making%20Eng.pdf.

[14] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, April 8, 1988, *available at*: http://www.refworld.org/docid/453883f922.html.

[15] *Id.*

the Target, the Legitimate Aim, or the Account, Device, or Repository to be searched. The scope of the Communications Surveillance, instead, must be narrowly tailored to minimize the impact on other Protected Information.

Implementing example:
In the case of Chaparro Alvarez and Lapo Íñiguez, the Inter-American Court of Human Rights recognized that intrusions into privacy must be "appropriate to achieve the purpose sought...necessary, in the sense that they are absolutely essential to achieve the purpose sought and that, among all possible measures, there is no less burdensome one in relation to the right involved, that would be as suitable to achieve the proposed objective. Hence, the Court has indicated that the right to personal liberty supposes that any limitation of this right must be exceptional and...that the measures are strictly proportionate, so that the sacrifice inherent in the restriction of the right to liberty is not exaggerated or excessive compared to the advantages obtained from this restriction and the achievement of the purpose sought."[16]

Implementing example:
In Canada, §186(1)(b) of the Criminal Code provides that wiretapping may be accepted as an appropriate investigative tool where "other investigative procedures are unlikely to succeed."[17] In R v Araujo, the Supreme Court of Canada interpreted this in light of "... two potentially competing considerations: enabling criminal investigations and protecting privacy rights."[18] Accordingly, in order to satisfy the investigative necessity test, the police must establish that there is no other reasonable or less intrusive method of investigation.

3. Format of the application

Applications to Conduct Communications Surveillance should be made in writing to a Judicial Authority and:
- clearly identify the requesting agency and officer; and
- certify as to the truth and accuracy of the information contained in the application.

Relevant principle(s): Due Process

In order to access Protected Information, a Government Agent must submit a written Application to Conduct Communications Surveillance to a Judicial Authority. The Application must include the name of the Government Agent seeking access, his or her position, proof of his or her valid authority to present the request, and his or her signature certifying the truth as to all included information.

[16] Chaparro Alvarez v. Ecuador, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 170 (Nov. 21, 2007), *available at* http://observatoriovihycarceles.org/en/hiv-and-prison-menu/jurisprudence-prison-menu.raw?task=download&fid=505.
[17] Criminal Code, R.S.C. 1985, c. C-46 (Can.).
[18] *R v Araujo* [2000] 2 S.C.R. 992 (Canada), *available at* https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1830/index.do.

The procedures by which a Government Agent files an Application to Conduct Communications Surveillance should be clearly delineated in law.[19] Regardless of his or her identity or position, a Government Agent must provide transparency into and take responsibility for the information contained in the Application (see below) in accordance with all applicable laws, including laws presumed within this Guide, and under the penalty of perjury.

Implementing example:
In the United States a certification would take the form of an affidavit presented under oath that accompanies the issuing warrant, subpoena, or other instrument.

4. Content of application

An Application to Conduct Communications Surveillance should clearly state:

- The Legitimate Aim that the Communications Surveillance seeks to accomplish and the Necessary Information sought to achieve that Legitimate Aim;
- The Target of the Communications Surveillance (if unknown, then all available facts related to the Target's identity should be included so that a reasonable person may verify that the Application relates to a valid Target);
- The relevant laws authorising the requested Communications Surveillance; and
- The precise scope of the requested Communications Surveillance.

Relevant principle(s): Legitimate Aim, Adequacy, Necessity, and Proportionality

All Applications to Conduct Communications Surveillance should explain what Legitimate Aim is served by the Communications Surveillance, the exact Necessary Information needed to achieve the Legitimate Aim, and why. The Application should explain why Communications Surveillance, including access to Protected Information, is required. The Application should also identify, to the fullest extent possible, the Target of the Communications Surveillance. A new Application should be submitted for every additional Target.

Finally, an Application must precisely describe the scope of the Communications Surveillance requested. A proper description of the scope should describe the Account, Device, or Repository subject to Communications Surveillance, the particular database thereon, any extraneous Protected Information expected to be accessed, the methodology to be used, the relevance of the Necessary Information to the identified Legitimate Aim, and the specific timetable, either in the time span over which they can acquire data or the period for which they have access to a certain Account, Device, or Repository.

[19] In common law countries, the application will typically be made by the law enforcement officer, whereas in civil law countries it is more common that the application be made by prosecutors. The Principles accommodate either system.

Implementing example:
The Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (ICCPR) explain circumstances in which limitations can be placed on international human rights, including on the basis of national security.[20] Although non-binding, the Siracusa Principles are considered persuasive interpretation of the ICCPR.

5. Burden of proof

The Application to Conduct Communications Surveillance should contain enough information to demonstrate to the Judicial Authority that:

- the Communications Surveillance will produce Necessary Information;
- the Necessary Information sought is contained in the identified Account, Device, or Repository subject to Communications Surveillance; and
- the identified scope of the Communications Surveillance (see above) is defined as to produce no more Protected Information than required to obtain the Necessary Information.

Relevant principle(s): Legitimate Aim, Adequacy, and Proportionality

Applications to Conduct Communications Surveillance must be reasonably supported and may not be part of a "fishing expedition." A Government Agent must provide sufficient detail in the Application to Conduct Communications Surveillance to demonstrate a sufficient nexus, defined clearly in public law, between the Account, Device, or Repository to be subject to Communications Surveillance and the Necessary Information identified. In order to meet this burden, a Government Agent must include the alleged acts and/or omissions that support the need for the Communications Surveillance and the lawfully acquired facts that provide the evidentiary basis for believing that the acts and/or omissions occurred. The facts in the Application must further support a finding that, to the greatest extent possible, the scope of the Communications Surveillance and the methodology to be used in the Search are appropriate and narrowly tailored to encompass the least amount of Protected Information in order to obtain the Necessary Information.

Implementing example:
In the U.S., in order to obtain a warrant, evidence must meet the standard of "probable cause" as required by the Fourth Amendment to the U.S. Constitution. "Probable cause" has been explained as a "fair probability that contraband or evidence of a crime will be found in a particular place."[21]

An application for a warrant should contain sufficient information to establish "probable cause" to believe that the evidence sought constitutes evidence of the commission of a criminal offence or represents contraband, the fruits of a crime or criminally derived

[20] UN Commission on Human Rights, *supra* note 11.
[21] *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

property. The application for a search warrant should also include reasonable grounds to believe that the evidence sought can be found at the specified location, along with a detailed description of the items to be seized, with sufficient specificity so as to identify them (for example, asking for specific records between certain limited dates or for specific personal property associated with the underlying crime).

6. Emergency procedures

Emergency procedures may be used under specific, enumerated Emergency Circumstances. In Emergency Circumstances, a Notice of Intent to Use Emergency Procedures must be filed before any Communications Surveillance may be undertaken. Then, an Application to Conduct Communications Surveillance must be filed with the Judicial Authority as soon as possible after the initiation of the Search. If the application is denied then Search must promptly stop and all information must be immediately destroyed.

Relevant principle(s): Legality, Due Process, and Safeguards Against Illegitimate Access

In a situation where Communications Surveillance is otherwise authorised and when the law provides specifically for their use, emergency procedures may be used to expedite the initiation of Communications Surveillance. Emergency procedures should only be used in situations where Emergency Circumstances are determined to exist. In Emergency Circumstances, a Notice of Intent to Use Emergency Procedures must be filed prior to the start of the Communications Surveillance that gives notice that emergency procedures are to be used. However, if the Government Agent determines at any time that the Emergency Circumstances no longer exist, they must immediately cease the Search and return to non-emergency protocols.

The Notice of Intent to Use Emergency Procedures must clearly demonstrate what Emergency Circumstances exist that require the use of emergency procedures, and how those Emergency Circumstances meet the established standard. As soon as possible after the Search is initiated, a full Application to Conduct Communications Surveillance must be filed within a timeframe established by law, preferably within 24-72 hours from the initiation of the Search.

Mere risk of flight or destruction of evidence should never be considered as a sufficient basis to justify the use of emergency procedures.

Implementing example:
In the Republic of Korea, whenever there is an imminent risk of a serious crime being committed which may cause death or serious injuries to individuals, the investigating officer may conduct electronic surveillance without the authorisation of the court. However, he or she must obtain judicial approval of the use of surveillance within 36 hours of the surveillance having begun.[22]

[22] Protection of Communications Secrets Act, art. 8, Act n. 6626/2002, Jan. 2002, *available at* https://www.imolin.org/doc/amlid/Republic_of_Korea_Protection_of_Communications_Secrets_Act.pdf.

Judicial consideration

1. Adjudicating authority

An Application to Conduct Communications Surveillance must be made to a Judicial Authority that is impartial, competent, and independent.

Relevant principle(s): Competent Judicial Authority, Due Process, and Public Oversight

All Applications to Conduct Communications Surveillance require authorisation by a Judicial Authority, which makes a determination on the content and sufficiency of the Application.

The Judicial Authority must be impartial, competent, and independent.[23] As explained in the Principles, this means that the Judicial Authority must be separate from the branch to which the Government Agent conducting Communications Surveillance belongs, conversant in issues related to the legality of Communications Surveillance, the technologies used to do so, and international human rights laws, and have adequate resources in exercising the assigned functions.

Adjudicators must have access to sufficient training to be able to issue informed decisions, as well as access to individuals with technical, procedural, and other necessary expertise. Proceedings in front of the Judicial Authority should be public and transparent, and its decisions must be published. States should dedicate adequate funding to ensure that an Adjudicator can respond to Applications in a prompt manner, as required in time-sensitive investigations and particularly to limit the instances when it is necessary to use emergency procedures.

Implementing example:
In interpreting the Article 17 obligation on States not to unlawfully or arbitrarily interfere with individuals' privacy, the Human Rights Committee has stressed the need for independent, impartial adjudication.[24]

[23] Domestic and international laws enshrine the right to access to justice and fairness in a legal proceeding, with judges playing a prominent role in guaranteeing these protections. *See* La Rue, *supra* note 2, for discussion of the importance of an independent judiciary to adjudicate issues impacting on freedom of expression.

[24] *See e.g.*, UN Human Rights Committee, *Concluding Observations of the Human Rights Committee Poland*, UN Doc. CCPR/C/79/Add.110, July 29, 1999, *available at* http://www.un.org/en/ga/search/view_doc.asp?symbol=CCPR/C/79/Add.110 ("As regards telephone tapping, the Committee is concerned (1) that the Prosecutor (without judicial consent) may permit telephone tapping; and (b) that there is no independent monitoring of the use of the entire system of tapping telephones."); *UN Human Rights Committee, Concluding Oberservations of the Human Rights Committee*, UN Doc. CCPR/C/79/Add.89, April 6, 1998, *available at* http:llwww.un.orglenlgalsearchlview_doc.asp?symbol=CCPRlCl79lAdd.89. ("The Committee recommends that steps be taken to ensure that interception be subject to strict judicial supervision and that the relevant laws be brought into compliance with the Covenant").

Implementing example:
In Sweden, signals intelligence that is intended to collect intelligence data must be approved by the Defense Intelligence Court, which ensures that the surveillance is lawful and could not be conducted in a less invasive manner. The Court also evaluates if the value of the surveillance outweighs human rights intrusions.[25]

2. Sufficiency of application

A Court Order for Communications Surveillance should only issue if a Judicial Authority determines that the substance of an application for Communications Surveillance meets the legal, substantive, and procedural requirements, including the burden of proof.

Relevant principle(s): Legality, Due Process, Legitimate Aim, Necessity, Proportionality, and Adequacy

A Court Order to Conduct Communications Surveillance must only issue if the Judicial Authority determines that the Application meets all legal and substantive requirements and all procedures have been followed, as set out above. The Adjudicator has a separate, independent responsibility to ensure that an Application to Conduct Communications Surveillance contains all of the required information as spelled out above, including sufficient detail so that the Adjudicator, without additional information, can determine that the evidentiary standard is satisfied (see below).

When assessing the content of the Application to Conduct Communications Surveillance, the Adjudicator must ascertain that the information it is based upon is credible and was lawfully acquired. Any information that does not meet this standard cannot be considered when determining if the Government Agent has met his or her Burden of Proof.

3. Evidentiary standards

A Court Order to Conduct Communications Surveillance should only issue if an Adjudicator determines that the Communications Surveillance is necessary (see above) and that there is a sufficient nexus connecting the specific Account, Device, or Repository with the identified Necessary Information. The Court Order should only authorise Communications Surveillance that is narrowly tailored to encompass no more Protected Information than is required to serve a Legitimate Aim.

Relevant principle(s): Proportionality, Legitimate Aim, Adequacy, and Necessity

The Judicial Authority may only authorise Communications Surveillance that represents the least intrusive means to obtain identified Necessary Information in order to serve an identified Legitimate Aim.

[25] The Law Library of Congress, *Foreign Intelligence Gathering Laws*, December 2014, 34, *available at* http:llwww.loc.govllawlhelplforeign-intelligence-gatheringlforeign-intelligence-gathering.pdf.

Before a Court Order may issue, the Judicial Authority must also determine that the Government Agent has demonstrated a sufficient nexus between the Account, Device, or Repository on which Communications Surveillance is to be performed and the Necessary Information sought and that the scope of the Communications Surveillance is narrowly tailored to encompass no more Protected Information than is required to obtain the Necessary Information.

Implementing example:
In the U.S., in order to obtain a warrant, evidence must meet the standard of "probable cause" as required by the Fourth Amendment to the U.S. Constitution. "Probable cause" has been explained as a "fair probability that contraband or evidence of a crime will be found in a particular place."[26]

An application for a warrant should contain sufficient information to establish "probable cause" to believe that the evidence sought constitutes evidence of the commission of a criminal offence or represents contraband, the fruits of a crime or criminally derived property. The application for a search warrant should also include reasonable grounds to believe that the evidence sought can be found at the specified location, along with a detailed description of the particular items to be seized, with sufficient specificity so as to identify them (for example, asking for specific records between certain limited dates or for specific personal property associated with the underlying crime).

4. Format and content of court order

A Court Order to Conduct Communications Surveillance should be in writing, and should include the:

- name of the Judicial Authority, the identity of the issuing Adjudicator, and the date the Court Order issues;
- law(s) under which the Court Order is issued
- methodology of the Search to be employed;
- scope and duration of the authorisation; and
- the underlying Application to Conduct Communications Surveillance

When an Application to Conduct Communications Surveillance involves novel or unique factual or legal issues, the Adjudicator should also issue a written opinion explaining the issues and the rationale for the Adjudicator's decision to issue the Court Order.

Relevant principle(s): Proportionality, Adequacy, and Due Process

In order to facilitate an accountable process which is subject to public oversight, all Court Orders to Conduct Communications Surveillance must be in writing and clearly state the law or laws under which the Court Order issues. It should indicate the time and date that the

[26] *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Court Order is issued, as well as the name and position of the authorising Adjudicator. The supporting Application should be attached.

In addition, the Court Order must precisely describe the full scope of the authorisation, including the exact Accounts, Devices, or Repositories subject to Communications Surveillance, and the particular database, as well as the time frame during which the Communications Surveillance may occur, the methodology for the Search, and the means and methods by which the Communications Surveillance may be conducted. In addition, whenever possible the Court Order should identify the particular databases to be searched and, at a minimum, the types of files that constitute Necessary Information should be listed.

The Adjudicator should tailor the terms of the Court Order to the substantive allegations in the Application to Conduct Communications Surveillance. The Court Order should never authorise a greater scope of Communications Surveillance than what is requested in the Application, and, when appropriate, the Adjudicator should sufficiently narrow the authorisation so that Necessary Information is the only accessible Protected Information.

A Court Order to Conduct Communications Surveillance must specifically limit the time that Protected Information may be stored. Accordingly, the Court Order must provide for regular reports on all information obtained under the Court Order. This includes Protected Information that is not Necessary Information within the context of the identified Legitimate Aim or any Protected Information that is outside the scope of the Court Order. In addition, the Court order must require that Necessary Information within the scope of the Court Order may only be stored for a reasonable time, specified by the Adjudicator, not to outlast the resolution of the Legitimate Aim of the Communications Surveillance.

When an Application to Conduct Communications Surveillance involves novel or unique factual or legal issues, the Adjudicator should issue a written opinion explaining the issues and the rationale for the decision to issue the Court Order. The written opinion should be made public and the adjudicator should within it specifically explain any interpretation of the public law that was necessary in order to reach any relevant conclusion and the rationale behind that interpretation, citing to previous cases, opinions, or acts when appropriate.

5. Judicial oversight

It is the duty of the Judicial Authority to monitor the implementation of Court Orders to Conduct Communications Surveillance (or, in the case of a Government Agent who failed to seek or obtain a Court Order, some other Adjudicator). The Adjudicator should ensure that the State reports on the activities conducted under the Court Order.

Relevant principle(s): Necessity and Adequacy

The State should report to the Judicial Authority on all of the information, including Protected Information, that was acquired during the Search so that the Judicial Authority can ensure that the implementing Government Agent complies with all terms of the Court Order.

The Government Agent must segregate Necessary Information. The Government Agent should report regularly to the Judicial Authority throughout the commission of the Search and during the entire time the State retains Protected Information obtained as a result of the Search. This reporting should take place not less than every 30 days, and during shorter periods of time for more invasive or broader Searches. The report must identify the Necessary Information sought, the scope of Protected Information obtained through the date of the Report, the scope of Protected Information accessed that did not constitute Necessary Information, and the reason for the access.

Following the report, the Judicial Authority should order the destruction of any Protected Information that does not constitute Necessary Information unless there is evidence of impropriety and bad faith on behalf of the Government Agent. In this instance, the Adjudicator should order the immediate and effective quarantine of the information pending investigatory proceedings of the violating Government Agent. Further, the Adjudicator should order the destruction of all Protected Information, including Necessary Information, once it is no longer required for the Legitimate Aim for which it was obtained.

The report should also identify progress on compliance with the Judicial Authority's order for the destruction of Protected Information. The Government Agent must specify to the Judicial Authority the ways in which information has been destroyed. If the Adjudicator determines that the destruction process is being delayed or obstructed investigatory proceedings should be initiated to determine the reason for the delay or obstruction and appropriate discipline should be ordered, including, when appropriate, more frequent reporting.

6. Investigatory proceedings

Where investigatory proceedings are necessary, the Adjudicator who authorised the Court Order to Conduct Communications Surveillance (or, in the case of a Government Agent who failed to seek or obtain a Court Order, some other Adjudicator) should order the information relevant to the investigatory proceedings to be quarantined. A separate Adjudicator should be assigned to any investigatory proceedings and given stewardship over the relevant information. Once the investigatory proceedings are concluded the information should be destroyed.

Relevant principle(s): Legality, Competent Judicial Authority, Due Process, and Safeguards Against Illegitimate Access

Arbitrary and unlawful interferences with individuals' privacy are violations of human rights that undermine democratic governance.[27] Even minor interferences can constitute a grave violation when viewed in aggregate. Government Agents should be subject to investigatory proceedings for misconduct related to the Application for or commission of Communications Surveillance. In addition to the circumstances in this Implementation Guide where investigatory procedures are required, an Adjudicator should order investigatory proceedings for any instance where a Government Agent is determined to have violated the terms of the Court Order to Conduct Communications Surveillance. This should include when a Government Agent acts or orders another to act outside of the scope of the Court Order, knowingly accesses Protected Information that does not constitute Necessary Information, uses Protected Information for purposes other than the Legitimate Aim stated in the Application to Conduct Communications Surveillance, or violates any other substantive policy or procedure established by the Judicial Authority.

Investigatory proceedings should be public and should be assigned to an Adjudicator other than the Adjudicator who authorised the Court Order to Conduct Communications Surveillance. Upon any circumstance where investigatory procedures are required, the information that led to the need for investigatory procedures should be quarantined from any other information obtained in the commission of Communications Surveillance. During the course of the investigatory proceedings, stewardship over the relevant quarantined information should be given to the assigned Adjudicator. The information should never be used for any purpose outside of the investigatory proceedings. Once the investigatory proceedings have concluded, the Adjudicator should order all of the information destroyed.

Any Government Agent subject to investigatory proceedings should be prevented from continuing any work related to Communications Surveillance until the proceedings are closed. All work should be assigned to other Government Agents. The Adjudicator assigned to the investigatory proceedings should have authority to order any necessary discipline for the Government Agent, including suspension (with or without pay), termination, remuneration,

[27] La Rue, *supra* note 2

public apology, prolonged peer or judicial oversight and reporting, or other actions as enumerated by law. Investigatory proceedings should never pre-empt civil actions by an affected user. If a user opts to bring a civil action, the quarantine of the relevant information must continue through the civil proceedings before it is destroyed to ensure that it can serve any evidentiary purpose necessary (see the section on remedy for more information).

7. Emergency procedures

In Emergency Circumstances, a Judicial Authority must assess the Notice of Intent to Use Emergency Procedures and ensure that such Notice contains all necessary facts and allegations for the Adjudicator to determine if Emergency Circumstances exist. In these instances, the Judicial Authority should ensure that an Application to Conduct Communications Surveillance is filed within a reasonable timeframe after the Search is initiated and must review the Application under an expedited timeframe. The rationale for emergency procedures must be independently reviewed.

Relevant principle(s): Legality, Competent Judicial Authority, Due Process, and Safeguards Against Illegitimate Access

When a Judicial Authority receives from a Government Agent a Notice of Intent to Use Emergency Procedures, such Judicial Authority must receive the notice and ensure that it is immediately assigned to an Adjudicator. The Adjudicator must ensure that a complete Application to Conduct Communications Surveillance is filed within a reasonable timeframe after which the Search is initiated pursuant to the Notice. A reasonable timeframe should typically not be longer than 24-72 hours from the initiation of the Search.

The Adjudicator must consider both the content and the substance of the Notice of Intent to Use Emergency Procedures and the Application to Conduct Communications Surveillance on an expedited schedule.[28] If the Adjudicator denies the Application to Conduct Communications Surveillance, the Search must immediately cease and all Protected Information must be immediately destroyed, except in cases where the Adjudicator determines the Government Agent acted with impropriety and in bad faith, in which case the information should be quarantined pending investigatory proceedings. In egregious cases where the Application is found to be substantively lacking in form and/or substance, disciplinary sanctions should be pursued against the requesting Government Agent.

If the Application is accepted but modified, and the Adjudicator finds that the request for emergency procedures was valid, the Search should be immediately adjusted as to comport with the modified requirements, and Protected Information that no longer falls within the scope of the

[28] An example of adequate justification for the use of emergency procedures would be collecting location data to find a stolen car with a child locked inside. *TELUS Transparency Report 2013*, TELUS, 2013, *available at* http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Repo rt%202013%20-English.pdf)

Court Order should be immediately destroyed, except in cases where the Adjudicator determines the Government Agent acted with impropriety and in bad faith, in which case the information should be quarantined pending investigatory proceedings. If the Application is accepted in any form, but the Adjudicator finds that an Emergency Circumstance, as defined by law, did not exist, emergency procedures were not appropriate for any other reason, or the Government Agent failed to provide sufficient justification, then the Search may continue. However, Protected Information subject to a Search prior to the issuance of the Court Order must be immediately destroyed (pending any necessary investigatory proceedings or accompanying civil actions) unless the Adjudicator makes a finding on the record that the Government Agent obtained the Protected Information, or inevitably would have done so, lawfully from an independent source.[29]

Implementing example:

The Indian Telegraph Act permits emergency collection when the Search is confirmed within seven working days. If not confirmed, the Search has to cease and further Collection may only occur with prior approval. A Review Committee meets to determine whether the Search was conducted in accordance to the law. If not, the Committee may end the Search and order the destruction of Collected data.[30]

[29] See Murray v. United States, 487 U.S. 583 (1988).

[30] *Law Enforcement Disclosure Report*, Vodafone, 42 (Jun. 2014), http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforce ment_disclosure_report.pdf.

The Search

1. Scope of the search

A Search must comport with the specific terms of the Court Order and should not interfere with the integrity of a Provider's services.

Relevant principle(s): Necessity, Proportionality, Adequacy, and Integrity of Communications and Systems.

A Search must be precisely limited to the bounds of the Court Order to Conduct Communications Surveillance, or, in the case of the use of emergency procedures, to the reasonable terms of the Notice of Intent to Use Emergency Procedures entered prior to a Judicial Authority's determination on the related Application to Conduct Communications Surveillance. Any Government Agent that requires a Provider, as part of a Search, to reconfigure its architecture in any instance or turn over a code, password, or other piece of information that would provide access to a Device, Account, or Repository other than that belonging to the Target should be considered to have acted outside the scope of the Court Order.

Implementing example:
The Human Rights Committee has interpreted the requirement of "reasonableness" in article 17 of the International Covenant on Civil and Political Rights as implying that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[31]

2. Costs

Costs associated with a Search should be borne by the State.

Relevant principle(s): Safeguards Against Illegitimate Access

The State should reimburse Providers for their reasonable costs incurred in conducting a Search. The basis for all costs should be specified in law. Providers should not be allowed to contract with a State for any costs that are above or in addition to the reasonable costs as established by law and determined by a Judicial Authority to prevent the creation of any perverse financial incentive to conduct Communications Surveillance. Reimbursement should be provided within a reasonable time period, not to exceed 30 days from the date the costs are incurred.

Implementing example:
In Switzerland, the federal government requires reimbursement for the costs of complying with surveillance requests. The government maintains a compensation chart based on the type of surveillance.[32]

[31] UN Human Rights Committee, *supra* note 17, at para 8.3.

[32] Regulation on fees and compensation for the monitoring of Mail and Telecommunications, SR 780.115.1, April 7, 2004, *available at* http://www.admin.ch/opc/de/classified-compilation/20032564/index.html

3. Request for search

A Request for Search issued to a Provider should be in writing, and should specify the User Data the State is requesting the Provider to remit, the legal basis for the Request, the name and contact information for the Government Agent issuing the Request for Search and the Judicial Authority who has authorised the Search, and a brief explanation of how the User Data sought is encompassed by the Court Order. Any documents necessary to understand the scope of the authorised Search should be attached to the Request for Search.

Relevant principle(s): Due Process and Public Oversight

Each Court Order to Conduct Communications Surveillance may produce more than one Request for Search, depending on the Providers implicated by the Court Order. A Request for Search should be specifically tailored to the Provider to which it pertains. Providers should only accept a Request for Search when it:

- is made in writing;
- explains the legal basis for the request;
- identifies the official making the request by name and title;
- specifies the permitted scope, duration, and methodology of the search; and
- complies with all relevant legal or regulatory requirements.

The relevant Court Order to Conduct Communications Surveillance and the Application to Conduct Communications Surveillance should be attached, in full, to any Request for Search, as well as any other supporting documents filed that the Provider would need access to to understand the scope of the Request for Search.

4. User notification

The Target should be notified of a Search before it is conducted unless a Government Agent can demonstrate to a Judicial Authority that a delay is strictly necessary to prevent serious jeopardy to the purpose for which Communications Surveillance is authorised. Responsibility for notification resides with the State.

Relevant principle(s): User Notification

The State must notify a Target of a Court Order to Conduct Communications Surveillance in order to provide an adequate opportunity for the Target to challenge the validity of the Search and to assert any privileges that may attach to the information sought.

Notification should include information that would enable the Target to obtain legal guidance and, if he or she so chooses, to challenge the validity of the Court Order or the scope of the Search, including the Court Order itself and the Application to Conduct Communications Surveillance filed with the Judicial Authority.

In limited circumstances, notification may be delayed for a limited period of time upon request of the Government Agent and subject to approval by the Judicial Authority. Approval of a request for delayed notification should be subject to rigorous review and should never be automatic. Instead, delayed notification should only be granted if the Government Agent demonstrates that a delay is strictly necessary for preventing serious jeopardy to the purpose for which Communications Surveillance is authorised.[33] Potential considerations in making this determination may include:

- clear and present danger to the life or physical safety of an individual;
- flight from prosecution;
- evidence tampering; or
- witness intimidation.

A delay should only be granted for a well-defined, reasonable amount of time that should generally not exceed 30 days. If the delay needs to be extended beyond the initial period, the Government Agent must seek an extension from the judicial authority by showing:

- the Government Agent has complied with all requirements as enumerated in the Court Order to Conduct Communications Surveillance;
- a good faith effort to gather the Necessary Information within the time allotted and to resolve the circumstances which require a delay in notification; and
- demonstrable need for further extension.

Additional delays should be subject to the same process as the initial delay and must be subject to the same time limitations. Delays must not be granted indefinitely: the Target should be notified as soon as possible after the rationale for the delay has expired.

In addition to notification by the State, Providers should always be able to notify its users of Court Orders to Conduct Communications Surveillance.[34]

Implementing example:
In Japan, the Act on the Interception of Communications requires that the subject of intercepted communications must be notified of the interception within 30 days of the surveillance having been completed. Where an ongoing investigation might be compromised by such notice, a district court judge can extend the period of time within which the subject must be notified.

[33] *See, e.g. Klass v. Germany*, App. No. 5029/71, 2 Eur. H.R.Rep. 214 (1978).
[34] The role of companies in user notification is discussed further below.

5. Provider responses and challenges

Providers must only supply Protected Information in response to a Request for Search, supported by a valid Court Order. Where it appears that a Request for Search does not comply with the Principles and/or international human rights law obligations, Providers should demand further explanation and, where appropriate, challenge the legality of the request.

Relevant principle(s): Legality, Legitimate Aim, Necessity, Adequacy, Proportionality, Competent Judicial Authority, and Due Process

Upon receipt of a Request for Search, a Provider must only provide Protected Information to the State as consistent with the most narrow construction thereof.[35] Any ambiguity should be resolved in favor of the Target. If the State and the Provider disagree as to an ambiguity, a Judicial Authority should resolve the disagreement and issue a clarifying addendum to the Court Order to Conduct Communications Surveillance and/or the Request for Search.

If a Request for Search is inconsistent with the law or this Implementation Guide a Provider should refuse to provide any Protected Information, and should instead file a legal challenge to the Request for Search.[36] If a Request for Search is consistent with local law, but inconsistent with international human rights law and/or made during a time of political turmoil, a Provider must evaluate the human rights risks, and the legal and operational risks. The Provider should also evaluate the potential to avoid or limit responses to any Request for Search through unilateral or multistakeholder advocacy, negotiation, litigation, or direct resistance.

Providers should assess the human rights situation in each operating environment in which they do or plan to do business. As part of these assessments, providers should engage with local and international stakeholders, independent human rights experts, and internal or external counsel with specific knowledge of relevant local laws and regulatory requirements. Providers should avoid pursuing business in operating environments in which users' access or human rights are subject to egregious restrictions inconsistent with international human rights law and the rule of law. Providers should conduct ongoing due diligence on human rights-related risks and review the appropriateness of continuing to operate in specific environments.

[35] A provider should treat User Data with a presumption that it is Protected Information. If a Request for Search rebuts this presumption and clearly applies only to non-Protected Information the Provider should act in the best interests of the User and with respect to the protections in this Implementation Guide.

[36] This section should be read in conjunction with the Access Telco Action Plan, which provides detailed guidance for telecommunications companies on respecting human rights.

Implementing example:
The Access Telco Action Plan offers 10 principles and implementation guidance for telecoms and ISPs to better prevent and mitigate any adverse human rights impacts.[37] The Plan counsels providers that, "Requests from governments and partners to restrict users' access, freedom of expression, or privacy should be presumptively rejected." To push back against requests that would restrict user rights, providers should, "Engage in unilateral and multistakeholder dialogue, and advocacy as needed, with governments and business partners." Joining with peer companies to resist particular requests has enabled providers to successfully reject government demands that threatened human rights.[38]

Implementing example:
Obligations under international human rights law attach to States, rather than directly to companies. However, Providers have a responsibility to respect human rights.[39] The UN Guiding Principles on Business and Human Rights explains:

> The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights.[40]

The Guiding Principles on Business and Human Rights set out the nature of businesses' responsibilities, including obligations to conduct due diligence and provide effective access to remedy.

6. Data governance

Providers should use good data security hygiene and should not build surveillance or monitoring capability into their systems.

Relevant principle(s): Integrity of Communications and Systems and Transparency

Providers must be transparent with users regarding terms of use, privacy policies, and other forms of user guidelines or restrictions on user rights. This information should use accurate, clear, and accessible language and should be broken down by country and requesting entity.

In order to ensure that the exclusive means for States to gain access to User Data is through the process set out in this Implementation Guide, Providers should implement meaningful

[37] Access, *Telco Action Plan*, https://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf
[38] Access, "Update: SMS finally unblocked in Central African Republic," 25 July 2014, https://www.accessnow.org/blog/2014/07/25/update-sms-finally-unblocked-in-central-african-republic.
[39] *See* Joseph, Sarah and Castan, Melissa (2013), *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary 3rd ed, p541.*
[40] *Guiding Principles on Business and Human Rights: Implementing the Protect, Respect, and Remedy Framework*, (2011), HR/PUB/11/04, p13.

data security practices. In the first instance, this should mean that Providers collect no more User Data than necessary in the ordinary scope of business. Further, the Provider should take meaningful steps to protect the User Data that it does retain, including User Data maintained at rest in databases or otherwise as well as User Data in transit to or from other users, companies, internal systems, or otherwise.

Data security should always be enabled by default and any critical updates should be pushed through to the user without altering any established privacy settings or access controls. When possible, the Provider should give the user the ability to control his or her own data without Provider access. Providers should always use security best practices and should undertake regular security audits to ensure that standards, systems, and technologies are up to date.

User Data should not be retained for longer than it is necessary for the Provider in the ordinary scope of business. When User Data is no longer necessary, it should be immediately and definitively destroyed, both that on the Provider's systems as well as the systems of any third party with which it has been shared. User Data should only be shared with third parties under valid, legitimate agreements that are necessary in the Provider's ordinary scope of business and communicated openly to the user in a manner that is easy to understand. Providers should not build surveillance or monitoring capability into their systems, or collect or retain User Data purely for State surveillance purposes.

7. Provider transparency

Providers should have the ability to publish granular statistics and policies on compliance with Request for Search and should do so. Wherever possible, providers should ensure that users are notified when their data are accessed.

Relevant principle(s): User Notification and Transparency

Providers should document and publish responses to Requests for Search and conduct regular reviews of these responses. Providers' transparency reports should include the:

- total number of each type of request, broken down by legal authority, including the total number of requests under emergency procedures;
- total numbers for each type of information sought;
- total number of users and accounts targeted;
- total number of users and accounts affected;
- total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total requests received and total requests complied with;

- legal challenge rate, provided as a percentage of total requests received and total challenged; and
- total amount of costs reimbursed to the Provider by the State, as allowed for above.[41]

In States where it is unlawful to provide this information, Providers should actively work for the ability to issue transparency reports.

Implementing example:
Many of the providers implicated in the NSA PRISM program, including Google, Facebook, Yahoo!, and Microsoft, release regular transparency reports. In 2013, these companies filed suit in the U.S. Foreign Intelligence Surveillance Court to be released from gag orders that prevent them from reporting more granular details about their involvement with state surveillance.[42] They eventually reached an out-of-court agreement with the Department of Justice,[43] but Twitter has argued that current parameters still violate the freedom of speech.[44]

Outside the U.S., many telecom providers, including Telstra,[45] TeliaSonera,[46] and Deutsche Telekom[47] have begun releasing transparency reports. In June 2014, Vodafone released "the most detailed transparency report ever,"[48] describing the laws governing surveillance and reporting in 29 countries, its own policies and procedures, and statistics on government requests.[49] In addition, the provider revealed related risks to user privacy and free expression, such as where provider's personnel are employed by government security agencies, and where governments enjoy direct access to its networks.

[41] Civil society groups, investors, and trade associations, such as those that participate in the WeNeedToKnow Coalition, agree that regulations must allow companies to report on the specific number of requests received, of users/devices/accounts/repositories affected, and of authorities involved. Access, "We need to know: companies, civil society call for transparency on surveillance," July 18, 2013, https://www.accessnow.org/blog/2013/07/18/tech-companies-and-civil-society-join-call-on-the-us-governmen t-to-issue-tr.
[42] Sam Gustin, *Tech Titans Press Feds in Battle Over NSA Transparency*, Time, Sept. 10, 2013, http://business.time.com/2013/09/10/tech-titans-press-feds-in-battle-over-nsa-transparency/
[43] Office of Deputy Attorney General, Letter to General Counsels, Department of Justice, Jan. 27, 2014, http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.
[44] Jack Linshi, Twitter Pushing DOJ, FBI To Let It Disclose More Info on National Security Requests, Time, July 31, 2014, http://time.com/3063761/twitter-transparency-report/.
[45] Telstra Transparency Report, Telstra, March 2014, http://exchange.telstra.com.au/wp-content/uploads/2014/03/Transparency-Report_2014.pdf.
[46] TeliaSonera Transparency Report, TeliaSonera, Aug. 2014, http://www.teliasonera.com/en/sustainability/transparency-report.
[47] Deutsche Telekom, http://www.telekom.com/sicherheitsbehoerden.
[48] Peter Micek, *Vodafone reports on law enforcement access to user data, worldwide*, Access, June 6, 2014, https://www.accessnow.org/blog/2014/06/06/vodafone-reports-on-law-enforcement-access-to-user-data-worldwide.
[49] Law Enforcement Disclosure Report, Vodafone, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_securit y/law_enforcement.html.

Appeals and Remedies

1. Penalties for unlawful access

Laws should establish criminal penalties for unlawful access to Protected Information. States and companies should ensure that any user whose Protected Information is obtained in violation of international or domestic law has access to complaint mechanisms and to appropriate legal remedies. Unlawful access should be considered inherently harmful to the user to whom the information pertains.

Relevant principle(s): Safeguards Against Illegitimate Access

Legislation should prohibit unwarranted, unnecessary, disproportionate, or extra-legal attempts to conduct Communications Surveillance by either law enforcement agents or private actors.[50] Any Government Agent who is determined to have committed such a violation, or to have compelled another to do so, should be subject to investigatory proceedings (described above). Depending on the nature of the breach, additional appropriate penalties may include criminal sanctions, administrative discipline measures, and/or other direct fines to individuals who were involved in the wrongful Search.[51]

Users whose information is obtained without proper authorisation and in violation of any domestic or international law or regulation should be able to seek redress.[52] Potential routes for remedy should include civil legal actions against the State, as well as non-judicial mechanisms, such as independent ombudsmen or national human rights institutions.

In order to ensure proper access to judicial relief, the wrongful Search should be considered inherently harmful to the user to whom the information pertains. In instances where a wrongful Search can be proven, both actual and punitive damages should be possible, as well as legal fees and restitution.[53] Improperly seized information should be returned to the user when appropriate and all copies should be quarantined under control of an Adjudicator and destroyed after investigatory proceedings or related civil actions have been closed.

[50] UN Human Rights Committee, *supra*, note 17

[51] This section should be read in conjunction with Access' Guide, *Forgotten Pillar: The Telco Remedy Plan*, May 2013, https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_0nm6ii982.pdf, which provides information on how telcos can meet their responsibility to provide access to remedy under the UN Guiding Principles on Business and Human Rights.

[52] *Guiding Principles on Business and Human Rights: Implementing the Protect, Respect, and Remedy Framework*, (2011), HR/PUB/11/04, Guiding Principle 25, ("As part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy"}.

[53] See John Ruggie, *Protect, Respect, and Remedy: a Framework for Business and Human Rights*, para. 25, A/HRC/8/5, April 7, 2008, available at http://www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

While the duty to provide remedy rests primarily with States, Providers should:

- incorporate the question of remedy into due diligence;
- implement accessible and secure grievance mechanisms; and
- respond quickly and effectively to user complaints.[54]

Providers should also adopt appropriate procedures to assist users in seeking remedy, such as investigating alleged breaches, preserving evidence, acknowledging and apologising as appropriate, and providing compensation as necessary.

Implementing example:
Article 2(3) of the International Covenant on Civil and Political Rights states that each State Party has an obligation to "...ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity."[55]

2. Admissibility of unlawfully obtained information

Protected Information that is improperly obtained should not be admissible in any legal proceedings.

Relevant principle(s): Safeguards Against Illegitimate Access

Protected Information that is acquired in violation of domestic or international law, including the procedures in this Implementation Guide, should not be admissible in any legal proceeding (except for investigatory proceedings, as described above, or a related civil action). Evidence derived from such information should also be inadmissible except in proceedings against the responsible Government Agent to provide culpability (see above sections on investigatory proceedings and civil remedies).

Implementing example:
In Ireland, evidence obtained in breach of an accused person's constitutional rights is automatically excluded from criminal trial unless an adequate excusing circumstance exists.[56] Evidence obtained illegally but in compliance with the Constitution may also be excluded under a balancing test with factors that include the nature and extent of the Government Agent's illegality.[57]

[54] *Telco Remedy Plan, supra*, note 47 at 3.
[55] See also ECHR art. 13; ACHR art. 25
[56] People (DPP) v. Kenny (1990) IR 110.
[57] People (AG) v. O'Brien (1965) IR 142.

3. Government transparency

Governments should should regularly publish comprehensive statistics on requests made and granted for access to Protected Information.

Relevant principle(s): Transparency and Public Oversight

States should publish regular transparency reports that inform the public about usage of Communications Surveillance authorities and practices and demonstrate how Government Agents comply with domestic and international laws.[58]

States' transparency reports should include the:

- total number of each type of request, broken down by legal authority and requesting State actor, be it an individual, government agency, department, or other entity, and the number of requests under emergency procedures;
- total number and types of responses provided (including the number of requests that were rejected);
- total numbers for each type of information sought;
- total number of users and accounts targeted;
- total number of users and accounts affected;
- total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total requests received and total requests complied with;
- legal challenge rate, provided as a percentage of total requests received and total challenged;
- number of investigations into filed complaints and the results of those investigations; and
- remedies ordered and/or actions taken in response to any investigations.

Information should be explained quantitatively as well as qualitatively, so that any person is able to understand how Communications Surveillance takes place.

Implementing example:

In the criminal context, many States require their governments to publish statistics on the number of requests for surveillance made, granted, etc. For example, see §100e of the Criminal Procedure Code (Germany),[59] §170-172 of the Search and Surveillance Act 2012 (New Zealand),[60] and §195 of the Criminal Code (Canada).[61]

[58] State-produced transparency reports act in tandem with, and not separate from, provider reports. More information on what should be in a provider report is available above.

[59] Strafprozessordnung [StPO] [Code of Criminal Procedure], April 7, 1987, Bundesgesetzblatt (Federal Law Gazette), I at 1074, as amended, Section 100e "[Duty to Report]", *available at* http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0622.

[60] Search and Surveillance Act 2012, Section 170 "Annual reporting of search and surveillance powers by Commissioner" (N.Z.), *available at* http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM3330254.html.

[61] Criminal Code (R.S.C., 1985, c. C-46), Section 195 "Annual report", *available at* http://laws-lois.justice.gc.ca/eng/acts/C-46/page-100.html#docCont..

In the security context, however, there has been little progress. In June 2014, the Office of the U.S. Director of National Intelligence (ODNI) released a transparency report that, as expected,[62] fell short of the standards established in the Principles.[63] A Google official pointed out that the ODNI report used imprecise language, making it "impossible" to cross-reference the report with service provider reports.[64] Moreover, the ODNI report failed to outline when and how the information was used, thereby "provid[ing] no basis for evaluating the utility or legitimacy of the surveillance activities."[65]

Other countries are even more opaque. Currently, not a single member of the Council of Europe releases a transparency report that includes requests made pursuant to national security-related investigations.

[62] Access, *Obama Administration continues to thwart meaningful transparency on NSA surveillance*, Aug. 30, 2013, https://www.accessnow.org/blog/2013/08/30/obama-administration-continues-to-thwart-meaningful-transpar ency-on-nsa-sur.
[63] *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year* 2013, IC on the Record, June 26, 2014, http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.
[64] Richard Salgado, *A step toward government transparency*, Google Public Policy Blog, June 27, 2014, http://googlepublicpolicy.blogspot.com/2014/06/a-step-toward-government-transparency.html.
[65] Steven Aftergood, *ODNI Declassifies Data on Frequency of Surveillance*, Federation of American Scientitsts, June 30, 2014, http://fas.org/blogs/secrecy/2014/06/odni-frequency/.

International Cooperation

1. Choice of laws and procedures

When a Government Agent seeks Protected Information from a foreign jurisdiction, a Request for Assistance must use publicly-available Formal International Channels.

Relevant principle(s): Safeguards for International Communication

Government Agents seeking access to Protected Information from a foreign jurisdiction must follow the appropriate Formal International Channel. The details of the Formal International Channel should be publicly available, including in each of the official or predominant languages of the State parties to the agreement to ensure accessibility for all users who are potentially affected by the agreements and practitioners charged with implementing them.[66]

Formal International Channels provide clear guidance on which laws apply in situations involving multiple jurisdictions. When faced with a choice, the Formal International Channel should require that the law with the higher standard for protecting individual rights applies. Formal International Channels should also specify the scope of Protected Information States may seek in a Request for Assistance and should require that Communications Surveillance conducted pursuant to a Request for Assistance conform to the standards set out in this Implementation Guide. Formal International Channels must provide clear guidelines for handling of Emergency Circumstances, including what constitutes an emergency, processes to be followed, documentation requirements, and the need for follow-up authorisation.

Implementing example:
Mutual Legal Assistance Treaties (MLATs) are formal treaties that necessarily must be published and registered with the United Nations.[67] While arrangements for law enforcement cooperation or other less-than-treaty status arrangements are not included in this obligation, States should also make them publicly available.[68]

2. Authority for response

States must only comply with Requests for Assistance from foreign governments for Protected Information when the applicable Formal International Channel has been followed. Judicial Authorities should approve access to Protected Information when the Request for Assistance satisfies the law and meets the standards set out in this Implementation Guide.

Relevant principle(s): Safeguards for International Communication and Due Process

[66] Access is working to make MLATs more publicly accessible through [www.mlatinfo.org]
[67] U.N. Charter art. 1.
[68] *See* e.g., Rush v Commissioner of Police [2006] 150 FCR 165 (Finn J) (Austl.).

When one State submits a Request for Assistance involving Protected Information in the custody of another State, the State receiving the Request for Assistance must verify the validity of the Request for Assistance, the legal basis for compelling access to Protected Information, and the scope and methodology of the Communications Surveillance required are consistent with the publicly available Formal International Channel, international law, and this Implementation Guide. Judicial Authorities should review the Request for Assistance and must give approval prior to initiating any search or transmittal for or of Protected Information. The requesting State should certify and demonstrate that it has acted in accordance with their substantive responsibilities under the domestic and international law and followed all domestic legal processes.

3. Emergency procedures

In Emergency Circumstances, a Request for Assistance for Protected Information should be initiated under the guidelines of the applicable Formal International Channel. The Request for Assistance for Protected Information should be made through (1) an administrative request or (2) a provisional order from a Judicial Authority.

Relevant principle(s): Legality, Competent Judicial Authority, Due Process, and Safeguards Against Illegitimate Access

A Government Agent may make a Request for Assistance for Protected Information via a Formal International Channel under Emergency Circumstances by seeking an administrative application or a provisional order from a Judicial Authority. In either instance, the Government Agent must certify that there are reasonable grounds to believe Communications Surveillance will ultimately be approved by a Judicial Authority of the State receiving the request. As soon as possible after the Request for Assistance is made under Emergency Circumstances, the State seeking the Protected Information should submit a follow-up authorisation request under non-emergency protocols through the Formal International Channel. If a Government Agent or Judicial Authority of either the seeking or receiving State determines at any time that the Emergency Circumstance no longer exists, the parties must return to non-emergency protocols.[69]

[69] Similar emergency protocols exist for international asset recovery; see Jean-Pierre Brun et al., *Asset Recovery Handbook: A Guide for Practitioners*, The World Bank and United Nations Office on Drugs and Crime, 135-6, 2011, *available at* http://www.unodc.org/documents/corruption/Publications/StAR/StAR_Publication_-_Asset_Recovery_Handb ook.pdf.

4. Safeguards and grounds for refusal

All agreements for the international transfer of Protected Information must include human rights safeguards. States should only initiate and maintain full cooperation relationships with States whose justice systems adequately protect human rights. States should ensure that any request for User Data complies with international law and policies and human rights.

Relevant principle(s): Safeguards for International Communication

All Formal International Channels must include human rights safeguards. The agreements should require the refusal of any requests for assistance that raise human rights concerns, such as a serious risk of a user being subjected to torture or the death penalty on the basis of the requested Protected Information. Protected Information should only be provided where the acts or omissions constituting the offence would have constituted an offence if they had occurred in the requested State (i.e., dual criminality).

Before entering into an agreement to cooperate with one another, States should analyse each other's criminal justice systems to determine whether they adequately protect human rights. States should periodically review these assessments to ensure other States are complying with human rights standards.

Implementing example:
Article 4 of the UN Model Treaty on Mutual Assistance in Criminal Matters contains grounds for refusal in circumstances such as where the request relates to a political offence, raises double jeopardy concerns or involves persecution on the basis of race, sex, religion, nationality, ethnic origin, or political opinions. However, these are not mandatory protections.[70]

[70] UN General Assembly, *Model Treaty on Mutual Assistance in Criminal Matters : resolution l adopted by the General Assembly.*, April 3, 1991, A/RES/45/117, *available at*: http://www.refworld.org/docid/3b00f21e1c.html.

APPENDIX A:

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

LEGALITY

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

LEGITIMATE AIM

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

NECESSITY

Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.

ADEQUACY

Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific Legitimate Aim identified.

PROPORTIONALITY

Communications Surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests. This requires a State, at a minimum, to establish the following to

a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

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

COMPETENT JUDICIAL AUTHORITY

Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. Separate and independent from the authorities conducting Communications Surveillance;
2. Conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
3. Have adequate resources in exercising the functions assigned to them.

DUE PROCESS

Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practised, 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, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

USER NOTIFICATION

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

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

The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

TRANSPARENCY

States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance.

PUBLIC OVERSIGHT

States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance. 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 comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations; to publish periodic reports and other

information relevant to Communications Surveillance; and to make public determinations as to the lawfulness of those actions, including the extent to which they comply with these Principles. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

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

SAFEGUARDS FOR INTERNATIONAL COOPERATION

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

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS AND RIGHT TO EFFECTIVE REMEDY

States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through Communications Surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.

APPENDIX B:

Principles' Implementation Guide Checklist

Capitalised words below are included in the Terminology on page six

I. The Request

- Based on publicly available, discernable law;
- Applicable to only a single Target;
- Narrowly tailored to minimize the impact on Protected Information;
- Written and signed by a Government Agent and Approved by an independent and competent Judicial Authority, who evaluates the request based on both the content and the sufficiency;
- Describes the Account, Device, or Repository subject to Communications Surveillance, the Necessary Information sought, any Protected Information that may be incidentally accessed, the methodology to be used, and the specific timetable for the Communications Surveillance;
- Establishes that the Necessary Information sought is contained in the Account, Device, or Repository identified for Communications Surveillance;
- Demonstrates a sufficient nexus between the Account, Device, or Repository to be subject to Communications Surveillance and the Necessary Information sought;
- Where emergency procedures are used, a formal application is filed within 24-72 hours after the initiation of the Search.

II. The Court Order

- Issued and signed by an impartial, competent, and independent Judicial Authority;
- Pursuant to public and transparent proceedings;
- Based on credible, lawfully acquired information;
- In writing, identifying all underlying legal authorities and with the request attached;
- Describes the full scope of the authorisation, including the Accounts, Devices, or Repositories to be subject to Communications Surveillance, as well as the scope, timeline, and methodology for the Communications Surveillance;
- Narrowed to ensure minimal incidental access to Protected Information;
- Limits the retention time for all Protected Information to a reasonable time, not to outlast the resolution of the Legitimate Aim of the Communications Surveillance;
- Includes a written opinion explaining the issues and the rationale for the decision in all cases of novel or unique factual or legal issues;

- Requires reporting on all Protected Information acquired during the search, including collection, access, retention, and eventual destruction; and
- In the case of emergency procedures, limits the authorisation to the time reasonably necessary for the Government Agent to complete a proper request.

III. The Provider's Response

- Responds only to Requests in writing and including the identify of the Government Agent making the request as well as a clear description of the scope, duration, and methodology of the Communications Surveillance to be conducted;
- Formally challenges all Requests outside the scope of domestic or international laws that should be formally challenged;
- Unless legally prohibited from doing so, requires notification to the user of the request;
- Limits the Search precisely to the bounds of the Request and provides no more information than the most narrow construction requires; and
- Provides regular transparency reports to document all Requests.

III. Execution of the Court Order

- Notifies the Target of the Court Order and provides an adequate opportunity to challenge the validity of the Search unless there is a demonstration that a delay is necessary;
- Regularly reports back to the Judicial Authority all of the Protected Information acquired during the Search;
- Segregates relevant information, promptly discards irrelevant information, and destroys evidence at the conclusion of the case or when it is no longer required;
- Respects Formal International Channels for any Request to or from an international jurisdiction;
- Prevents the use of any Protected Information that was not legally obtained from being used in any judicial proceeding or as the basis for further investigtations;
- Reimburses all costs to Providers within a reasonable time; and
- Compiled within regularly published transparency reports on the usage of Communications Surveillance authorities and practices.

APPENDIX C:

Case study 1: Twitter Parody Case in Chile

In 2011, a blogger named Rodrigo Ferrari created a Twitter account with the username "@losluksic." The account included a picture of three members of the Luksic family, one of the wealthiest families in Chile.[71] Behind the picture of the three relatives were images of money bills. The account tweeted comments like "tenemos cualquier plata" ("we are so loaded").

One of the family members, Mr. Andronico Luksic, filed a criminal complaint for the creation of this account and for two other accounts ("@andronico_luksic" and "@luksic_andronico"). The complaints were based on a misdemeanor, "usurpaci6n de nombre" ("name usurpation") whose single element is the appropriation of another person's identity.

Twitter is outside Chilean jurisdiction because its headquarters and servers are in California. Therefore, the prosecutor from the Chilean Public Ministry filed a request to the U.S. government under the Inter-American Treaty on Mutual Assistance in Criminal Matters seeking the IP addresses of the Twitter accounts and the identity and contact information of their owners. The prosecutor skipped the mandatory step under the Chilean Criminal Procedure Code of seeking judicial authorisation.[72]

In response to the MLAT request, Twitter provided the IP addresses to the prosecutor. The prosecutor then directly asked the Chilean mobile phone provider, V.T.R. Telecomunicaciones, for the ISP account information linked to the IP addresses. V.T.R. Telecomunicaciones provided Rodrigo Ferrari's information. Although Mr. Ferrari is only the owner of the "@loslukic" account, the prosecutor charged him for creating all three accounts based on deficient and misconstrued police reports.

On April 1, 2013, a judge in Chile dismissed the charges against Mr. Ferrari ruling that it was clear that the "@losluksic" account was a parody account, and punishing him would infringe the fundamental right to freedom of expression.

Lessons Learned

The Chilean Government

- The Chilean prosecutor should have sought judicial authorisation before sending a request to the U.S. government, and again before sending a search request to V.T.R. Telecomunicaciones (due process).

[71]Forbes, Worlds Richest Families: Andronico Luksic & family (2005), *available at* http://www.forbes.com/static/bill2005/LIR0CJD.html.
[72] Unlike U.S. law, which does not require a court order for subscriber information, Chilean law dictates that any search for information must be approved by a judicial authority.

- The Chilean Public Ministry should have confirmed that all requirements under Chilean law had been met before sending the MLAT request to the U.S.. This includes judicial authorisation, as well as the broader issue of whether pursuing prosecution under this law is appropriate (due process, legality, proportionality).
- Since there were three accounts involved, the Chilean Prosecutor and the Chilean Public Ministry should have submitted separate search requests for each account (proportionality).

The U.S. Government

- The U.S. government should have required that the request satisfied dual criminality, particularly given the implications for freedom of speech (legality).
- The U.S. Department of Justice should have sought judicial authorisation from a U.S. court to access the user's IP address, which is Protected Information (competent judicial authority).

Twitter

- Twitter should have ensured that the request was specific and that the search was authorised by pertinent legal procedures (necessity, adequacy, legality, and proportionality).

V.T.R. Telecomunicaciones

- V.T.R. Telecomunicaciones should have refused to provide the information sought by Chilean prosecutors until served with a valid and properly issued court order (due process).

The Chilean Judge

- The judge correctly dropped the complaint against Mr. Ferrari, recognizing the account as a parody, which constitutes protected expression.[73] The judge should also have granted indemnification of legal costs and damages (safeguards against illegitimate access).
- The judge should have made sure that the Chilean prosecutor properly discarded all the information that relates to Mr. Ferrari (safeguards against illegitimate access).
- Civil, criminal, or disciplinary sanctions against the prosecutor and Public Ministry should be considered.

[73] Renata Avila, *#FreeRod: Preliminary Victory in Chilean Twitter Parody Case*, GlobalVoices Advocacy, (April 24, 2013, 17:48 GMT), http://advocacy.globalvoicesonline.org/2013/04/21/freerod-preliminary-victory-twitter-parody-case/.

APPENDIX D:

Case study 2: An Overreaching Subpoena — Surveillance of the Associated Press' Records

In May 2013, the U.S. Department of Justice sent a letter to the Associated Press ("AP") notifying them of a two-month search of call records of AP personnel from 2012. This covered approximately 20 work and personal phone numbers from 40 AP reporters and editors in three different states. Reports indicate that the Department of Justice (DOJ) was trying to uncover the source of information that the AP published a year before on a foiled terror plot.

In its letter to the AP, the DOJ stated that it had issued subpoenas to conduct the search (an administrative process, not requiring the approval of a judge). The New York Times revealed that telecommunications carriers (including Verizon Wireless) handed out the information to the DOJ without questioning whether they should make their customers aware of the search.[74]

Such conduct not only creates a chilling effect on the freedom of expression of journalists, but it also raises fears for human rights defenders, whistleblowers, and the general public. The widespread collection of information also violates the due process rights of the journalists, since their privacy was interfered with proper oversight or limitations.

The U.S. government has insisted that federal laws allow it to do non-content search through a subpoena. This case demonstrates that a lot can be revealed simply by searching a user's numbers, who that user calls, the length of calls, and the location where the calls were made. This calls for a revision of U.S. federal laws to ensure that a court warrant will be used every time a user's identify, associations, communications, and locations can be discerned.

Lessons Learned

The U.S. Attorney General's Office

- The Attorney General should have sought authorisation for the searches from an impartial, competent, and independent judicial authority (competent judicial authority).

- The request should have been narrowed in time and scope. Call records of 20 numbers from three different states involving more than 40 individuals for two months is an overbroad search (proportionality, adequacy, and necessity).

[74] Charlie Savage and Scott Shane, *Justice Dept. Defends Seizure of Phone Records, New York Times*, May 13, 2013, *available at* http://www.nytimes.com/2013/05/15/us/politics/attorney-general-defends-seizure-of-journalists-phone-record s.html?pagewanted=1&_r=2&hp..

- The search should have been limited to one court order per telephone number.
- The request should have demonstrated that other less burdensome techniques were exhausted, that this request was made pursuant to a Legitimate Aim, that there was a fair level of probability that the information would be found, and that this type of search was absolutely necessary to acquire the sought information.
- The government should have notified the AP (and other affected users) that their accounts were accessed as soon as possible (after any of the risks indicated in the section on notification exceptions had abated).

The Telecommunications carriers (including Verizon Wireless)

- The telecommunications carriers should have challenged the overly broad request and interpreted it as narrowly as possible.
- Unless the telecommunications carrier is prohibited from doing so, it should notify its clients promptly. While the government had the primary responsibility to notify the Associated Press, Verizon Wireless should have at least inquired whether it could notify the journalists.