Written Submission for the Inter-American Commission on Human Rights in support of the position advanced by the American Civil Liberties Union (ACLU)

Thematic Hearing on

Freedom of expression and communication surveillance by the United States

149th Ordinary Period of Sessions
October, 2013

Submmited by

The Electronic Frontier Foundation, Access, ARTICLE 19 - Mexico and Central America office, ARTIGO 19 - Brasil, Asociación por los Derechos Civiles, Asociación para el Progreso de las Comunicaciones, APC, Asociación para una Ciudadanía Participativa, British Columbia Civil Liberties Association, BC Freedom of Information and Privacy Association, Center for Technology and Society at Fundação Getúlio Vargas, Colectivo Contingente MX, Comisión Colombiana de Juristas, Data, DeJusticia, Derechos Digitales, Instituto DEMOS, Fundación Karisma, Fundación para La Libertad de Prensa, Open Media, ONG Hiperderecho, Privacy International, Propuesta Cívica, Rio Institute for Technology & Society, TEDIC and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

Table of Contents

Communication Surveillance by the United States and the Impact on Freedom of Expression on Non-U.S. Persons[1]

Introduction

The Electronic Frontier Foundation, Asociación por los Derechos Civiles, Access, ARTICLE 19 - Mexico and Central America office, ARTIGO 19 - Brasil, Asociación para el Progreso de las Comunicaciones, APC, Asociación para una Ciudadanía Participativa, British Columbia Civil Liberties Association, BC Freedom of Information and Privacy Association, Center for Technology and Society at Fundação Getúlio Vargas, Colectivo Contingente MX, Comisión Colombiana de Juristas, DATA, DeJusticia, Derechos Digitales, Fundación Karisma, Fundación para La Libertad de Prensa, Instituto DEMOS, Open Media, ONG Hiperderecho, Privacy International, Propuesta Cívica, Rio Institute for Technology & Society, TEDIC and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic provide this submission in support of the position advanced by the American Civil Liberties Union (ACLU) that the mass surveillance programs of the United States NSA violate fundamental human rights of both U.S. and non-U.S. persons (a term employed by the United States to describe any individual not a citizen of the United States or a lawful permanent resident). The focus of our submission, however, will address only the impact of these programs on the rights of the latter.

The primary objective of our submission is to explain how certain recently-admitted aspects of the NSA's programs impact the rights of non-U.S. persons, and to this end, will include a description of how the programs operate and how the U.S. legal system fails to protect this class of person. We will also describe some of the current efforts underway internationally to articulate how human rights laws, including specifically, the rights to free expression, privacy and association should be interpreted in this age of mass surveillance capabilities, including the technical ability to analyze communications and communications metadata in ways that have profound impacts on these rights. We hope this analysis will assist the Commission in its consideration of these issues during this hearing and in defining the perameters of a future in-depth investigation into the U.S. mass surveillance programs and their impacts on human rights in the Americas.

About us

Electronic Frontier Foundation (International)

EFF is the leading international non-governmental organization dedicated to the protection of the individual's fundamental rights online. EFF has over 24,000 dues paying members around the world, including in the Americas region, and has been active since 1990, defending existing

human rights in the digital environment and building a more free Internet for all, through impact litigation, policy advocacy and public participation.

EFF has expertise in the field of national security and surveillance for intelligence purposes. In this field, EFF has conducted legal proceedings in the United States courts since 1990. EFF staff have testified before the Congress of the United States on this topic, and the organization has currently two cases in the United States against the country's dragnet surveillance programs: Jewel v. National Security Agency, a case concerning the mass surveillance of communications within the United States by the United States' National Security Agency ("NSA"), and the First Unitarian Church v. National Security Agency, which challenges the collection of bulk phone records by the NSA, also known as the Associational Tracking Program. At the international level, EFF advocates for the protection of human rights online at the United Nations Human Rights Council, United Nations Internet Governance Forum, the Council of Europe, the Organization for Economic Cooperation and Development, and the Asia Pacific Economic Forum. Its staff testifies and gives advice on the legal ramifications of technology in the fields of privacy and freedom of expression before national legislatures and to governmental officials in different countries around the world.

Access (International)

Access is an international human rights organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. Access is staffed across the world - in Santiago de Chile, Brussels, Tunis, Washington, D.C., and New York. In 2012 it hosted the largest conference on digital rights in Latin America (RightsCon:Rio) and has an established network of over 40 leading digital rights groups and activists in Latin America.

ARTICLE 19 - Global Campaign for Free Expression (International)

Article 19 is an international freedom of expression NGO, based in London with regional and national offices in Brazil, Mexico, Bangladesh, Senegal and Kenya. ARTIGO 19 and ARTICULO 19 are regional offices of ARTICLE 19 in the Americas. ARTICLE 19, which takes its name from Article 19 of the Universal Declaration of Human Rights, works globally to protect and promote the right to freedom of expression, including the right to information.

Asociación por los Derechos Civiles (Argentina)

ADC is an Argentinean non-governmental human rights organization founded in 1995 with the aim of protecting human rights and strengthening democratic institutions. ADC has acted before the Inter-American Commission of Human Rights through cases and hearings on issues such as freedom of information, human rights in prisons, women's rights and freedom of expression. It has also produced reports to the United Nations Human Rights Council and holds ECOSOC status within the United Nations.

Association for Progressive Communications / Asociación para el Progreso de las Comunicaciones (Internacional)

The Association for Progressive Communications (APC) is a global network of more than 30 organisations in Africa, Asia, Latin America and the Caribbean, Central, East and West Europe and North America. We have worked on internet access and rights for more than 20 years including developing the APC Internet Rights Charter. APC advocates for promotion and protection of human rights online including for human rights defenders and women's human

rights defenders. We are active in the United Nations Human Rights Council and other treaty body mechanisms, carry out human rights monitoring and advocacy in the Universal Periodic Review with a focus on freedom of expression, freedom of association and in women's rights (particularly sexual rights online), among others.

Asociación para una Ciudadanía Participativa (Honduras)
La Asociación para una Ciudadanía Participativa is a civil organization, independent, staffed by professionals with extensive experience and training in various areas of human knowledge. Its mission is to promote respect for human rights in Honduras, helping to ensure that all people, aware of their rights and duties, participate in making decisions of common interest.

British Columbia Civil Liberties Association (Canada)
BCCLA is a non-government organization in British Columbia, Canadadedicated to the preservation, maintenance and extension of civil liberties and human rights in Canada. Founded in 1962, the BCCLA is the oldest civil liberties organization in Canada. It is based in Vancouver and is jointly funded by the Law Foundation of British Columbia and by private citizens through membership.

BC Freedom of Information and Privacy Association (Canada)
FIPA is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform.

Center for Technology and Society at Fundação Getúlio Vargas (Brazil)
Founded in 2003, the Center for Technology and Society (CTS) aims to study the legal, social and cultural implications resulting from the advancement of information and communication technologies. Research center from the law school of Getulio Vargas Foundation in Rio de Janeiro, CTS develops its activities with a focus on producing academic research and policy papers that may impact the development of public policies so they will uphold democracy, fundamental rights and the preservation of the public interest. The four lines of research developed by the center are: Creative industries, culture and access to knowledge; Industrial property, innovation and development; Internet governance and Human Rights; Digital democracy, communication and participation.

Colectivo Contingente MX (Mexico)
A digital activism collective founded in 2011 focusing on defending freedom of expression online. Along with other organizations, they run the campaign Internet para Todos ('Internet for All'), a constitutional reform to obtain access to internet as a fundamental right. Contingente MX provides legal defense to bloggers and users of social networks who have been unjustly arrested by state authorities for their activities.

Comisión Colombiana de Juristas (Colombia)
Since its creation in 1988, this Colombian nongovernmental organization has had a dual purpose: to contribute towards improving the human rights situation in Colombia, and to the development of international human rights law and international humanitarian law worldwide. The first purpose, associated with the situation in Colombia, is divided into two objectives: the validity of the social and democratic state under the rule of law, along with the achievement of

lasting peace based on human rights (particularly the rights to truth, justice and reparation, and land redistribution as a central element of the armed conflict in Colombia). The second purpose, aimed at developing instruments of international law, is pursued simultaneously with the work that we carry out with respect to Colombia at the international level, but its scope goes beyond the national borders and associates us with human rights promotion in the Americas and in the four other continents of the world.

DeJusticia (Colombia)

A group of Colombian professors founded Dejusticia in 2003 with the aim of engaging in debates about law, institutions and public policy, by drawing upon rigorous studies and actions that promote social inclusion, democracy, the Rule of Law, and human rights in Colombia and Latin America. DeJusticia is a center for applied research that seeks to influence public opinion, academic debate and public policy. To accomplish this objective, it combines research, strategic litigation, training and education, and diffusion. Its work is carried out in collaboration with networks of social organizations, research centers and human rights advocates both in Colombia and abroad.

Derechos Digitales (Chile)

Founded in 2004, ONG Derechos Digitales is an independent, non-profit and non-governmental organization, which mission is to defense and promote human rights in the digital environment. Its main working topics include Freedom of Expression, Access to Knowledge, Transparency and Democracy, Privacy and Personal Data Protection, and Consumer Protection.

Instituto DEMOS (Guatemala)

El Instituto DEMOS está concebido como un centro de pensamiento y formación que permita incidir en las políticas públicas a través del trabajo con jóvenes, mujeres y pueblos indígenas, desde la perspectiva y promoción de los Derechos Humanos, a través de la capacitación y el fortalecimiento de las capacidades organizativas y de funcionamiento de las organizaciones con las cuales trabaja. DEMOS promueve el desarrollo de propuestas alternativas al modelo de desarrollo del país y busca incidir democráticamente en la toma de decisiones, tanto a nivel local, como regional y nacional.

Fundación Karisma (Colombia)

Fundación Karisma is a Colombian not-for-profit organization founded in 2003 and located in Bogotá. Its mission is to support and promote the beneficial use of Information and Communication Technologies (ICT) in the Colombian and Latin American societies, and seeks a responsible and reflective appropriation of ICT in various sectors. The potential of ICT regulations to affect human rights and civil liberties has been the motivation for Karisma to develop and support initiatives in this field during the last years, both in Colombia and throughout the Latin American region.

Fundación para la Libertad de Prensa (Colombia)

Established in 1996, FLIP is a non-governmental organization that systematically monitors violations to press freedom in Colombia, develops activities that contribute to the protection of journalists and the media, and promotes the fundamental right to information. FLIP has as lines of work the protection of journalists, access to information, prevention of indirect censorship and fight against impunity.

Hiperderecho (Perú)

Hiperderecho is a Peruvian non-profit organization working to promote freedom and civil rights in the digital environments. Our mission is to enrich the public debate by enhancing wide understanding of tech policy issues and representing the users' interests in public debates and legislative processes. To accomplish that mission, we engage in a wide range of activities including research, media campaigns, public speaking and direct advocacy.

Rio Institute for Technology & Society (Brasil)

The Rio Institute for Technology and Society (Instituto de Tecnologia e Sociedade) is a non-profit think-tank specifically aimed at dealing with the interplay of technology and all it's social spheres: law, politics, economics, culture, development and democracy. Focused on an interdisciplinary approach, most of it is meant to be developed in collaboration with specialists from different fields, from lawyers to technologists, media experts, anthropologists etc. It is formally affiliated with the University of the State of Rio de Janeiro.

Privacy International (International)

Privacy International is a human rights organisation committed to fighting for the right to privacy across the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law, and advocate for strong national, regional and international laws that protect privacy. Established in 1990, Privacy International was the first organisation to campaign at an international level on privacy issues, and have advised and reported to international organisations like the Council of Europe, the European Parliament, the OECD and the UN Refugee Agency.

Propuesta Cívica (Mexico)

A human rights defender organization founded in 2005 and is specialized on defending journalist and human rights defenders.

Open Media (Canada)

OpenMedia.ca is a Canadian non-partisan, non-profit advocacy organization working to encourage open and innovative communication systems within Canada. Its stated mission is "to advance and support a media communications system in Canada that adheres to the principles of access, choice, diversity, innovation and openness

TEDIC (Tecnología, Educación, Desarrollo, Investigación y Comunicación (Paraguay)

We are non-profit organization in Paraguay that develops open technology and promotes digital rights for a free culture on the Web. TEDIC's mission is to further civic initiatives founded on the principles of common goods and those that stimulate individual and collective creativity by facilitating their work, designing technologies and platforms that encourage the transfer of knowledge and providing resources and free Web platforms to organizations and citizens alike. In light of that mission, we engage in a wide range of activities including advocacy, projects design, and training.

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (Canada)

CIPPIC is a law and technology clinic based at the Centre for Law, Technology & Society at the University of Ottawa's Faculty of Law in Canada.[1] CIPPIC's mandate is to advocate in the public interest on diverse issues arising at the intersection of law and technology. In pursuit of its

[1] Samuelson Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), <https://cippic.ca>

public mandate, CIPPIC regularly provides expert testimony before Canadian parliamentary committees, participates in the regulatory activities of various Canadian quasi-judicial bodies such as the Office of the Privacy Commissioner of Canada, appears at all levels of Canada's judicial system, and participates in various international Internet governance fora.

Disclaimers

Please note that this submission is not, and cannot provide a complete recitation of the facts of NSA surveillance. Our goal is to support the presentation by the ACLU, including to add information about the impacts and rights of non-U.S. persons under U.S. law. We also aim to provide some crucial information to the Commission, not a comprehensive description. We do not, for instance, discuss the foreign collection of communications information by the NSA, since the recent revelations are focused on the collection within the United States implemented since 2001. We also do not discuss the now-public efforts by the NSA to degrade security technologies or penetrate them. We also note that many facts are not publicly known since both the surveillance facts and legal analysis are still largely being kept secret by the government. Finally, none of these assertions should be taken as admissions or legal conclusions or in any other way as statements by any EFF clients.

Setting the Scene: Evolving Surveillance Technologies

The emerging details of the United States National Security Agency (NSA) mass surveillance programs have painted a picture of pervasive, mass, cross-border surveillance of unprecedented reach and scope. As we document below, the United States government has now admitted using its access to telecommunications and Internet networks to surveil Internet users both domestically and worldwide. While the NSA has long had broad authority under United States law to spy on foreigners abroad, it was, until recently, limited in practice to counter-espionage against foreign powers and their agents, not the mass surveillance of ordinary telecommunications users. The NSA was believed to be limited in its legal authority to conduct surveillance domestically inside the United States. But due to a series of technical advancements, unilateral and secret executive decisions, legal changes, and secret court opinions, it is now understood that the NSA is also conducting sophisticated mass surveillance of communication content and communications records of individuals across the world, including when their communications travel through U.S. networks or are stored by U.S. companies.

Initially, it is important to recognize that the NSA (along with other U.S. foreign surveillance authorities) has traditionally been granted nearly limitless legal capacity to surveil non-U.S. persons for foreign intelligence purposes, because U.S. national laws and constitutional protections provide limited protection to non-U.S. persons located outside the United States and little oversight aimed at surveillance programs targeting these individuals. Surveillance of members of this group, conducted outside the United States, has long occurred in practice, although the recent revelations indicate a much broader capability and actual collection, retention and use of non-U.S. based mass surveillance than has been documented to date. Furthermore, surveillance has being done for purposes that go way beyond national security. It can include commercial spying, it can include political spying on totally non-violent groups, environmental groups, gay rights groups, among others.[2] More importantly, recent revelations have signalled a dramatic increase in the extent to which data stored in the domestic United

[2] "Caso de espionagem dos EUA viola direitos humanos, diz Dilma na ONU," 09 September 2013, http://www.bbc.co.uk/portuguese/noticias/2013/09/130924_dilma_assembleia_onu_lgb.shtml (last accessed, 20 October 2013).

States (or merely transiting through it) is being accessed, analyzed and retained. For such surveillance, non-U.S. persons have been unable to detect or seek recourse against this unchecked surveillance as a matter of U.S. constitutional and statutory law in the United States.

Contrasted with more targeted attempts at interception and acquisition of data – attempts limited to data that is demonstrably likely to assist in the resolution or prevention of an actual crime or terrorist threat – this catch-all approach is excessively overbroad and interferes with privacy in ways that are not proportionate nor necessary to the objectives of national security.

Some of these collection methods, as discussed further below, include the wholesale collection of the entire contents of communications: telephone calls, online video chat footage, the contents of email, web searches and activities and more. Further, even those mass surveillance programs limited to the collection and retention of meta-data (information about communications, such as the parties to the communication, and time and place of the communication) are problematic, as metadata can be as revealing of individuals sensitive preferences and associations as the content of communications, if not more so.

These bulk collection programs represent a pervasive and continuous interference with the privacy of the communications of billions of users from around the world, including millions from the Americas. It also represents a clear need to consider how existing human rights law should apply in this new world of pervasive, mass surveillance.

Concerns over the growing capacity of states to interfere with the communications privacy of individuals have been raised by the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights in a joint declaration:

> "Effectively, in recent years, the technology available to states for capturing and monitoring private communications has been changing very rapidly. The Internet has created unprecedented opportunities for the free expression, communication, possession, search for, and exchange of information. It has thereby facilitated the development of large amounts of data on persons, including their locations, online activities, and with whom they communicate. All of this information, which is maintained in archives that are accessible and systematized, can be highly revealing. Because of this, its use by police and security forces running surveillance programs intended to combat terrorism and defend national security has increased without adequate regulation in the majority of the states in our region."[3]

The recently adopted International Principles on the Application of Human Rights to Communications Surveillance, which have been endorsed to date by over 280 international organizations, represent an attempt to highlight and address some of these concerns.[4] These

[3] United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, "Joint Declaration on surveillance programs and their impact on freedom of expression", 21 June 2013, available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1 (last accessed, 20 October 2013).

[4] International Principles on the Application of Human Rights to Communications Surveillance. https://en.necessaryandproportionate.org/text (last accessed, 20 October 2013).

principles provide a framework in which to assess whether surveillance laws and practices are consistent with human rights standards in the current digital environment.

The Principles focus upon legality, legitimate aim, necessity, adequacy, proportionality, judicial authority and due process. They also consider user notification, transparency, public oversight and safeguards, both for international cooperation and against illegitimate access.

The Principles document begins with an explanation of the problem:

> "The explosion of digital communications content and information about communications, or "communications metadata" -- information about an individual's communications or use of electronic devices -- the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale. Meanwhile, conceptualizations of existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.
>
> The frequency with which States are seeking access to both communications content and communications metadata is rising dramatically, without adequate scrutiny. When accessed and analyzed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications."

In the United States, since the revelations of increased NSA surveillance activities, most of the engagement in the courts and legislature—as well as the United States Administration's defense of the surveillance—has concentrated on the impact on the constitutional rights of United States citizens.

But we should take into account that this is an extremely important issue not only for U.S. citizens but also for citizens throughout the Americas region and around the world, and one on which we hope that the Commission will take action. We believe that this hearing should be the beginning of a sustained and active engagement by the Commission with these issues, and we hope our written contribution assist the Commission in this process. We make ourselves available to the distinguished Commission for further considerations.

Recent Revelations About U.S. Government Surveillance and Its Impact on Non-United States Persons

The basic authority for collection of information on non-U.S. persons exists in Executive Order 12333.[5] Thus, this collection and analysis is not done pursuant to U.S. statute or generally subject to oversight from the Foreign Intelligence Surveillance Court (FISA Court). Thus, any consideration of the mass collection and analysis of non-U.S. persons communications must include recognition that U.S.-based collection is not the only way, and potentially not even the primary way, that the NSA is collecting massive amounts of information about non-U.S. persons.

[5] Executive Order 12333 United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)) https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf (last accessed October 22, 2013)

Recent revelations have brought two additional domestic-based programs to light: PRISM and UPSTREAM.[6]

PRISM is the name of an internal government computer system established and implemented by the NSA.[7] It permits the NSA to access metadata and internet content from some of the largest internet service providers in the United States and the world, and other companies providing communications services, including Microsoft, Yahoo, Google, and Facebook.

UPSTREAM is a government program established by the NSA to copy traffic passing through the fiber optic cables of United States communications services providers, such as AT&T and Verizon.[8]

Between them, PRISM and UPSTREAM provide very broad access to the communications content and metadata of non-United States persons from inside the U.S.[9] They provide for the bulk seizure, acquisition, collection and storage of all or nearly all of the communications content and metadata of non-United States persons that passes through the United States. They also provide for various kinds of searching and analysis of that content and metadata with little or no restriction, in order to determine whether content is related to a United States person. Moreover, they appear to provide for additional searching and analysis of the content and metadata once the material is determined as unrelated to a United States person; or where it has been determined that it does relate to a United States person, but subject to one of many exceptions to the general exclusion of searching of data relating to United States persons.

The United States government claims that both programs are authorized under Section 702 of the Foreign Intelligence Surveillance Act 1978 ("FISA") (as amended by the Foreign Intelligence Surveillance Amendment Act 2008 ("FISAAA"), 50 U.S.C. § 1881a ("§702"). Other surveillance programs are authorized by §702, likely including many that have not yet been made public, but for purposes of this statement, we will refer to PRISM and UPSTREAM collectively as "§702 programs" or "programs."

Because of the network structure of the Internet -- which now carries a large number of telephone calls as well as what is conventionally thought of as "Internet" traffic such as email,

---

[6] Note that these names may not be the only names used to identify these programs. We understand that the NSA gives multiple names for each of its programs to better track how information about the programs is shared and otherwise travels both inside the NSA and outside the NSA.

[7] Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", Director of National Intelligence, 7 June 2013, available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-thecollection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act [7](last accessed, 20 October 2013).

[8] For example, *see,* "Brief summary of the testimony of Mark Klein, a former AT&T technician, and of expert witness J. Scott Marcus, a former Senior Advisor for Internet Technology at the FCC," available at https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf. The complete declaration of Mark Klein is available at http://www.eff.org/legal/cases/att/SER_klein_decl.pdf. The declaration of J. Scott Marcus is available at http://www.eff.org/legal/cases/att/SER_marcus_decl.pdf (last accessed, 20 October 2013).

[9] Under the FISA law, 50 U.S.C. §1801 (i) "United States person" means "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section."

web activity, social networking, chat and others -- PRISM and UPSTREAM together allow NSA access to a tremendous amount of non-U.S. persons' communications and metadata.[10] A 2010 Washington Post article discussing content and metadata reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."[11]

For instance, for just metadata, the 'Boundless Informant' documents published by The Guardian on 11 June 2013 show the agency collecting almost 3 billion pieces of intelligence from United States computer networks over a 30-day period ending in March 2013.[12]

A key feature of these programs is that they do not respond to specific operations or investigations, but are designed as broad, *a priori* authorizations for the NSA to collect a wide range of data concerning non-United States persons (as identified below in light of the United States legal framework). As explained further below, all of the oversight and limitation processes put into place for the programs are apparently aimed at ensuring protection for the communications of United States persons, despite being collected along with those of non-United States persons. Much of the discussion in the United States is about whether those steps are sufficient to accord with the legal protections in United States law of United States persons, but notably, for these purposes, none of those protections or processes are aimed at protecting non-suspect, innocent non-United States persons from having their communications or communications records collected or searched by the NSA or transferred to other countries.

The PRISM program was first revealed through newspaper reports in The Guardian and The Washington Post on 6 June 2013. These reports were based on disclosures to those newspapers by the former defense contractor employee Edward Snowden. The reports exposed the NSA's practice of "*collect[ing data] directly from the servers*"[13] of nine leading United States Internet companies, including Microsoft, Google, Yahoo, Facebook and Apple.

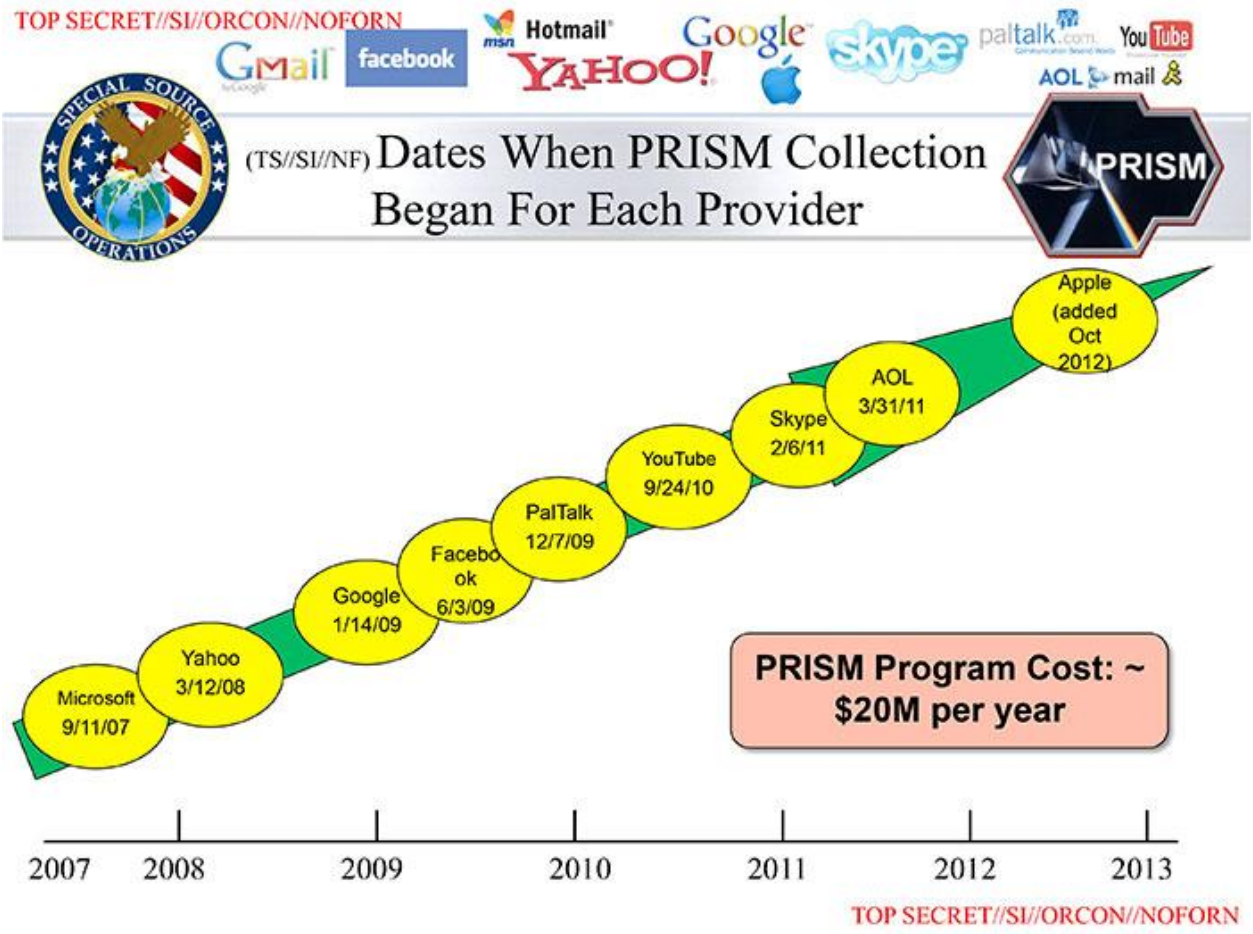
These companies had begun their cooperation with the NSA when Microsoft first joined the program on 11 September 2007. A timeline of this cooperation recording the program's annual cost to the NSA was set out in an internal NSA slide from April 2013 published by the newspapers:

[10] "Using Domestic Networks to Spy on the World," Katitza Rodriguez and Tamir Israel, available at https://www.eff.org/deeplinks/2013/06/spies-without-borders-i-using-domestic-networks-spy-world (last accessed, 20 October 2013).

[11] "Top Secret America: A Hidden World, Growing Beyond Control," Dana Priest and William M. Arkin, available at http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/ (last accessed, 20 October 2013).

[12] "Boundless Informant: The NSA's Secret Tool To Track Global Surveillance Data," Glenn Greenwald and Ewan MacAskill, theguardian.com, Tuesday 11 June 2013 14.00 BST, available at http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining; see also "How the NSA is still harvesting your online data," Glenn Greenwald and Spencer Ackerman, theguardian.com, Thursday 27 June 2013 16.03 BST available at http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection (last accessed, 20 October 2013)

[13] See slide on page 8.


TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

The Washington Post provided a helpful description of the operation of the system, in light of information from insiders with experience of the program:

According to the slides, through PRISM the NSA is able to "*[c]ollect[data] directly*" from U.S. service providers' servers and extract audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets as well as phone calls.[14]

> "According to slides describing the mechanics of the system, PRISM works as follows: NSA employees engage the system by typing queries from their desks. For queries involving stored communications, the queries pass first through the FBI's electronic communications surveillance unit, which reviews the search terms to ensure there are no U.S. citizens named as targets.
>
> That unit then sends the query to the FBI's data intercept technology unit, which connects to equipment at the Internet company and passes the results to the NSA. The

[14] "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", Barton Gellman and Laura Poitras, available http://www.washingtonpost.com/investigations/us-intelligence-miningdata-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (last accessed, 20 October 2013).

system is most often used for e-mails, but it handles chat, video, images, documents and other files as well."[15]

The scale of the operation is probably unprecedented. The Guardian's reports noted that over 2,000 Prism-based "reports" of communications were being issued every month by the NSA and that more than 77,000 intelligence reports had been made by June 2013.[16]

The UPSTREAM program copies traffic flowing through the United States Internet system and then runs it through a series of filters. These filters are designed to sift for communications that involve at least one person outside the United States and that may be of foreign-intelligence value, or that are subject to one of the other exceptions such as being encrypted or revealing a crime.

The Wall Street Journal reported that: "[…] there are two common methods used, according to people familiar with the system.

In one, a fiber-optic line is split at a junction, and traffic is copied to a processing system that interacts with the NSA's systems, sifting through information based on NSA parameters. In another, companies program their routers to do initial filtering based on metadata from Internet "packets" and send copied data along. This data flow goes to a processing system that uses NSA parameters to narrow down the data further."[17]

The existence of the UPSTREAM program was first exposed by AT&T Whistleblower Mark Klein[18] in 2006 and is the basis of EFF's Jewel v. NSA lawsuit, pending since 2008[19]. It was also the basis of an earlier case, Hepting v. AT&T, which was brought directly against AT&T but dismissed after Congress passed retroactive immunity for the companies assisting NSA in 2008[20]. The UPSTREAM program gives the NSA a copy of all content and metadata of all communications travelling over the fiber-optic cables of major American telecommunications carriers.

The PRISM and UPSTREAM programs are both used by the NSA to collect information from the United States' Internet infrastructure and between them, they give access to nearly all traffic traveling over or stored by the infrastructure. Indeed, the April 2013 Slides instruct NSA personnel to make full use of both programs:

---

[15] U.S., company officials: Internet surveillance does not indiscriminately mine data", 8 June 2013, http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-doesnot-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story_1.html (last accessed, 18 September 2013).

[16] "NSA Prism program taps in to user data of Apple, Google and others", Glenn Greenwald and Ewen MacAskill, The Guardian, Friday 7 June 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (last accessed, 18 September 2013).

[17] What You Need to Know on New Details of NSA Spying," Jennifer Valentino-Devries and Siobhan Gorman, 20 August 2013, 8:12 p.m. ET, available at

[18] Declaration of Mark Klein, available at https://www.eff.org/node/55051.

[19] Jewel v. NSA Case page: available at https://www.eff.org/cases/jewel.

[20] Hepting v. NSA Case page: available at https://www.eff.org/nsa/hepting.

The names "Fairview, Stormbrew, Blarney and Oakstar" reportedly refer to code names of the surveillance programs linked to each participating major telecommunications company in the U.S. including Verizon, AT&T and Sprint.[21]

Admissions by the United States Government

Since the newspaper disclosures, the United States government has publicly acknowledged the existence of the PRISM and UPSTREAM §702 programs and provided information about their operation. On 6 June 2013, the DNI confirmed PRISM's existence and explained that it was authorized under FISAAA.[22] The government has also confirmed that the various protections in the programs as well as the oversight regimes are aimed solely at protecting U.S. persons, not at non-U.S. persons.

On 21 August 2013, the DNI declassified two FISA court rulings confirming the existence of both §702 programs, and explaining problems with the UPSTREAM program.[23] Notably for these purposes, the problems arose from the retention and searching of United States persons' information. The bulk seizure, collection, search and analysis of the communications and communications records of non-United States persons was not questioned or limited by these decisions.

On 8 June 2013, the DNI provided a 'fact sheet' on the programs, setting out the Executive's understanding of their purpose and limits[24]. The fact sheet stated, in summary:

- PRISM is an internal government computer system used to facilitate the government's statutorily authorized collection of foreign intelligence information from electronic communication service providers under court supervision, as authorized by section 702 of FISA.
- Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States, under court oversight.
- Service providers supply information to the Government when they are lawfully required to do so. Under section 702 of FISA, the United States Government does not unilaterally

[21] "New Details Show Broader NSA Surveillance Reach" Jennifer Valentino-Devries and Siobhan Gorman, 20 August 2013, 11:31 p.m. ET, available at http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html#project%3DNSA0820%26articleTabs%3Darticle (last accessed, 20 October 2013).

[22] "U.S. Confirms That It Gathers Online Data Overseas", Charlie Savage, Edward Wyatt and Peter Baker, June 6, 2013, New York Times, http://www.nytimes.com/2013/06/07/us/nsa-verizoncalls.html?pagewanted=all&_r=0 (last accessed, 20 October 2013).

[23] These files are available at http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf' and http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf (last accessed, 11 September 2013).

[24] Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", Director of National Intelligence, 7 June 2013, available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-thecollection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act (last accessed, 18 September 2013).

obtain information from the servers of U.S. electronic communication service providers. All such information is obtained with FISA Court approval and with the knowledge of the provider based upon a written 'Directive' from the Attorney General and the DNI.

- In order to obtain authorization under section 702 the Government needs to document that the purpose of the acquisition is the prevention of terrorism, hostile cyber activities, or nuclear proliferation, or another appropriate foreign intelligence purpose and the foreign target is reasonably believed to be outside the United States.
- Section 702 cannot be used to intentionally target any United States citizen, or any other United States person, or to intentionally target any person known to be in the United States. Likewise, Section 702 cannot be used to target a person outside the United States if the purpose is to acquire information from a person inside the United States.

The fact sheet stated that the collection of intelligence information under section 702 is subject to an oversight regime, incorporating reviews by the executive, legislative and judicial branches. As to the judicial branch, the fact sheet states:

- "All FISA collection, including collection under Section 702, is overseen and monitored by the FISA Court [FISC], a specially established Federal court comprised of 11 Federal judges appointed by the Chief Justice of the United States.
- The FISC must approve targeting and minimization procedures under Section 702 prior to the acquisition of any surveillance information.
- Targeting procedures are designed to ensure that an acquisition targets non- U.S. persons reasonably believed to be outside the United States for specific purposes, and also that it does not intentionally acquire a communication when all the parties are known to be inside the United States.
- Minimization procedures govern how the Intelligence Community (IC) treats the information concerning any U.S. person whose communications might be incidentally intercepted and regulate the handling of any nonpublic information concerning U.S. persons that is acquired, including whether information concerning a U.S. person can be disseminated. Significantly, the dissemination of information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance, is evidence of a crime, or indicates a threat of death or serious bodily harm."

It is notable, for the purposes of this case, that the "minimization" procedures which are applied by the FISC *are only concerned* with ensuring minimal use and discarding of the data of United States-persons after initial analysis and searching. In other words, the consideration of non-U.S. persons are left out of these minimization processes.

On 7 June 2013, President Obama also made a statement to journalists with regard to the program that confirms that it is aimed at non-U.S. persons:

> "Now, with respect to the Internet and emails, this does not apply to U.S. citizens, and it does not apply to people living in the United States."[25]

Protection of Privacy of Non-U.S. Persons under United States Surveillance Statute and Practice

As described further below, the U.S. legal regime for prevention of illegal wiretaps does not generally protect non-U.S. persons, nor are the current legal challenges in the U.S. currently considering the impact of NSA surveillance on non-U.S. persons.

The standard rule under United States law is that the intentional interception, use, or disclosure of wire and electronic communications is prohibited unless a statutory exception applies. There are two key ways that the government can be relieved of this general prohibition against the interception of communications. First, when authorized by the Justice Department and signed by a United States District Court or Court of Appeals judge, a wiretap order permits domestic law enforcement, such as the FBI, to intercept communications of named individuals or premises for up to thirty days for certain identified domestic law enforcement purposes (18 U.S.C. §§ 2516(1), 2518(5)). 18 U.S.C. §§ 2516-2518 imposes several formidable requirements that must be satisfied before investigators can obtain a Title III order. Most importantly, the application for the order must show "probable cause" to believe that the interception will reveal evidence of predicate federal felonies. 18 U.S.C. §2516(3).

A second method is via FISA, which allows interception of communications for national security purposes, but importantly, FISA authorises the acquisition of foreign intelligence data. Applications for court orders authorising searches or surveillance under FISA are made to the secret FISA Court, must identify or describe the target of the search or surveillance, and establish that the target is either a "foreign power" or an "agent of a foreign power" (50 U.S.C. §§ 1804(a)(3), 1804(a)(4)(A), 1823(a)(3), 1823(a)(4)(A)). A "foreign power" is defined to include, among other things, a "foreign government or any component thereof" and a "group engaged in international terrorism" (50 U.S.C. §§ 1801(a)(1), (4)). The purpose of the tap must be to obtain foreign intelligence (although this need only be a "significant" and not necessarily the "primary" purpose (50 U.S.C. § 1805(a)(2)). FISA Court proceedings are conducted in private and its rulings are not published – unless the Executive branch declassifies them.

Significantly, the statutory protections offered as part of FISA do not address or defend the privacy rights of non-U.S. persons. To the contrary, in United States v Duggan, 743 F. 2d 59 (2d Cir. 1984) at page 73, the Second Circuit held that although Amendment IV affords protection to non-United States citizens, Congress is not prevented "from adopting standards and procedures that are more beneficial to United States citizens and resident aliens than to non-resident aliens, so long as the differences are reasonable."

[25] "Transcript: Obama's Remarks on NSA Controversy", June 7, 2013, available at http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/ (last accessed, 8 September 2013).

Section 702 of FISA represents a particularly clear departure from the standard rule, however, because it establishes a mechanism of a priori authorizations of untargeted surveillance, rather than being directed at specific individuals or identifiers like email addresses or phone numbers. The public rationale behind the enactment of FISA 702 is put starkly by the United States Justice Department as follows:

> "Before the enactment of [s. 702], in order to conduct the kind of surveillance authorized by section 702, FISA was interpreted to require that the Government show on an individualized basis, with respect to all non-U.S. person targets located overseas, that there was probable cause to believe that the target was a foreign power or an agent of a foreign power, and to obtain an order from the [FISA Court] approving the surveillance on this basis. In effect, the Intelligence Community treated non-U.S. persons located overseas like persons in the United States, even though foreigners outside the United States generally are not entitled to the protections of the Fourth Amendment. Although FISA's original procedures are proper for electronic surveillance of persons inside this country, such a process for surveillance of terrorist suspects overseas can slow, or even prevent, the Government's acquisition of vital information, without enhancing the privacy interests of Americans. Since its enactment in 2008, section 702 has significantly increased the Government's ability to act quickly."[26]

Section 702 of FISA, enacted in 2006, allows the Attorney General ("AG") and the DNI jointly to authorize, for up to one year "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information": s. 702(a) FISA, 50 USC §1881a. Specifically, section 702 allows the following to be obtained from or with the assistance of an electronic communications provider, stored and searched:

- targeted information against a person outside the United States unless they are a "United States person" or the target is a United States person where one or more recipients of a communication are outside the United States;
- non-targeted information in bulk where one or more recipients of communications are outside the United States as long as the actual target is not a United States person;
- data on United States persons or persons inside the United States so long as this is an unintended by-product of an authorization, where the person is not the target, not based solely on a person's exercise of his or her First Amendment rights and is held for a permitted purpose;

While FISA 702 does include language limiting its use, and placing requirements on targeting and minimization, these restrictions are designed to ensure that *U.S. persons'* rights are given a pretense of protection (although whether that minimal protection is to the level demanded by the United States constitutional and international human rights standards is still an open question).

[26] James R Clapper and Eric H Holder, 'Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of Director of National Intelligence' 8 February 2012, available at http://www.justice.gov/ola/views-letters/112/02-08-12-fisa-reauthorization.pdf, (last accessed 15 August 2013).

Once sufficient process has taken place to determine to the administration's satisfaction that the target is a non-U.S. person, no limitations are placed on the collection, analysis, use and transfer of data for privacy purposes.

Use of U.S. Companies and Infrastructure for Data Collection

Section 702 envisages that the acquisition of information will be obtained "from or with the assistance of an electronic communication service provider" (s.702(g)(2)(A)(vi)) i.e. in collaboration with private companies. This takes place through the use of "Directives" given by the NSA to electronic communication service providers to provide "all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition." (s. 702(h)(1)(A)). These Directives may be given to telecommunications providers subject to U.S. jurisdiction, only. The NSA has stated that it considers this "the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the United States and around the world"[27]. It appears that this collaboration formed the backbone of the PRISM and UPSTREAM programs.

United States Legislative Oversight and Review

FISA includes oversight mechanisms, but none of this oversight is concerned with the degree to which information is collected on non-U.S. persons, nor how that information may be used. Instead, the AG and DNI must adopt guidelines, to ensure targeting and minimization procedures are respected and self-assess compliance. (s. 702(f)(1)).

The assessments consider the number of reports that contain a reference to a U.S. citizen or resident, and the number of targets that were determined after they had been targeted to actually be within the United States(s. 702(l)(2)). These self-reviews are provided to the AG, DNI, and key Congressional committees and the same review must be done on an annual basis by the head of each intelligence agency that acquires foreign intelligence information under (s.702(l)(3)).

There is no indication that the FISA Court considers the rights of non-U.S. persons when considering its decisions.

Freedom of Expression, Privacy and Communication Surveillance

Privacy and freedom of expression are fundamental and interconnected human rights, equally recognized in the Inter-American human rights system.[28] Notably, Article X of the American

[27] National Security Agency, 'The National Security Agency: Missions, Authorities, Oversight and Partnerships', 9 August 2013 http://www.nytimes.com/interactive/2013/08/10/us/politics/10obama-surveillance-documents.html?hp&_r=0#document/p24 (last accessed 15 August 2013).
[28] Articles 11 and 13 of the American Convention on Human Rights, Article 5 of the American Declaration of the Rights and Duties of Man.

Declaration on the Rights and Duties of Man explicitly recognizes the critical importance of maintaining communications privacy: "Every person has the right to the inviolability and transmission of his correspondence."[29] Communications privacy is central to the maintenance of democratic societies. With the expansion and increased pervasiveness of digital networks, communications privacy now encompasses a vast range of activity. The Internet and other digital networks now include a near-complete record of our activities, detailed and intricate maps of our interactions and inter-personal networks, even our locations – all transformed into a constant and often real-time stream of correspondence. Interference with the right to private correspondence results in a chilling effect on a person's ability to seek, receive, and impart information, impacts on their associational rights, and their right to move and assemble freely, and can have far-reaching democratic impacts by undermining the abilities of journalists, lawyers, political dissidents and the general public to engage in political debate.

This relationship between privacy and freedom of expression can be founded in Article 5 and 9 of the Declaration of Principles on Freedom of Expression of the Organization of American States, which state, respectively that:

> "Prior censorship, direct or *indirect interference* in or pressure exerted upon any expression, opinion or information transmitted through any means … must be prohibited by law." It further stated, that any "intimidation of and/or threats to social communicators ... violate the fundamental rights of individuals and strongly restrict freedom of expression."

The United Nations Special Rapporteur on Freedom of Expression and Opinion, explained the interrelation of privacy and freedom of expression in a landmark report on State Surveillance and Human Rights[30]:

> *"*The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas*"...*
>
> *"*States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny*."*

For many individuals throughout the Americas region (especially journalists and dissidents), the Internet and mobile telephony have been transformed into a threat. The use of these mediums is difficult or almost impossible without the risk of state interference. This encompasses who, what, when and where of the communication as well as the content itself. Even if no single

---

[29] American Declaration of the Rights and Duties of Man. See *Biset et. al. v. Cuba*, Report No. 67/06, Case 12.476, IACHR, 2006, http://www.cidh.oas.org/annualrep/2006eng/CUBA.12476eng.htm#_ftnref148| (withholding or intercepting the correspondence and telephone communications of prisoners by state is a violation of Article X).

[30] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (last accessed, 20 October 2013).

person is actually listening, the chilling effects of surveillance are felt, as the risk of revealing a journalistic source or legal client, for example, may be too high.[31] Electronic surveillance is silent and undetectable in most situations, but its lack of visibility causes speakers to curtail their private conversations, even when the surveillance is only implied or only potentially aimed at them.[32]

Lawyers, who often speak to clients via electronic communications, are vulnerable to becoming targets. Here, too, the 'who' you are talking too as well as the 'when, where and what' need special protection. But mass surveillance does not provide an easy means of excluding legal interactions. Given that lawyers are often representing the social or politically dissident in a context that is adversarial to the government, these situation raises serious concern.

Journalists are particularly vulnerable to becoming targets of communications surveillance, especially where they are conducting investigations regarding political affairs. Not only do such measures impact upon their ability to freely express themselves, they also inhibit the important functions that the media plays in maintaining transparency and accountability of the state. While journalists' work is meant to be viewed widely and in public, and therefore not seemingly directly affected by surveillance, privacy plays an important role in ensuring news gatherers can seek and receive information, and freely impart their findings to all.

The protection of journalistic sources has long been established as a requirement implicit in the right of freedom of expression.[33] An environment where surveillance is widespread, and unprotected by due process or prior judicial restraint–cannot sustain the presumption of protection of sources. Again, even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its current use, and known checks and balances to prevent its misuse. For example, the former Colombian Administrative Security Agency (DAS) used wiretapping devices, cameras, and cell phone interception systems to spy on political opponents, journalists, labour organisers, and even NGOs seeking to alleviate human rights abuses. These acts caused a chilling effect including even on those that were not directly victims of the illegal activities of the DAS.[34] Moreover, the purposes of the surveillance to journalist's communications, in several instances, seek "to gain

[31] For instance, Andrew Jacobs, a New York Times journalist, who on discovering that his email had been hacked by unknown parties, stated he felt "vulnerable. I've always assumed my e-mail was being read, and that my phones were tapped". Attacks on the Press 2010, Committee to Protect Journalists, available at http://www.cpj.org/2011/02/attacks-on-the-press-2010-internet-analysis-danny-obrien.php (last accessed, 20 October 2013).

[32] R. Carey & J. Burkell, "A Heuristics Approach to Understanding Privacy-Protecting Behaviors in Digital Social Environments", http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_04.pdf (last accessed, 20 October 2013).In this article the author descibes how individuals self-censor when they know they are being observed.

[33] *See* Goodwin v. the United Kingdom at the European Court of Human Rights, available at http://worldlii.org/eu/cases/ECHR/1996/16.html (last accessed, 20 October 2013) "[p]rotection of journalistic sources is one of the basic conditions for press freedom ... Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected."Inter-American Declaration of Principles on Freedom of Expression, Principle 8: "every social communicator has the right to keep his/her source of information, notes, personal and professional archives confidential."Declaration of Principles on Freedom of Expression in Africa, protection of sources, Principle XV.

[34] Fundación para La Libertad de Prensa, "Informe del Espionaje Contra Periodistas: La Justicia Tiene la Palabra," 2010, available at http://flip.org.co/resources/documents/95f9e2d7404a6c47089502b298cbe0ac.pdf (last accessed, 23 October 2013).

knowledge of their journalistic sources" as well as to gather information of those "with critical positions to the government". The investigations have proven that the strategy was not limited to the surveillance itself but the DAS used that information to start a campaign of intimidation and discredit against journalists."[35]

Mass surveillance can have a devastating impact on groups traditionally subject to discrimination, whether based on race, religion and political viewpoint or otherwise. A recent example of this can be seen in the NYPD randomly surveilling Muslims along the East Coast of the United States.[36] These practices had been challenged earlier in the case Handschu v. Special Services Division where it became evident that NYPD surveillance practices targeted groups in a discriminatory manner.[37]

Political dissidents and human rights defenders are similarly impacted by mass surveillance, as peaceful protestors are a frequent object of state surveillance[38] that even extends to those *associated* with dissenters or targeted groups.[39]

Mass surveillance affects human rights defenders and political activists who are also disproportionately subjected to surveillance. Freedom of expression and freedom of information allow human rights defenders to challenge abuses to human rights; without the privacy to conduct investigations and communications away from the prying eyes of the state, this becomes impossible.

Permissible Limitation on the Right to Privacy Under International Human Rights Law

Communications privacy in particular should only be interfered with restricted in exceptional cases, and even then, any interference must still follow the rule of law. On this point, the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, Frank la Rue has stated clearly that:

> "Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and

[35] Catalina Botero, "Informe Anual de la Comisión Interamericana de Derechos Humanos 2010." Informe de la Relatoria Especial para la Libertad de Expresion, available at http://www.cidh.oas.org/annualrep/2010sp/RELATORIA_2010_ESP.pdf (last accessed, 23 October 2013).

[36] American Civil Liberties Union, Resolution Introduced in House to Condemn NYPD Muslim Spying, November 5, 2012, available at http://ww.aclu.org/blog/national-security-religion-belief-technology-and-liberty/resolution-introduced-house-condemn (last accessed, 20 October 2013).

[37] Handschu v. Special Services Division (Challenging NYPD surveillance practices targeting political groups). 288 F.Supp.2d 411), available at http://www.nyclu.org/files/8.6.03_Handschu_Guidelines.pdf (last accessed, 20 October 2013).

[38] The Canadian Press, "RCMP Snooped on Occupy Ottawa Protests", CBC News, February 3, 2013, http://www.cbc.ca/news/canada/ottawa/rcmp-snooped-on-occupy-ottawa-protesters-1.1410899; Partnership for Civil Justice Fund, "FBI Considers the 'Occupy Movement" as a "Terrorist Threat", December 22, 2012, http://www.justiceonline.org/commentary/fbi-files-ows.html.

[39] Farnaz Fassihi. Iranian Crackdown Goes Global. The Wall Street Journal. December 2009,available at http://online.wsj.com/article/SB125978649644673331.html (last accessed, 20 October 2013). In this article security agencies in Tehran arrested an individual's father in response to facebook comments made by the son.

> exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law."

Moreover, the Rapporteur has taken the position that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as elucidated in General Comment 27.[40]

The test as expressed in the comment includes, inter alia, the following elements:[41]

> (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)."

While the focus of this report is on the surveillance itself, the secrecy surrounding the activities of the NSA and the limited role of the FISA court (merely reviewing processes, not the actual use of the authorities) and focusing primarily on placing limits on the impact of surveillance on U.S. persons infringe upon international human rights standards. The Inter-American Court has held:

> "what is incompatible with the Rule of Law and effective judicial protection" ... "is not that there are secrets, but rather that these secrets are outside legal control, that is to say, that the authority has areas in which it is not responsible because they are not juridically regulated and are therefore outside any control system."[42]

International Principles on the Application of Human Rights to Communications Surveillance

In order to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques, more than 280 human rights, media, digital rights and organizations around the

[40] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (last accessed, 20 October 2013).
[41] CCPR General Comment No. 34
[42] Myrna Mack Chang case v. Guatemala, paragraph 181

world have signed the International Principles on the Application of Human Rights to Communications Surveillance. The principles can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. They also speak to a growing global consensus that modern surveillance has gone too far and needs to be restrained.

The Principles are grounded in international human rights law including Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the American Declaration of the Rights and Duties of Man, the American Convention on Human Rights, and the European Convention on Human Rights.[43] They apply to surveillance conducted within a state or extra-territorially. They can be found at necessaryandproportionate.org.

The key elements of the 13 Principles are outlined below.

> **"Transparency in Surveillance:** Privacy-invasive activities must be based on publicly described powers that are clear and detailed enough so that individuals can foresee the conditions under which privacy invasion will occur; individuals must be notified as soon as possible once their privacy has been invaded; aggregate and detailed public reporting on all state surveillance activities is a must. This will prevent scenarios where state agencies are able to benefit from one-sided and secret interpretations of legal ambiguities as a means of expanding the reach of their surveillance powers and effectively insulating them from adversarial challenge. In addition, the principles envision "sufficient and significant" protection for whistleblowers -- an important mechanism for ensuring transparency in surveillance -- as well civil and criminal penalties that provide enough sting to ensure illegal surveillance does not occur.
>
> **Technical Neutrality:** Individuals cannot be robbed of their right to live free of state scrutiny on the basis of arbitrary definitions based on technical delivery mechanisms inherent in digital networks, such as whether the information is under the control of a third party (as almost all online data is); whether the 'content' of communications is sought or not (as the metadata that surrounds this 'content' in Internet transactions can be equally or more revealing of people's lives); whether the information is artificially categorized as 'subscriber information' (as identifying the computer behind an IP address is the key to vast amounts of otherwise anonymous online activity); or whether a particular item of information, analyzed in isolation, is not revealing, but has the capacity to reveal highly private information if collected systematically or pervasively, or if connected with other readily available information (an IP address, for example, may not reveal much in isolation but if left completely unprotected, indiscriminate collection and retention of all IP addresses can transform the Internet into a tool of mass surveillance).
>
> **Proportionality and Due Process:** Given the invasive nature of electronic surveillance, it should not be frivolously undertaken for trivial means and should always be narrowly

[43] See the cases of Klass v. Germany (Judgment of 6 September 1978), Weber and Saravia v. Germany (Admissibility Decision of 29 June 2006), Liberty and Others v. the UK (Judgment of 1 July 2008), and Kennedy v. the UK (Judgment of 18 May 2010). See in particular the summaries in Weber and Saravia, paras. 93 – 95, and in Kennedy, paras. 151 – 154 (which quote Weber and Saravia, paras 93 – 95, thus re emphasising that the approach there summarised is now regarded as settled case-law).

tailored. As Canadian Supreme Court Justice La Forest noted in R. v. Duarte[44] "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance." Therefore, in an investigative context, electronic surveillance can only occur subject to an independent, objective and competent authority determination that the invasion is highly likely to reveal evidence of a serious offence; where this determination occurs before privacy is invaded, except in instances of immediate emergency (as retroactive authorization has been greatly abused in the past); and that no more information should be accessed than is strictly necessary for the specific purpose for which the invasion was authorized (given that data is now highly centralized, a tailored invasion for a specific purpose can easily become an expedition, as vast amounts of data are swept into plain sight once access has been granted).

Formalize Trans-Border Access: Domestic data storage is rapidly becoming a thing of the past, and states are discovering new and creative ways to access data on computers stored around the world. This means, however, that data is often under the control of third parties in foreign countries and can generally be accessed under foreign laws. The Principles seek to address this issue by ensuring that trans-border access to data occurs through frameworks formalized in state to state agreements; that, were more than one law may facilitate access to data, the higher level of protection will be applied and trans-border access will not be used as a means of circumventing domestic protections; that voluntary cooperation by private parties will no longer occur and states will not be able to rely on the voluntary cooperation of private parties as a means of bypassing domestic protections, subject to criminal sanctions for those who permit or carry out illegitimate access; and by ensuring that the protections offered by these principles is applied to all individuals, whether they are based domestically or not (any access to the information of any individual can only occur in a manner consistent with their specific requirements of the Principles)."[45]

United States Government Surveillance Under Scrutiny Globally

The mass surveillance practices of the United States have been under scrutiny in several countries and globally. We note, at the outset, that the expansive surveillance practices of foreign intelligence activities are being challenged in several international fora for their consistency with international human rights obligations. These include the Human Rights Committee,[46] and the European Court of Human Rights.[47]

---

[44] R. v. Duarte, [1990] 1 SCR 30, available at http://canlii.ca/t/1fszz (last accessed 21 October 2013).

[45] Tamir Israel, "Brief Summary of the International Privacy Principles for Surveillance in the Digital Age", CIPPIC, The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), available at https://cippic.ca/en/news/International_Privacy_Principles (last accessed, 20 October 2013). *See also* ARTICLE 19, Freedom from suspicion: Principles to protect freedom of expression and privacy against mass surveillance, http://www.article19.org/resources.php/resource/37186/en/freedom-from-suspicion:-principles-to-protect-freedom-of-expression-and-privacy-against-mass-surveillance#sthash.tsD6pTSo.dpuf (last accessed, 20 October 2013).

[46] Global Initiative for Economic, Social and Cultural Rights, "Parallel Report to the Country Report Task Force of the Human Rights Committee on the occasion of the consideration of List of Issues related to Fourth Periodic Report of the United States during the Committee's 107th Session", January 2013, <http://globalinitiative-escr.org/wp-content/uploads/2013/04/130102-GI-ESCR-Parallel-Report-HRC-USA-2013.pdf>

As a starting point, while surveillance activities conducted by the NSA are often defended as necessary to combat terrorist threats, no attempt is made to limit the agencies surveillance activities to addressing these most serious threats. The definition of 'foreign intelligence' which prescribes the NSA's mandate is excessively broad, seemingly encompassing any information that may give the United States a political,[48] or even economic[49] advantage. The United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression has explicitly warned against the use of vague and broad terms such as 'national security' and 'foreign intelligence' as a justification for surveillance:

> Vague and unspecified notions of "national security" have become an acceptable justification for the interception of and access to communications in many countries... The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often-unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.[50]

In the opening statement by Ms. Navi Pillay, United Nations High Commissioner for Human Rights at the Human Rights Council 24th Session, the eminent South African human rights lawyer[51] raised concerns about the broad scope of national security surveillance in countries, including the United States, and the impact of these regimes on individuals' right to privacy and other human rights. She further emphasized:

> "While national security concerns may justify the exceptional and narrowly-tailored use of surveillance, I would urge all States to ensure that adequate safeguards are in place against security agency overreach and to protect the right to privacy and other human rights."

On September 13, the German Ambassador Schumacher delivered a joint statement on behalf of Austria, Germany, Liechtenstein, Norway, Switzerland and Hungary expressing their concern

---

[47] *Big Brother Watch, Open Rights Group, English PEN, Dr. Constanze Kurz v. United Kingdom*, App. No. 58170/13, <https://www.privacynotprism.org.uk/assets/files/privacynotprism/496577_app_No_58170-13_BBW_ORG_EP_CK_v_UK_Grounds.pdf>.

[48] E. MacAskill, N. Davies, N. Hopkins, J. Borger & J. Ball, "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits", The Guardian, Monday 17, 2013, <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>.

[49] Colin Freeze and Stephanie Nolan, "Charges that Canada Spied on Brazil Unveil CSEC's Inner Workings", Globe and Mail, October 7, 2013, <http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/>

[50] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[51] "Opening Statement by Ms. Navi Pillay United Nations High Commissioner for Human Rights at the Human Rights Council 24th Session", 9 September 2013, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13687&LangID=E (last accessed, 20 October 2013).

about the consequences of "surveillance, decryption and mass data collection, which may severely intrude in people's right to privacy[52]:

> "legitimate national security considerations and the necessities of law enforcement may justify, in well-defined cases and under specific circumstances, limitations to the right to privacy. Any restriction to the right to privacy must be based on law, respect for the principles of proportionality and must be susceptible to review by an independent authority. Every instance of interference needs to be critically and thoroughly assessed by the yardstick of law, which itself must be in conformity with relevant international human rights standards. "

In a Joint Declaration on surveillance programs and their impact on freedom of expression, the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, stated clearly that:

> "Any surveillance of communications and interference with privacy that exceeds what is stipulated by law, has ends that differ from those which the law permits, or is carried out clandestinely must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media".[53]

Yet the United States foreign intelligence surveillance programs are excessively broad and indiscriminate in their reach, *especially* in its application to non-U.S. persons.[54] It is difficult to see how such an expansive and broad program can be viewed as 'proportionate' in the context of human rights protections for privacy.[55]

Elements of the United States foreign intelligence surveillance program are premised on the assumption that non-U.S. persons enjoy limited protection under the fourth amendment to the United States constitution.[56] However, this premise is untenable in an interconnected world

---

[52] Joint Statement by Austria, Germany, Liechtenstein, Norway, Switzerland and Hungary to the Human Rights Council", September 13, available at https://www.eff.org/document/joint-statement-austria-germany-liechtenstein-norway-switzerland-and-hungary (last accessed, 20 October 2013).

[53] United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, "Joint Declaration on surveillance programs and their impact on freedom of expression", 21 June 2013, available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1 (last accessed, 20 October 2013).

[54] Cindy Cohn, Witness Statement of Cindy Cohn, *Big Brother Watch et. al. v. United Kingdom*, European Court of Human Rights, Application No.: 58170/13, <https://www.privacynotprism.org.uk/assets/files/privacynotprism/CINDY_COHN-FINAL_WITNESS_STATEMENT.pdf>,

[55] Dr. Ian Brown, Witness Statement of Dr. Ian Brown, *Big Brother Watch et. al. v. United Kingdom*, European Court of Human Rights, Application No.: 58170/13, <https://www.privacynotprism.org.uk/assets/files/privacynotprism/IAN_BROWN-FINAL_WITNESS_STATEMENT.pdf>, commenting on related activities carried out by the NSA's United Kingdom-based foreign intelligence partner, GCHQ, paras. 61 *et. seq.*

[56] See T. Israel, K. Rodriguez & M. Rumold, "An International Perspective on FISA: No Protections, Little Oversight", Electronic Frontiers Foundation – Spies June 15, 2013, <https://www.eff.org/deeplinks/2013/06/modern-foreign-surveillance-legal-perspective>

where data is no longer territorially bound. Moreover, the assumption has no basis in International Law, which guarantees privacy rights to all individuals everywhere in the world.[57]

The activities of national security agencies by the United States, and the arrangements under which they cooperate, have been outside the scope of effective democratic oversight and outside clear legal frameworks for too long; they must be brought under the rule of law. Moreover, these practices are excessively broad, and interfere with privacy rights far beyond what is necessary to achieve legitimate security-related state interests.

Media reports have affirmed that the NSA has intercepted emails and telephone call by Brazilian President Rousseff and her key Ministers and advisers.[58] Further news that the Brazilian state company Petrobras and the Ministry for Mines and Energy had also been subject to surveillance led the Presidency to state that economic reasons were behind the US actions. The situation reached a critical point when President Rousseff opened the United Nations General Assembly meeting in New York, in September 2013, by stating that such actions were "inadmissible" and that they constitute a "grave violation of human rights and civil liberties". She also affirmed that they were not only a violation to national sovereignty, but also involved the capture of confidential information relating to corporate activities and implicitly denied the US argument that the data was collected for terrorism prevention only.[59]

European Digital Rights and FREE NGO in a submission to the European Parliament committee investigating the suspicionless mass surveillance activity by the United States, explained:

> "Failure of a European State to prevent improper spying by non-European countries constitutes a breach of that country's "positive obligations" under the ECHR. Active support for, complicity in, or even passive condoning of such spying would breach the State's primary obligations under the [ECHR - European Court on Human Rights]
>
> Under the ECHR, these principles must be applied to anyone who is affected by surveillance measures taken by any Council of Europe Member State under domestic law. In addition, European States have a "positive obligation" to protect their citizens from surveillance contrary to the above, perpetrated by any other State. A fortiori, they are under a legal obligation not to actively support, participate or collude in such surveillance by a non-European State."[60]

At a hearing in the European Parliament, the surveillance initiatives operated by the National Security Agency were the subject of legal scrutiny as part of an ongoing inquiry.

---

[57] Global Initiative for Economic, Social and Cultural Rights, "Parallel Report to the Country Report Task Force of the Human Rights Committee on the occasion of the consideration of List of Issues related to Fourth Periodic Report of the United States during the Committee's 107th Session", January 2013, <http://globalinitiative-escr.org/wp-content/uploads/2013/04/130102-GI-ESCR-Parallel-Report-HRC-USA-2013.pdf>

[58] Dilma diz que espionagem na Petrobras mostraria interesse econômico dos EUA, 09 September 2013, noticias.uol.com.br/ultimas-noticias/reuters/2013/09/09/dilma-diz-em-nota-que-espionagem-na-petrobras-mostraria-interesse-economico-dos-eua.htm (last accessed, 20 October 2013).

[59] Caso de espionagem dos EUA viola direitos humanos, diz Dilma na ONU, http://www.bbc.co.uk/portuguese/noticias/2013/09/130924_dilma_assembleia_onu_lgb.shtml (last accessed, 20 October 2013).

[60] Submission by the European Digital Rights Initiative (EDRi) & Fundamental Rights Experts Group (FREE) to the United States Congress, the European Parliament, the European Commission & the Council of the European Union, & the Secretary-General & the Parliamentary Assembly of the Council of Europe. http://www.edri.org/files/submission_free_edri130801.pdf (last accessed, 20 October 2013).

Douwe KORFF, Professor und Datenschutz, explained that from the considerable amount of case law in Strasbourg on surveillance, you can deduce that:[61]

> "States have a positive obligation ... not to carry out improper surveillance to start with; they also have a positive obligation to prevent other states from spying on their citizens, and of course they shouldn't collude in illegal surveillance by third-party states either."

Moreover, KORFF explained that modern international law generally requires that States should comply with their human rights requirements also when they are acting in relation to people outside their territory — and that has been very well established by the European court:

> "The court has said very clearly that states should not be allowed to do things in the territories of other state parties that they are not allowed to do at home. That makes good common sense and I think is something to remember."

In his testimony on 10 October 2013 before the European Parliament, Martin Scheinin, former U.N. special rapporteur on human rights and counterterrorism from 2005 to 2011, stated that the mass surveillance of the United States amounted to "an unlawful or arbitrary interference with privacy or correspondence." Moreover, Scheinin concluded that the overall electronic mass surveillance architecture developed by the national security authority of the United States "did violate several elements of the permissible limitation test, resulting in a breach by the United States of Article 17 of the ICCPR. In other words, we are going beyond of what could be justified as permissible limitations. The surveillance conducted constituted an unlawful and arbitrary interference with privacy of correspondence and these conclusions follow independently from multiples grounds."[62]

The ICCPR and other human rights treaties in general, Scheinin explained, does not discriminate between citizens and not citizens. Privacy right "applies equally no matter whether the person is citizen or not."

In this context, it should be noted that the first article of the American Declaration of the Rights and Duties of Man affirms that "***all*** human beings are born free and equal in dignity and rights".[63] It is difficult to see how limitless surveillance of non-U.S. persons can justly fit within this framework.

---

[61] *See* page 6 of EDRI-FREE Submission, available at http://www.edri.org/files/submission_free_edri130801.pdf (last accessed, 20 October 2013). In particular, Weber & Sevaria judgement against Germany. Liberty and other against the UK.

[62] See Martin Scheinin Testimony,Committee on Civil Liberties, Justice and Home Affairs, LIBE Committee meeting 14.10.2013, available at http://www.youtube.com/watch?v=RIrXtyU2ryg (last accessed, 20 October 2013). *See also* Ryan Gallagher. "The World's Policeman Is Looking Mighty Guilty 449 466 13 NSA snooping exposed by Snowden breaches international law, experts say", 17 October 2013, available at http://www.slate.com/articles/technology/future_tense/2013/10/martin_scheinin_u_s_u_k_surveillance_programs_violate_iccpr.html (last accessed, 20 October 2013).

[63] American Declaration of the Rights and Duties of Man. *See also*: International Convention on the Elimination of All Forms of Racial Discrimination. Adopted and opened for signature and ratification by General Assembly resolution 2106 (xx of 21 December 1965. http://www.ohchr.org/EN/ProfessionalInterest/Pages/CERD.aspx; United Nations General Assembly Resolution 1904(XVIII). United Nations Declaration on the Elimination of All Forms of Racial Discrimination. 1963.http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/185/79/PDF/NR018579.pdf?OpenElement.

Indeed, the Human Rights Committee has consistently held that the International Covenant on Civil and Political Rights can have extraterritorial application, clearly demonstrating its understanding that a State's human rights obligations extends beyond its territorial boundaries.

The Human Rights Committee has adopted an effects-based approach to extra-territorial application, focused on "whether or not the act is attributable to a State and a violation of an international legal obligation".[64]

> "In Burgos/Lopez v. Uruguay, were the Committee held that Uruguay violated its obligations under the Covenant when its security forces abducted and tortured a Uruguayan citizen then living in Argentina.
>
> Following the command of Article 5(1) that "[n]othing in the present Covenant may be interpreted as implying… any right to engage in any activity… aimed at the destruction of any of the rights and freedoms recognized herein," the Committee reasoned that "it would be unconscionable to so interpret the responsibility under article 2 of the Covenant as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory."[65]

The Human Rights Committee has adopted an effects-based approach to extra-territorial application, focused on "whether or not the act is attributable to a State and a violation of an international legal obligation".[66]

Conclusion

The mass surveillance programs of the United States NSA violate fundamental human rights of non-U.S. persons. In order to meet their human rights obligations, the United States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks. Currently, U.S. mass surveillance practices ignore any consideration of proportionality and due process in favor of the unchecked interference of the right to privacy. Moreover, any measure of communications surveillance should not be applied in a manner that discriminates on the basis of, inter alia, nationality or other status.

In our view, there is a clear international consensus that mass surveillance on U.S. and non-U.S. persons is inconsistent with human rights standards and so the Commission should immediately recommend to the Member States of the Organization of American States adopt measures prohibiting unchecked mass surveillance in law and in practice.

The United States needs to meet its international human rights obligations, including the American Declaration of the Rights and Duties of Man in relation to communications

---

[64] Global Initiative for Economic, Social and Cultural Rights, "Parallel Report to the Country Report Task Force of the Human Rights Committee on the occasion of the consideration of List of Issues related to Fourth Periodic Report of the United States during the Committee's 107th Session", January 2013, <http://globalinitiative-escr.org/wp-content/uploads/2013/04/130102-GI-ESCR-Parallel-Report-HRC-USA-2013.pdf>

[65] Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004).

[66] Global Initiative for Economic, Social and Cultural Rights, "Parallel Report to the Country Report Task Force of the Human Rights Committee on the occasion of the consideration of List of Issues related to Fourth Periodic Report of the United States during the Committee's 107th Session", January 2013, <http://globalinitiative-escr.org/wp-content/uploads/2013/04/130102-GI-ESCR-Parallel-Report-HRC-USA-2013.pdf>

surveillance, in the United States and extraterritorially. We respectfully request the Commission to monitor the practices denounced in this document and closely follow the practices of surveillance explained in this document insofar as they affect the fundamental right to privacy guaranteed by Article 11 of the Covenant.

From the position of strengthening the rule of law and protection of human rights, the Commission should deepen the human rights standards that the Inter-American Human Rights has developed.

We hope that the mass surveillance activities of the United States will be condemned in the strongest terms, reaffirming the above human rights principles, established by international human rights law.

Written Submission Signed by,

Katitza Rodriguez, International Rights Director
Danny O'Brien, International Director
Cindy Cohn, Legal Director
Electronic Frontier Foundation - International

Ramiro Álvarez, Director del Área de Acceso a la Información
Eleonora Rabinovich, Directora Adjunta
Asociación por los Derechos Civiles - Argentina

Valeria Betancourt Directora del Programa de Políticas de Información y Comunicación
Asociación para el Progreso de las Comunicaciones - International
Association for Progressive Communications - International

Darío Ramírez, Director
Antonio Martínez, Oficial de comunicación
ARTICLE 19 - Mexico and Central America office

Fabiola Carrión, Policy Counsel
Access - International

Paula Martins, Diretora para América do Sul
ARTIGO 19 - Brazil

Hedme Sierra-Castro
Asociación para una Ciudadanía Participativa – Honduras

Micheal Vonn, Policy Director
BC Civil Liberties Association – Canada

Vincent Gogolek, Executive Director
BC Freedom of Information and Privacy Association - Canada

Marilia Maciel - Researcher and Coordinator
Luiz Fernando Moncau - Researcher and Coordinator
Joana Varon Ferraz - Researcher
Center for Technology and Society at Fundação Getúlio Vargas (CTS/FGV) - Brazil

Jesús Robles Maloof
Colectivo ContingenteMx - México

Gustavo Gallón Giraldo, Director
Juan Camilo Rivera, Abogado, Área de Incidencia Nacional
Comisión Colombiana de Juristas - Colombia

Claudio Ruiz, Director Ejecutivo
Derechos Digitales - Chile

Anabella Rivera
Instituto DEMOS

Carolina Botero, Directora del Grupo Derecho, Internet y Sociedad
Amalia Toledo y Pilar Saenz, Coordinadoras Proyectos Especiales
Fundación Karisma - Colombia

Pedro Vaca Villarreal, Director ejecutivo
Emmanuel Vargas Penagos, Coordinador legal
Fundación para la Libertad de Prensa - Colombia

Board of Directors
DATA- Uruguay

Miguel Morachimo, Director Ejecutivo
ONG Hiperderecho - Perú

Steve Anderson, Executive Director
OpenMedia.ca

Carly Nyst, Head of International Advocacy
Privacy International - International

Pilar Tavera Gómez, Directora
Propuesta Cívica - México

Ronaldo Lemos, Director Ejecutivo
Rio Institute for Technology & Society – Brazil

Maricarmen Sequera, Executive Director
Jazmín Acuña, Projects Director
TEDIC (Tecnología, Educación, Desarrollo, Investigación y Comunicación) - Paraguay

Tamir Israel, Staff Lawyer
The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic - Canada