# State Communications Surveillance and the Protection of Fundamental Rights in Peru

By Miguel Morachimo
*in collaboration with Katitza Rodríguez*

July 2016

ELECTRONIC FRONTIER FOUNDATION

hiperderecho

Miguel Morachimo is a lawyer from the Pontifical Catholic University of Peru and the director of the nonprofit Hiperderecho, a Peruvian civil organization devoted to facilitating public understanding, research, promotion, and observance of human rights and freedoms in the digital world.

This report was written in alliance with the Electronic Frontier Foundation (EFF), an international non-profit organization that has been defending freedom of expression and privacy in the digital world since 1990. We would like to thank Katitza Rodríguez, EFF's international rights director, for leading a substantial revision of this report; and Kim Carlson and David Bogado of EFF for their copyediting and formatting contributions.

This report is part of a larger regional project called "Surveillance and Human Rights" that is being conducted in eight Latin American countries by EFF.

# Table of Contents

# Introduction

There aren't many issues that have created as much controversy as state communications surveillance has in the past few years. In June 2013, Edward Snowden, a former US government contractor, revealed convincing evidence about the existence of several national and international programs led by the National Security Agency (NSA). These programs were designed to monitor the private communications of millions of Internet users on a massive scale.

Since then, not only in the United States but also in the rest of the world, there has been a public debate over the contexts and limits in which it is acceptable for a State to systematically monitor its citizens with the purposes of foreseeing or reducing crime and conducting intelligence activities. On one hand, there are those who believe these measures are a necessary evil to prevent or counteract even greater evils like acts of violence and terrorism. On the other hand, there are those who oppose these sorts of measures because they think that handing over full control of citizens' communications to the State is a clear violation of fundamental rights and weakens democratic institutions.

This controversy is relevant not only to governments and the democratic process but also to users and private companies. In late 2013, a survey by PEN International showed that as a consequence of the surveillance activities denounced by the international press, 24% of respondents deliberately avoided discussing certain topics over the phone or via email, and 9% had seriously considered doing the same.[1] In addition, it is estimated that some of the large U.S. tech companies' cooperation with the NSA surveillance programs could result in an income loss of up to 25% in their sectors, due to the consumers' and social partners' loss of confidence.[2]

Peru has suffered from a complicated history of State and private surveillance practices. It has been recorded that between 1990 and 2001, multiple instances of communications surveillance and interception were conducted by the now-defunct Peruvian National Intelligence Service. Since it shut down, it is thought that the specialists and teams devoted to surveillance have not gone missing, but have moved to the private sector or pursued other aims. In 2011, journalist Óscar Castilla's research revealed the functioning of the system of communications interception used by the Peruvian National Police Anti-Drugs Directorate. The police worked with teams and technical assistance from the U.S. Drug Enforcement Administration (DEA), which had been operating in drug trafficking and organized crime cases since 2009.[3] Furthermore, several reports of intelligence operations

conducted by the National Intelligence Directorate (DINI, in Spanish) were published in early 2015. These operations were allegedly carried out by the government for political and strategic purposes. As a consequence of these revelations, the president of the Council of Ministers decided to dissolve the DINI in February 2015 and redesign the whole national intelligence scheme. A month later, these revelations inspired a successful motion of censure against the entire cabinet presided by Ana Jara. This was the first motion of censure in Peru in over 52 years.[4] In July 2015, a new regulation was passed which broadened the power of the police. In the case of blatant crimes, it enabled the police to access the location of any telecommunications user in real time. It also established mandatory data retention.[5]

Thus, it is important to open the debate on surveillance in other contexts and situations. The legal justifications and technological tools enabling these practices in certain States can be rapidly implemented by private telecommunications companies in Peru. The UN Special Rapporteur for Freedom of Expression highlighted, in his April 2013 report, the pressing need to analyze new State surveillance methods and national laws that regulate these practices vis à vis the international standards on human rights.[6] From that point of view, this report elaborates on the contents and the scope of different surveillance methods conducted by the Peruvian State and their implications on fundamental rights. This report aims to analyze whether the existing mechanisms and justifications for State surveillance in Peru abide by the limits imposed by constitutional law, as interpreted and recognized by the Peruvian legislation and national and international courts.

First, this report explains the concept of communications surveillance activities, according to the definition given by the international jurisprudence. Next, there is a discussion on how these activities may be at odds with the core content of certain fundamental rights, as recognized in the Constitution, their implementing regulations and in the jurisprudence of the constitutional court. Then there is a list of the several communications surveillance methods allowed by the Peruvian legal framework and an analysis on the appropriateness of the international standards setting a limit on State communications surveillance. Finally, some public policy recommendations are given, which could be a basis for future law reforms.

# I.

# What is State Communications Surveillance?

In the past analog world, an individual's communications and their private networks were easy to identify and protect. The only copies of private communications available were with their intended recipients, and any data related to an individual's private life would be limited in reach in accordance with the interlocutor's credibility. Any aspects of an individual's private life that needed to stay private were sufficiently shielded by simply keeping them within the boundaries of their houses. Not until the invention of certain technologies, like photography, did the concern and the legal notion of privacy arise. When the practice of publishing photographs in newspapers and magazines arose, Samuel Warren and Louis Brandeis published the seminal article, *The Right to Privacy,* in the U.S. in the late nineteenth century, which outlined the concept of privacy. In the article, the authors specifically raised the issue about the press's capacity to invade private life due to the proliferation of cameras.[7]

The invention of photography and the telephone made us think about the need to identify and legally protect our privacy. Similarly, the ability to intercept these means of communication was limited by clear legal principles and physical restrictions inherent to those means—for instance, it was impossible to monitor a phone call without physically accessing the network at some point. In recent years, the use of devices that are permanently connected to the Internet and the evolution towards "the Internet of things" have caused us to reconsider what is protected when it comes to communications surveillance and private information. Nowadays, photos taken with smartphones have radically different implications from ones taken with non-digital cameras. To begin with, a countless number of identical copies can be instantly made from a digital photo at a negligible cost. Moreover, digital photos may contain metadata, including the time, date, camera model, geographical location, and even the author's name or camera series. In addition, whenever a digital photo is taken with a smartphone or tablet, there is a strong possibility that a copy will be immediately and even automatically stored on an external server under the control of the device provider; an Internet service provider; or a remote storage service such as Apple, Google, or Dropbox. In light of this new situation, it is crucial to broaden the discussion on the legal treatment of privacy and the appropriateness of legal tools in order to prevent privacy violations, especially by State authorities.

Similarly, with the proliferation of new technologies that are connected to servers and the increase of information-processing capacities, privacy protections must be extended to areas that have been traditionally left unprotected. In the past, a call log with several phone numbers from the past hours or even days meant nothing in terms of privacy infringement. Today, telecommunications companies have records that date back several years that include frequency, location, time, and duration of each communication. These records allow them to process information in such a way that they can obtain private data and information about an individual's habits that reveal aspects of their private lives, such as the places where they spend the night or the numbers they call frequently.

## I.1. State Communications Surveillance Activities

In this report, the concept of "State communications surveillance" encompasses any measure—justified or unjustified—taken by a national authority with the purpose of accessing any kind of information related to the development or the content of an individual's private communications through any monitoring, intercepting, collecting, preserving, or retaining action. The techniques used for surveillance activities are unimportant, whether they are conducted manually by human intervention or mechanically through automatic access to and storage of information. Likewise, this term is used regardless of whether a legal justification or any kind of authorization exists or not. This report recognizes the existence of valid and legal forms of communications surveillance conducted by State authorities. The limits of these practices are discussed in detail in the following sections.

International experience points to the fact that some State communications surveillance activities are not necessarily conducted in the framework of specific governmental programs recognized as such. Sometimes, State surveillance of communications can take the form of isolated monitoring, recording or intercepting mechanisms carried out by State authorities. These surveillance activities may be a part of the justice administration systems or the intelligence systems.

According to its scope, State communications surveillance may be conducted on an individual or a massive scale. The former is carried out on an individual or on a particular group—for instance, groups being investigated for a crime. Surveillance is considered to be massive whenever it is exerted upon a large group of individuals that are not necessarily connected to a particular investigation or process—for instance, intercepting phone calls made by members of a political party or by individuals who live in a specific geographic zone.

At the same time, surveillance activities can be carried out via a wide range of technical measures, including telephone tapping, intercepting electronic communications, spreading malicious software (*malware or spyware*), or remote control of cellphones or computers, with the purpose of extracting information from those who are being surveilled. Other techniques include monitoring metadata obtained from optical fiber and accessing a user's geolocation data, among others. These techniques and the several tools used for State communications surveillance are subject to constant study and evolution.

Finally, State communications surveillance also includes legally imposed obligations or particular orders from State authorities to third parties such as phone companies or Internet service providers. These orders compel the third parties to record the progress and content of their users' communications and to hand such records over to the State authorities. When this occurs, communications surveillance is not carried out directly by State authorities, but indirectly through the access to the users' communications and protected information stored by or under the control of third parties.

The instances in which surveillance is carried out independently by third parties—individuals or companies—without any legal obligation or order are not included in this definition. This is called industrial espionage. These instances of interception of communications by private actors are illegal according to the Peruvian law, as long as the service users have not given authorization to the third parties. In those cases, the third parties may be investigated and may face criminal penalties. Given that this practice is not related to State intervention, it will not be analyzed in this report.

## I.2. Protected Information

The concept of "protected information" was traditionally understood exclusively in terms of the contents of a communication, such as phone conversations or the contents of a letter. However, new forms and means of interpersonal communication have forced us to broaden this concept. Today, other aspects are considered protected information vulnerable to surveillance, such as the location records related to communications, the identifying information on the terminals used, and others. The processing of such data enables the collection of information about the behavior of communications agents.

Taking all this into account, this report considers the information that might be the target for State surveillance programs to be information related to an individual's or a group's process of communication, as long as the information has not been previously made public. In other words, this definition includes not only the contents of communications, but also other aspects related to the development of communications, such as their occurrence, frequency, routing, origin, and destination. All of this is in accordance with the criterion

established by the Inter-American Court of Human Rights. The Court has noted that not only does this definition encompass the content of communications but also any other type of information, complementary to the content as well as "any other element in the communication process."[8]

Nationally, the Peruvian Constitutional Court has adhered to the conclusions reached in the case of Escher et al. v. Brazil on its sentence on File Nº 00655-2010-PTH/TC when it was specified that the right to the protection of private life includes "telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by tapping it, and any other elements of the communication process; for example, the destination or origin of the calls, the identity of the speakers, the frequency, time and duration of the calls, and other aspects that can be verified without the need to register the content of the call by recording the conversation."[9]

When communication takes place through the Internet, the definition of protected information also includes elements like data related to IP number, browsing histories, and all the information gathered by tracking applications of Internet activity, such as cookies.

# II.

# Which Fundamental Rights are Threatened by State Communications Surveillance?

State communications surveillance is likely to pose a threat to several rights, such as freedom of expression and privacy, according to how they have been defined in the constitution and international treaties on human rights signed by Peru. This section describes the tension that exists between State communications surveillance methods and the aforementioned fundamental rights.

This does not mean that every form of surveillance conducted by the State is illegal and should be outlawed. The specific assessment of how and under which safeguards the State may conduct surveillance activities without infringing human rights shall be discussed towards the end of this section.

## II.1. How is Privacy Affected by State Communications Surveillance?

The right to privacy is the first fundamental right interfered with by State communications surveillance. This right comprises an individual's right to the protection of their personal and family information. Privacy protects this information from being accessed, recorded, or altered by third parties without authorization. Therefore, whenever a State authority conducts activities with the purpose of recording, intercepting, or accessing an individual's communications and electronic records, the State is interfering with an individual's personal and family privacy.

Article 12 of the Universal Declaration of Human Rights indicates that no individual shall be subjected to arbitrary interference with their privacy, family, home or correspondence, and it points to the fact that everyone has the right to the protection of the law against such interference or attacks.[10] The contemplation of the right to privacy can be also found in Article 11 of the American Convention on Human Rights[11] and in Article 17 of the International Covenant on Civil and Political Rights.[12]

In Peru, privacy is protected in Article 2 of the Political Constitution of 1993, which in several sections indicates that every individual has the right to: (i) assurance that

information services will not provide information affecting personal and family privacy, (ii) personal and family privacy, (iii) inviolability of home, and (iv) secrecy and inviolability of private communications and documents.

In this regard, the Peruvian Constitutional Court has recognized repeatedly in case law the scope of this right, understood as:

"[...] the personal context in which a human being has the capability to freely develop and encourage their personality. Therefore, privacy comprises any data, facts or situations unknown to the community that, being true, are kept to the knowledge of the subject and a limited group of individuals. The disclosure or knowledge of the contents of these aspects by third parties may cause some harm."[13]

Hence, privacy protection is not limited to geographical spaces or particular objects, but encompasses any space, object, or situation from which information may be disclosed causing damage to an individual or a limited group of individuals.

Regarding the privacy of communications, the Peruvian Constitution establishes in Article 2 that "Communications, telecommunications or any private correspondence may only be opened, seized, intercepted, or confiscated with warrant issued by a judge and with all guarantees provided for by law." Similarly, Article 4 of the *Texto Único Ordenado* on Telecommunications Law stipulates that everyone has the right to the inviolability and secrecy of their telecommunications,[14] while Article 13 of the Regulations under the Telecommunications Law establishes that a violation of this right occurs when someone besides the sender or addressee deliberately steals, intercepts, interferes with, alters, changes the text of, deviates the course of, publishes, reveals, uses, or tries to gain knowledge for himself or any other from the contents of any communication.[15]

Finally, another legal safeguard of privacy is found in the Personal Data Protection Law, as established in Article 13:

"Communications, telecommunications, computer systems, or their instruments, when they are of a private character or use, may be opened, seized, intercepted, or audited only by reasoned order by the judge or with the authorization of their subject, with the guarantees provided in the law. Secrecy should be kept concerning the matters unrelated to the fact that motivates their examination. The personal data obtained in violation of this precept is devoid of legal effect."[16]

According to the aforementioned legal provisions, the seizure or interception of communications is a potential interference with the right to privacy. On this matter, the

UN Human Rights Council has established that "even the mere possibility of communications information being captured creates an interference with privacy."[17]

## II.2. How is Freedom of Expression Affected by State Communications Surveillance?

As stated in Article 2 of the Peruvian Constitution, every individual has the right to freedom of information, opinion, expression, and the dissemination of thought through the spoken or written word or images, by any means of social communication, and without previous authorization, censorship, or impediment whatsoever. Accordingly, the Universal Declaration of Human Rights stipulates in Article 19 that this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.[18] Article 13 of the American Convention on Human Rights[19] and Article 19 of the International Covenant on Civil and Political Rights[20] define this concept likewise.

The Peruvian Constitutional Court has further established this fundamental right as the guarantee that "all persons (individually or collectively) have the right to the free transmission and dissemination of their ideas, thoughts, value judgments, or opinions."[21]

Taking this into consideration, State communications surveillance activities are also capable of interfering with freedom of expression. Under surveillance, many individuals may be punished for the contents of their communications or may self-censor to avoid being the subject of repression. The pernicious consequences of State surveillance of communications and self-censorship have been studied in a wide variety of experiments in the social sciences. The experiments show that these consequences not only affect social and political activism but also change habitual behavior.[22] In simple terms, individuals tend to behave differently when they are monitored, and this has a negative effect on their freedom to freely express their opinions and be the recipients of any kind of information. This also has a negative effect on those who use communication tools for domestic and educational purposes.

In the context of State surveillance of communications, privacy is compromised and thusly affects the right to freedom of expression. The UN Special Rapporteur considers that privacy and freedom of expression are linked and are co-dependent.[23]

## II.3. A Compatibility Model Between State Communications Surveillance and the Observance of Human Rights

Since realizing State communications surveillance may jeopardize the exercise of fundamental rights, thorough studies and arguments as to where limits should be imposed have been made. The most reliable sources that can answer this question are the several international treaties endorsed by States. The validity of their provisions to give an answer to this question has been confirmed at a national level by the Peruvian Constitutional Court, which stated:

"Like any other fundamental rights, privacy is not an absolute right, hence, it may be limited as long as the interferences are not abusive nor arbitrary. Such interferences should be determined by law, adequate, and pursue a legitimate aim. They should also be necessary and proportional in a democratic society (Article 11.2 of the American Convention on Human Rights). The same is true in the case of the right to secrecy and inviolability of communications."[24]

In answering this question, in December 2013, the General Assembly of the United Nations issued Resolution 68/167 on the right to privacy in the digital age.[25] In it, the Assembly calls upon the States to respect and protect the right to privacy in the context of digital communications and to review their procedures, practices, and legislation regarding the surveillance of communications, with an aim to uphold the right to privacy by the implementation of all their obligations under international human rights law. It points out the need to establish independent domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception, and the collection of personal data.

Upon the request of the General Assembly, the UN Office of the High Commissioner for Human Rights presented a detailed report on the protection and promotion of the right to privacy in relation to surveillance and interception of digital communications, before the Human Rights Council and the General Assembly in June 2014. This report explicitly states that in order to provide a solution to the scope of State surveillance of communications, it is necessary to define the cases of "arbitrary" or "unlawful" interference in private life. Expanding on this, the report concludes that the surveillance practices authorized by international law must: (i) be explicitly provided for by law, (ii) be necessary for reaching a legitimate aim, (iii) be proportional to the aim, and (iv) provide for effective safeguards against abuse.

International civil society has established the International Principles on the Application of Human Rights to Communications Surveillance to structure the content of several sources

on International Law and set limitations to State surveillance of communications.[26] Led by the Electronic Frontier Foundation, Access, and Privacy International, this document was written collaboratively by civil organizations devoted to the protection of privacy and by lawyers who specialize in human rights. The 13 Principles interpret the contents of international treaties and help determine whether certain activity of State surveillance of communications is illegal according to the international human rights framework. The treaties and decisions interpreted by these principles also apply to Peru. They are a relevant and valuable source of legal doctrine used for analyzing the practices of surveillance conducted by local authorities. This document points to the fact that surveillance practices conducted by States must be consistent with the following principles:

> i. Legality: Any limitation to human rights must be explicitly prescribed by an exisiting publicly available legislative act.
>
> ii. Legitimate aim: Laws should only permit communications surveillance by specified State authorities with the purpose to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society;
>
> iii. Necessity: The activities of State communications surveillance must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim;
>
> iv. Adequacy: Any instance of communications surveillance authorized by law must be appropriate to fulfill the specific legitimate aim identified;
>
> v. Proportionality: State surveillance of communications should be, to the greatest extent possible, respectful of the human rights threatened by the implemented measure;
>
> vi. Competent judicial authority: All decisions related to communications surveillance must be made by a competent judicial authority that is impartial and independent;
>
> vii. Due process: Everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial judge established by law;
>
> viii. User Notification: Those whose communications are being surveilled should be notified with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization, as long as it does not interfere with the legitimate aim;

ix. Transparency: States should be transparent when publishing information about the use and scope of communications surveillance laws, regulations, activities, powers, or authorities;

x. Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance;

xi. Integrity of communications and systems: States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State communications surveillance purposes;

xii. Safeguards for international cooperation: States should ensure that where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied; and,

xiii. Safeguards against illegitimate access and right to effective remedy: States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected.

# III.
# State Communications Surveillance Practices in Peru

This section describes the surveillance practices conducted by the State that are recognized by the Peruvian legal system and evaluates their adequacy with regard to the international human rights framework established in the aforementioned International Principles on the Application of Human Rights to Communications Surveillance.

## III.1. Communications Surveillance in the Criminal System

The current criminal legislation of Peru establishes two regulatory groups for communications surveillance: (i) through the regulations establishing the applicable procedures for the interception of individuals' communications as a means of collecting evidence in a criminal investigation; and, (ii) through any type of regulation classifying illegal surveillance of communications as a criminal offense.

On one hand, communications surveillance is most frequently conducted in a criminal investigation framework: (i) through measures of postal interception and seizure; and (ii) through measures ordering the interception of communications and telecommunications. The general procedure applicable to any kind of interception of communications is described in Law 27697 and detailed in the Criminal Code and Criminal Procedure Code, as well as in the protocol of joint action for the interception or recording of telephone communications or other forms of communication, implemented by Ministerial Order Nº 0243-2014-JUS.

According to this legal framework, only a judge may authorize a prosecutor to gain knowledge of and to control an individual's communications under preliminary or jurisdictional investigation. The prosecutor may only do so in the following cases: (i) kidnapping, (ii) human trafficking, (iii) child pornography, (iv) aggravated robbery, (v) extortion, (vi) drug trafficking, (vii) migrant smuggling, (viii) crimes against humanity, (ix) crimes against national security and treason against the nation, (x) embezzlement, (xi) corruption of public officials, (xii) terrorism, (xiii) tax and customs crimes, (xiv) money laundering, and (xv) cyber crime.

Interception of communications can only be requested by criminal prosecutors, attorneys general and the national prosecutor. Communications surveillance is conducted by the Public Prosecutor's Office authorized personnel and/or the Peruvian National Police under the supervision of the prosecutor in charge of the investigation. The law outlines that communications companies should provide them with the technical support needed in order to guarantee the real-time interception and monitoring of communications. They may also request the support of natural or legal persons specialized in information collection activities.

There are two stages of this: collection and monitoring. The former refers to the processes through which the communication is gathered and registered. The latter comprises the official acknowledgment of the content of communication and eliminating what is not of interest to the investigation.

The request that the prosecutor sends to the judge must be reasoned and contain all the necessary data. Moreover, it must include evidence that allows the judge to grant, under his or her judgment, the corresponding authorization. If the request is denied, the prosecutor may appeal the judgment to a hierarchical superior starting the day after he or she is notified. The prosecutor's request and the judicial authorization must contain the necessary specifications to distinguish the different types of collection and monitoring that are intended to be conducted, including:

> i. Whether a certain communication is going to take place either in an indeterminate group of communications, or under particular circumstances.
>
> ii. Whether the communication is going to take place in the future or has already taken place.
>
> iii. Whether the communication is closed or encrypted.
>
> iv. Whether the communication's sender, recipient, or any other individual connected to the communication has tried to hide either their identity or any fact or circumstance mentioned in the communication; and whether access to or the identification of the communication or any of its parts, or the information transmitted has been obstructed in any way.

During the authorized time span for collection, the prosecutor may regularly monitor the data collected so far, providing that the collecting method is compatible with this practice. If any other evidence of criminal acts is discovered during this period, the prosecutor should notify the competent judge for him or her to decide whether the acts are relevant in relation

to the current investigation, or for the Public Prosecutor's Office to determine whether the discovered acts require criminal investigation.

Finally, Law 27697 establishes that those involved in the process of investigation—the judge, court staff, the prosecutor, the prosecutor's support team, the Peruvian National Police, judicial experts, attorney generals, and any natural or legal authorized persons—should maintain confidentiality of the information obtained during the investigation. Violation of confidentiality is penalized with disqualification regardless of the applicable criminal, civil, and administrative consequences.

The Protocol on the Interception and Recording of Communications was passed in November 2014 by Ministerial Order Nº 0243-2014-JUS. Its aim is to organize the procedure into clear stages so that the police, the Public Prosecutor's Office, and the Judicial Branch can improve their implementation. This protocol divides the procedure into seven stages, describing in detail their requirements: (i) initial police report establishing the measure needed, (ii) prosecutor's request or petition, (iii) judicial decision, (iv) notification of the decision to the prosecutor, (v) implementation of the measure, (vi) transcription of the recordings, (vii) control or re-examination at the request of the affected.

### III.1.1. Interception of Postal Communications for Investigation and Prevention Purposes

Article 226 of the Criminal Procedure Code regulates the procedure for the interception of postal communications, such as letters, documents, telegrams, and other kinds of objects sent by mail. This type of interception can only occur at the prosecutor's request and with judicial authorization by the judge in charge of the preliminary investigation. The Code outlines that the court order be issued when interception is indispensable for the clarification of the facts under investigation. It shall continue until necessary, but it shall not continue after the investigation has finished. Postal interception may not last longer than the investigation of the case.

With regard to notification, Article 227 establishes that when the investigation has finished, the individual being surveilled must be notified about the procedures conducted. The individual may ask for judicial re-examination within three days of receiving notice. In said hearing, the judge shall determine the appropriateness of the procedure and the relation of the intercepted and seized communications to the investigation.

### III.1.2. Communications Surveillance for Investigation and Prevention

Article 230 of the Criminal Procedure Code indicates that whenever there exists sufficient evidence to consider the commission of a crime punishable by over four years in prison, the

prosecutor may request the judge in charge of the preliminary investigation to intercept and record the individual's telephone, radio or other kinds of communications. The communications of the individuals connected to the person being surveilled may also be intercepted and recorded.

Nonetheless, the article indicates that this interception should prove absolutely essential to continuing with the investigation. It is necessary that the request and the judicial decision authorizing the surveillance indicate the name and address of the affected, as well as the identification of the telephone or any other type of telecommunications being intercepted, recorded or registered. They should also describe the form of interception, its scope and duration, and the police unit and prosecutors conducting the intercepting, recording or registering actions.

The interception or surveillance activity shall not last longer than sixty (60) calendar days. Exceptionally, this term may be extended, provided that there is a reasoned request from the prosecutor and a decision by the judge in charge of the preliminary investigation. Interception should immediately be interrupted when the aforementioned sufficient evidence ceases to exist or when the requested period of surveillance is over.

Article 231 of the Criminal Procedure Code establishes that communications must be registered by recording in order to guarantee accuracy. In addition, it stipulates that all recordings, signs or evidence collected during the procedure ordered by the judge, as well as the Protocol of Collection and Monitoring shall be delivered to the prosecutor, who is in charge of preserving them, and shall ensure their confidentiality.

Regarding the notification and contestation of the measure, the aforementioned article of the Criminal Procedure Code establishes that, once the surveillance activities and the investigation have finished, the individual being surveilled must be notified about it. The affected may ask for judicial re-examination within three days of receiving notice. On this subject, the Code specifies that the affected shall only be notified if the investigation allows so, and as long as it does not jeopardize the lives or physical integrity of third parties. Finally, the law says that the secrecy of the surveillance activities conducted requires a reasoned special judicial decision and shall be subject to a period set by the judge.

Additionally, Article 231 of the Criminal Procedure Code allows for an emergency mechanism applicable exclusively when there is an acknowledgment of new subjects or telephone numbers requiring interception in order to prevent terrorism, drug trafficking, or kidnapping on the verge of being conducted. Under these circumstances, the interception may only be ordered by the prosecutor, as long as he or she subsequently notifies the judge for the revision of such measure.

Furthermore, Article 207 of the Criminal Procedure Code establishes that, in investigations related to violent or serious crimes or criminal organizations, the prosecutor, on his or her own initiative or upon police request, may conduct surveillance activities through photographs and any other special technical means of observation, without notifying the affected. This article establishes the need for judicial authorization only when said activities are performed indoors.

### III.1.3. Use of State Surveillance Devices for the Restriction of Individuals' Freedoms

Article 52 of the Criminal Code describes another instance in which State authorities may subject an individual to electronic surveillance. It establishes that a judge may, ex officio or upon a party's request, turn the punishment of imprisonment into a punishment of personal electronic surveillance. This faculty is described in Law 29499, which defines personal electronic surveillance as a monitoring mechanism, whose aim is to monitor the movement of the accused and the convicts, within a scope of action that takes an indicated address or place as a reference point. The monitoring is carried out by using bracelets, ankle bracelets or body devices.

### III.1.4. Protection of Communications Against Surveillance Activities

In several articles, the Criminal Code stipulates a series of crimes that may be committed by private actors conducting surveillance activities, such as the infringement of personal and family privacy (Article 154), personal data trafficking (Article 154-A), disclosure of personal and family privacy (Article 156), illicit use of digital files (Article 157), violation of secrecy of communications (Article 161), telephone interference (Article 162), seizure or illicit mislaying of correspondence (Article 163), and illicit publication of correspondence (Article 164).

## III.2. Surveillance in the Intelligence System

The National Intelligence System also considers situations in which surveillance of communications may be needed, according to the procedures described in Legislative Decree 1141 on the enhancement and updating of the National Intelligence System (SINA, in Spanish) and of the National Intelligence Directorate (DINI, in Spanish) and their regulations.[27]

Article 32 of Legislative Decree 1141 regulates the special procedures for the collection of information. These procedures enable access to strictly indispensable information that is essential to accomplish the aims of surveillance activities. Their execution should be

approved by any of the two (02) ad hoc superior judges in the Judicial Branch appointed by the Supreme Court of Peru.

Article 33 of the aforementioned legislative decree establishes that the authorization enabling the execution of these procedures might only be requested by the Director of National Intelligence, and that it must contain: (i) the identification of the individual or individuals affected, (ii) the specification of the measures requested, and (iii) the motivation and duration of these measures.

Said article also specifies that the judicial decision by the ad hoc superior judge must be issued within the first twenty-four (24) hours after the submission of the request, and that it is binding on all public entities that should contribute to its execution and obey the provisions on classified information. If the request for the procedure is denied, there follows an appeal, which shall be resolved by an ad hoc superior tribunal presided by the other active ad hoc superior judge and the two alternate ad hoc superior judges. The process of appeal must also be initiated and resolved within twenty-four (24) hours.

Legislative Decree 1141 further establishes that in cases of national security and under emergency situations, the Director of National Intelligence may, exceptionally, authorize the execution of a special procedure of information collection, and should immediately legalize the request before the ad hoc superior judge. The judge may, within the following twenty-four (24) hours, ratify or deny it. If he or she decides to deny it, an appeal follows.

The aforementioned regulation lays out that in no case shall the intelligence reports be of probative value in judicial, administrative and/or disciplinary procedures, but their content may act as a guiding element during the investigation. To that effect, Article 35 states that all information collected during the intelligence activities by the National Intelligence System (SINA, in Spanish) that proves irrelevant to the aim must be destroyed by the officials in charge of the agency that detects it since it compromises individuals' private lives. Failure to comply with this requirement may result in penalty of disqualification regardless of the applicable criminal, civil and administrative consequences.

With reference to the possibility of external control of the surveillance activities conducted by the intelligence system, Article 5 of Legislative Decree 1141 stipulates that authorities, officials, or legally authorized institutions, using their delegated powers of control and oversight, may request the access to classified intelligence information from the components of the National Intelligence System (SINA, in Spanish), which will be provided with the mandatory notification to the National Intelligence Directorate. According to its current organization, established by the Legislative Decree 1141, the National Intelligence Directorate is subject to three stages of control:

***Judicial Branch:*** Whenever it is necessary to access information protected by the secrecy of telecommunications or by bank secrecy. In these cases, there exist two superior court judges specially appointed by the Supreme Court, who exclusively receive and respond to the requests for "information collection" submitted by the Intelligence Directorate.

***Legislative Branch:*** The Intelligence Commission in Congress is the closest to an independent authority capable of reviewing intelligence activities. The Commission has the power to review every intelligence plan as well as cases processed before the judges responding to the requests for information collection. It receives an annual report directly from the Director of Intelligence.

***Government Accountability Office:*** The Institutional Supervisory Body only has the power to oversee the activities related to administrative and financial management of the resources and goods of the components of the National Intelligence System.

## III.3. Surveillance Conducted by the Peruvian National Police

Since late July 2015, a new regulation allowing the police to access geolocation data in real time from any user's cellphone or electronic devices connected to a telecommunications network has been in force. Legislative Decree Nº 1182 aims to legislate on data resulting from telecommunications for the identification, localization, and geolocalization of communication equipments in the fight against delinquency and organized crime on the part of the Peruvian National Police. This legislative decree creates a mechanism through which the police can send a request to any telecommunications operator to access cellphone location data or electronic devices. According to this regulation, after the police make the request, companies like Movistar or Claro are immediately required to provide access to this information in real time. In order to accomplish this, the police need not be granted any type of prior judicial authorization to obtain this information from the companies.

Accordingly, the police may only use this mechanism when the following three requirements occur simultaneously: (i) when there is a blatant crime (*delito flagrante, in Spanish*),[28] (ii) when the punishment for the crime under investigation is superior to four years of imprisonment, and (iii) when the access to this information is necessary to the investigation. Failure to comply with these requirements shall only be reviewed after the police have accessed the data. Thus, the unit in charge of the police investigation shall have twenty-four (24) hours to send the prosecutor a report justifying its request. Then, the prosecutor shall have again twenty-four (24) hours to request the "validation of the measure" to a judge. At the same time, the judge receiving the request shall have 24 hours to

take a stance on the legality of the request and to set a period during which it shall be in force.

Following this system, up to 72 hours may go by from the time the police start to monitor any citizen until the time the judge issues a decision on the legality of the measure and verifies whether the requirements have been met.

Under the former scheme, whenever the police needed to access the geolocation of any phone line, it was necessary for a prosecutor to request authorization from a judge, whether a blatant crime had taken place or not. The prosecutor was responsible for convincing the judge of the existence of sufficient evidence; and it was the latter who established the way of proceeding, the appropriateness, time period and the safeguards applicable to the interception. In the past, the police needed explicit judicial authorization to access information. But since this new decree has been in force, the police are able, upon their sole request, to access it directly from the communications companies, as long as the provisions established by Legislative Decree Nº 1182 are met.

Article 6 of the aforementioned legislative decree specifies that this mechanism shall only apply to the geolocation data of the users of public telecommunications services. Consequently, any type of communications interception that requires special procedures are left outside the scope of this regulation. Moreover, Article 7 lays down a liability regime for police agents who use this system maliciously. At the same time, it establishes that operators and their dependents should maintain confidentiality of the information given to the Police under this mechanism.

On September 10, 2015, Bill No. 4809/2015-CR was introduced into Congress, and signed by Congressman Hector Becerril and five others from the bench "Popular Force" (Fuerza Popular), which seeks to repeal Legislative Decree 1182.[29]

For the most part, the proposal rewrites the decree retaining many of its articles, but with a fundamental change: access to location data can only be authorized by a criminal judge on duty. The three concurrent instances in which this order can be used remain: (i) blatant crime, (ii) more than four years in prison, and (iii) test of necessity. In Article 4, the draft points out that the whole procedure, from when the Public Ministry places the order until the criminal judge authorizes or rejects it, should last a maximum of twenty-four (24) hours and encourages communication to be conducted by phone, email, teleconferencing, or other means.

The proposal seeks to restore the role of the prosecutor as the leader of a criminal investigation. In the model proposed in Legislative Decree No. 1182, the police were the only

ones who could request immediate access to geolocation data. This is a misunderstanding of the constitutional role that the prosecutor had as the main authority responsible for investigating any crime.

Article 3 of the new bill clarifies that the prosecutor is the only one authorized to request urgent access to location data from a criminal judge. This new provision would, if approved, be consistent with the Criminal Procedure Code which authorizes the attorney general to do the same thing during a preliminary investigation. The new bill would make such access requests during preliminary hearings prior to the preliminary investigation.[30]

In October 2015, under Ministerial Order No. 0631-2015-IN, the Ministry of Interior approved the "Protocol for access to geolocation data of cellphones and electronic devices of similar nature," that establishes the workflow of the procedure for accessing geolocation data created by Legislative Drecree No. 1182. However, based on the national security exception of the Freedom of Information Law, the Ministry categorized this Protocol as "reserved information." This means that no Peruvian citizen can obtain knowledge or access content of the Protocol, despite the fact that the procedure described on it may be applied to him or her. After a few months of this approval, a spokesperson from the Ministry declared that between December 2015 and January 2016 there had been 45 requests to access this data, but didn't say how many suspects had been found in those cases.[31]

## III.4. Obligation to Telecommunications Companies to Cooperate with State Communications Surveillance Activities

The Peruvian law further imposes obligations on private companies to cooperate with the surveillance activities conducted by the State. The main obligation provided for in the Peruvian legislation is that of communications traffic data retention. It is described in Legislative Decree Nº 1182 and has been in force since July 2015.[32]

The Second Complementary Final Provision of the aforementioned decree imposes on all public telecommunications licensees—fixed and mobile telephony and Internet access—and on the public institutions related to these services the obligation to keep the data obtained from telecommunications for a period of up to thirty-six (36) months or three years. The decree requires the obtained data to be stored during the first twelve (12) months allowing for online requests and real-time delivery to the authorities, after the granting of a judicial authorization.

Additionally, the data of the remaining twenty-four (24) months must be kept in a special electronic storage system and delivered within seven (7) days following the judicial

authorization. According to what is established by this legislative decree, operating companies that fail to comply with these obligations shall be held liable. However, given the recent enactment of this new obligation, it is still not clear what data is considered "data derived from telecommunications." Even though this obligation on data retention shall not be able to address the content of communications, pending regulations on this issue may or may not include certain types of metadata within its scope.

Before Legislative Decree Nº 1182, the only existing obligation was to keep information that was likely to be supervised by the regulatory authority and the information of call records for up to two (2) months. However, under the aforementioned legislative decree, these regulations have not been repealed. On one hand, Law 27336 stipulates that all entities under the supervision of the Supervisory Body for Private Investment in Telecommunications (OSIPTEL, by its Spanish acronym) have the obligation to keep, for at least 3 (three) years, information like valuation, details of call records, invoicing of the services operated, and any information that must be kept in order to comply with the technical standards mandated by a competent authority, or with contractual or statutory obligations applicable to these services.[33] On the other hand, the regulation on the users' rights passed by OSIPTEL —the Terms of Use of Public Telecommunications Services— stipulates a similar obligation to keep records. However, this one is much narrower. Specifically, Article 65 of the Terms of Use lays out that the subscribers have the right to request a copy of their incoming calls records from the past two (2) months from the operating companies.[34] Accordingly, the operating companies are compelled to keep the information of subscribers' incoming and outgoing calls for at least two (2) months to comply with this obligation.

Furthermore, Article 230 of the Criminal Procedure Code also establishes that public telecommunications licensees are compelled to immediately provide the geolocation of cellphones and to execute real-time, uninterrupted interception, recording, or register of communications mandated by judicial decision. This obligation should be fulfilled by the licensees 24 hours a day, 365 days a year, under penalty of being deemed responsible under the law in case of a compliance failure.

It further establishes that the employees of said companies must maintain confidentiality of this information, except when they are summoned to be witnesses of the procedure. The aforementioned article compels the licensees to enable access, compatibility, and connection between their technology and the Peruvian National Police System of Interception and Monitoring of Communications. In the same vein, it is further established that whenever the licensees renew their equipments and software, they are compelled to maintain compatibility with the Peruvian National Police System of Interception and Monitoring of Communications.

In regard to the special case of monitoring activities conducted by the intelligence system, Article 41 of Legislative Decree 1141 stipulates that all natural and legal persons are legally compelled to give the National Intelligence System (SINA, in Spanish) the information linked to any intelligence activities required by the governing body, at no cost. When the required information is confidential, the delivery of such information shall not be an infringement of the duty of confidentiality, since intelligence personnel is compelled to maintain it. The only exception to this obligation exists whenever there is a threat to information protected by professional confidentiality, personal or family privacy, bank secrecy, financial secrecy, and other types of protection of information recognized by the Constitution.

## III.5. Does the Peruvian Legislation Comply with the International Standards for Surveillance Activities?

The Peruvian legislation presented in this section provides us with a general view on how the Peruvian State understands and conducts surveillance of communications in the case of blatant crimes. As a consequence of the reforms of criminal and intelligence laws in the past few years, the majority of these regulations have been in force for less than ten years, and are still being modified. There is a striking difference in the provision of safeguards for fundamental rights between the criminal and intelligence systems.

In terms of *legality*, the limits of and requirements for the interception of communications in the framework of a criminal investigation are better delineated than the ones conducted by the intelligence system. On one hand, the criminal system specifies what the objects of surveillance may be and demands that they be explicitly stated in the request and ensuing authorization. On the other hand, the intelligence system makes reference only to "information collection measures" without specifying which may be included.

However, there is still a lack of accuracy regarding the scope of surveillance in the interception of electronic communications and devices. While the criteria used for the interception of telephone communications have been thoroughly developed and specified, the guiding elements for the interception of other types of communications through the Internet—like e-mail accounts or social media profiles—have not really been discussed. The mechanism for accessing geolocation information deserves special mention. A decision by the Ministry seriously violates the principle of legality as it classifies the Protocol that establishes the procedure for accessing the geolocation data of cellphones and electronic devices, as "reserved information." Through this decision, the Peruvian government has created a "secret law" that could be applied to every Peruvian citizen. This decision also

contradicts past decisions issued by the Ministry, who previously established that the Protocol used in cases of telecommunications wiretapping is public information.

This imbalance in the rigor of the legal framework can also be seen in the analysis of the *legitimate aim of surveillance activities.* Law Nº 27697 provides a closed list of crimes in which interception may be required for investigation. This list, currently made up of fifteen crimes, displays that the State has the power to affect the secrecy of communications exclusively when there is an investigation of the most serious crimes. For their part, the intelligence laws recognize that interception mechanisms may only be used for any of the aims of intelligence activities—the aims are: the protection of human rights, the protection of the people against threats to their safety, the defense of national sovereignty, and the promotion of general welfare and comprehensive national development.

Both systems agree an analysis of *necessity, adequacy* and, *proportionality* are needed when ordering surveillance activities, either through the substantiation of the request sent by the prosecutor to the judge or that of the request sent by the Director of Intelligence to the special judge. The criminal system demands that both the police and the prosecutor be compelled to specify the requested measures, the individuals affected, the period during which the surveillance shall take place, and the existence of enough criminal evidence. The intelligence laws require that the request for information collection identify the individuals affected, establish the requested measures and their duration, and justify the reasons for the request.

In terms of proportionality, both systems compel the authorities in charge of the interception to destroy all collected material that is useless for the investigation. Nonetheless, it is worth mentioning that the data retention mechanism encompassing all the Peruvians' data related to communications, has not proven to be necessary, adequate, nor proportionate.

Both systems comply with appointing an independent and *competent judicial authority* that must receive, evaluate, and authorize the requests for the interception of communications. In the criminal system, this authority is the judge of the preliminary investigation, who is appointed independently by the Judicial Branch and is even different from the judge who, in case a proceeding is initiated, shall rule on the basis of the criminal complaint. On the other hand, the intelligence system stipulates that the requests for the collection of information must be addressed to one of the two ad hoc superior judges of the Judicial Branch, who shall be appointed by the Supreme Court of Justice of Peru, exclusively to rule on these requests.

Unfortunately, this requirement is not met in cases involving the Peruvian National Police's access to geolocation data. In such cases, operators are compelled to deliver this information upon receipt of a police request for data provided the following requirements are met: there is blatant crime, the crime's punishment exceeds four years of imprisonment, and accessing this information is necessary for the investigation.

With respect to the *observance of due process,* the guarantees of independent judge, justification and judicial review are fulfilled; however, publicizing the investigation files during and after the investigation has not been provided for yet. In some cases, the complete publicizing of the process may compromise the aims of the investigation. However, there are no obligations whatsoever to publicize such files in the future. Several provisions establish the need for complete confidentiality by any public or private official involved in the activities of interception of communications. Once again, in the case of access to geolocation data, there is no previous judicial process. Therefore, there is an evident violation to the presumption of innocence and to the right to a natural judge of those affected by the measure.

Another principle that is complied with only by the criminal system is that of *user notification.* Thus, the Criminal Procedure Code explicitly establishes that after the execution of the interception measure and of the subsequent immediate investigations, the individual affected must be notified about all the procedures conducted. This way, the individual whose communications were surveilled may ask for judicial re-examination within three days of receiving notice. Conversely, the intelligence system orders to maintain complete confidentiality of all procedures conducted, classifying information as secret.

In the case of the police accessing geolocation data, not only does user notification not exist, but also companies are not allowed to reveal their participation on the case and must maintain confidentiality of the shared information.

There are no specific obligations of *transparency* or *public oversight* on the Peruvian State activities of communications surveillance. With the exception of occasional notifications given to those whose communications were intercepted under a criminal investigation, there are no legal provisions that compel the entities conducting these activities to periodically inform about the number, type, and scope of the practices conducted.

In the intelligence system, the only existing oversight mechanism is that of the Intelligence Commission in Congress; however, all information provided to the commission is also classified as secret. Recently, the lack of oversight of the activities of surveillance conducted by the intelligence system has triggered a political crisis that caused the termination of the system and its ensuing reorganization.[35] This lack of transparency is apparent when, during

their occasional press appearances, the police share only partial statistics about the number of times geolocation data has been requested. They also omit the precise number of times that this informations was used to capture a suspect or formally trigger a criminal court case.

In terms of the *Integrity of Communications and Systems,* the Criminal Procedure Code establishes the specific obligation for the public telecommunications licensees to enable access, compatibility and connection between their technology and the Peruvian National Police System of Interception and Monitoring of Communications. Even though there is no public record of this obligation of interconnection being misused by the State, it does impose a restriction on the freedom of licensees to develop their communications infrastructure according to their interests and to be able to guarantee their users' privacy.

Concerning the *safeguards for international cooperation,* Peru has signed mutual legal assistance agreements in the criminal field with twenty-five (25) countries.[36] Among others, Peru also signed a treaty on the execution of penal sentences in 1980 and an extradition treaty in 2003 with the United States. These agreements consider investigation, inspection and the delivery of information and evidence—which may be related to the monitoring of communications—as an act of legal international cooperation.

Finally, the Peruvian criminal system provides for *safeguards against illegitimate access* by private actors. The Criminal Code establishes a punishment of up to eight years of imprisonment for those who intercept or eavesdrop on telephone communications or communications of the sort, with aggravations in the case these communications are disseminated through mass media.

# IV.
# Recommended Law Reforms

There is a plethora of possible and necessary reforms that could be added to the Peruvian legislation in order to coordinate State surveillance mechanisms with Peru's international obligations relating to human rights. Under no circumstance is the purpose of these reforms to weaken the mechanisms of criminal investigation or national security. On the contrary, the following suggestions intend to legitimize and balance the power of State surveillance.

The most urgent reform is related to revising the mechanism by which the Peruvian National Police may access the geolocation data of any user. In such cases, a judicial authorization prior to the investigation should always be a constitutional requirement. The system like the one described in Legislative Decree Nº 1182 represents a shortfall in the guarantees of the right to privacy of all the Peruvians. Similarly, it is important to reconsider the need to continue to have a storage system that keeps data traffic for up to three (3) years, with regards to Peruvians' communications.

It is also necessary to describe the legislation applicable to intelligence activities in detail, in order to establish a limit to the scope of intelligence activities and tasks. Hence, it is important to specify what the intelligence collection activities are, and to indicate the time period in which the collected information will be destroyed, or the criteria under which it shall be shared with other institutions or foreign States.

Moreover, it cannot be left unsaid that there is a dissociation between the regulations on the activities of State surveillance and the manner in which they are conducted. Nowadays, there are no means of knowledgeably determining the level of compliance to legal guarantees applicable to communications surveillance. Thus it is necessary to implement additional transparency measures such as the regular publication of statistical information by the police and the Judicial Branch on annual requests for communications interceptions, as well as the specific scope of the requested telephonic, electronic or location tracking interceptions. These reforms do not jeopardize the effectiveness of the measures ordered, and they allow the general public democratic control over authorities' power to execute such activities. Furthermore, given the new legal framework approved in 2015, these types of transparency measures shall provide valuable insight for the evaluation of recent reforms and their usefulness in our context.

The minimal checks and balances mentioned previously, especially regarding intelligence activities, have triggered a real government crisis. During the first months of 2015, press reports published a series of practices and activities of surveillance conducted by the National Intelligence Directorate. These collection activities of public and private information were conducted against political leaders from the opposition. Such revelations motivated a process of reorganization of the System of Intelligence and the dismissal of the President of the Council of Ministers.[37]

Similarly, the telecommunications companies and Internet service providers' obligations should be better specified. It is clear that they are compelled to facilitate the interception and storage of communications, provided a judge requests it for a criminal investigation. However, their obligations to the intelligence system are too broad and may be misused in ways different from intelligence work. Thus, the law should specify the form and the limits of the requests submitted by the intelligence body to communications service providers.

Finally, it is necessary for the Intelligence Commission in Congress to have more autonomy. This Commission is the independent body with the greatest capability to control intelligence work. Nonetheless, little is known about its work, since the meetings and decisions are confidential. Thus, transparency obligations could be imposed on the Commission, without weakening its functions, so that it reports on the number of times its members or special judges are summoned and on the number of special procedures conducted for the collection of the information it reviews. In this way, the information gap between the authorities in charge of overseeing intelligence work and the general public may be bridged.

# Endnotes

1 PEN American Center, Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor, November 12, 2013, available at: https://eff.org/r.ozzn

2 James Staten, The Cost of PRISM Will Be Larger Than ITIF Projects, *Forrester Research* (blog), August 14, 2014, available at: https://eff.org/r.37z0

3 Oscar Castilla, This is How *Constelación* Works, the System of Telephone Tapping of DIRANDRO (Anti-drug Directorate) *El Comercio*, November 30, 2011, available at: https://eff.org/r.e3f2

4 The Peruvian congress censors the prime minister for espionage, El País, March 31, 2015, available at: https://eff.org/r.vxsy

5 Miguel Morachimo, Nuevo proyecto de ley quiere derogar la #LeyStalker, Septiembre 18, 2015, disponible en: https://eff.org/r.7z02

6 Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, United Nations, A/HRC/23/40, April 17, 2013, available at: https://eff.org/r.8fb6

7 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review 193 (1890), available at: https://eff.org/r.bbgj

8 Inter-American Court of Human Rights. Case of Escher et al v Brazil Preliminary Objections, Merits, Reparations, and Costs. Judgment on July 6, 2009.

9 Constitutional Court Sentence on case No. 00655-2010-PHC/TC. October 27, 2010 Legal basis 18, available at: http://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

10 Universal declaration of Human Rights, Article 12.—No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

11 American Convention on Human Rights, Article 11.—Right to Privacy (1) Everyone has the right to have his honor respected and his dignity recognized; (2) No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation; (3) Everyone has the right to the protection of the law against such interference or attacks.

12 International Covenant on Civil and Political Rights, Article 17.—(1) No one may be the object of arbitrary or abusive interference with his private life, his family, or his correspondence, or of unlawful attacks on his honor and reputation; (2) Everyone has a right to the protection of the law against such interference or attacks.

13 Constitutional Court Sentence on case No. 6712-2005-HC/TC. October 17, 2005.

14 Supreme Decree Nº 013-93-TCC, *Texto Único Ordenado* on Telecommunications Law.

15 Supreme Decree Nº 020-2007-MTC, Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones.

16 Law No. 29733, Personal Data Protection Law, available at: https://eff.org/r.beoh

# Endnotes

17 United Nations Human Rights Council, The Right to Privacy in the Digital Age. Report of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014.

18 Universal Declaration of Human Rights, Article 19.— Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers.

19 American Convention on Human Rightsm, Article 13.—Freedom of Thought and Expression (1). Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. (2). The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: (a) Respect for the rights or reputations of others; or (b) The protection of national security, public order, or public health or morals. (3) The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impeded the communication and circulation of ideas and opinions. (4). Notwithstanding the provisions of paragraph 2, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence. (5). Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.

20 International Covenant on Civil and Political Rights, Article 19.—(1). Everyone shall have the right to hold opinions without interference. (2). Everyone shall have the right to freedom of expression; this right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. (3). The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) Respect for the rights or reputations of others; (b) The protection of national security, public order, or public health or morals.

21 Constitutional Court Sentence on case No. 0905-2001-AA/TC. August 14, 2002.

22 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014), 179.

23 Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/23/40, April 17, 2013.

24 Constitutional Court Sentence on case No. 00655-2010-PHC/TC. Octorber 27, 2010. Legal basis 19, available at: http://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

25 United Nations General Assembly, *The Right to Privacy in the Digital Age,* Resolution adopted by the General Assembly on December 18, 2013, A/RES/68/167.

26 International Principles on the Application of Human Rights to Communications Survellance, available at: https://es.necessaryandproportionate.org/text and EFF, ARTICLE19, Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to

# Endnotes

Communications Surveillance, available at: https://es.necessaryandproportionate.org/AnalisisLegal

27 In early February 2015, while this report was in its final stages, the Peruvian government announced its intention to completely reorganize the national intelligence system. This reorganization may imply a partial or total renovation of the aforementioned legal regulations.

28 A flagrant crime is a crime that has just been committed, is being committed, or less than 24 hours has passed since it was committed (Article 259 Criminal Procedural Code).

29 Bill No. 04909/2015-CR proposes to establish the rules of coordination between National Police, Public Ministry, and the Judicial Branch in cases of flagrant crime, to access the location or geolocation of mobile phones and electronic devices of similar natures, available at: http://www.proyectosdeley.pe/p/4twcy6/

30 At the time this report went to press, this bill was still pending in Congress.

31 Pierina Chicoma Castro, "En 2 meses la PNP geolocalizó 34 celulares de extorsionadores," *El Comercio*, February 8, 2016, URL: http://elcomercio.pe/lima/seguridad/2-meses-pnp-geolocalizo-34-celulares-extorsionadores-lima-callao-noticia-1877159

32 Legislative Decree 1182, the Second Complementary Final Provision – Preservation of the data obtained from telecommunications. All public telecommunications licensees and public institutions related to these must preserve the data obtained from telecommunications for the first twelve (12) months in computer systems enabling its online query and real time delivery. After this time period has finished, said data must be preserved for twenty-four (24) additional months in an electronic storage. Data stored for a time period not exceeding twelve months is delivered online and in real time, after the reception of the judicial authorization. Data stored for a time period exceeding these twelve months is delivered within seven (7) days following the judicial authorization, under penalty of being deemed responsible under the law.

33 Law No. 27336, Law for the Development of the Role and Authority of the Supervisory Body for Private Investment in Telecommunications, Article 16. - Obligations on the supervised entities. The supervised entities are compelled to:(...) (e) Preserve, for a time period of at least three (3) years, information like valuation, details of call records, and invoicing of the services operated in order to comply with the obligatory technical standards mandated by a competent authority, or with contractual or statutory obligations applicable to these services.

34 Resolution by the Governing Body Nº 138-2012-CD-OSIPTEL, Terms of Use of Public Telecommunications Services, Article 65.- Register of Information about Incoming Calls. Upon their request, the subscribers have the right to request a copy of their records of incoming calls from the past two (2) months from the telecommunications operators. This information includes voice communications received by the users of line and mobile telephone services. The request must be submitted personally by the user, either orally or in writing, in any of the operators' offices. The operating company may allow additional mechanisms for submitting this request. The issuance of this record may be charged. This record shall include the caller's number, the date, start time and duration of the call. The operating company may hand this information, in accordance with the user's instructions, in the office of the company, or the user's home, through a printed document, electronically, or through any computer form with the capacity to store information, in a time period of, at most, fifteen (15) working days following the submission of the request. Should the operating company refuse to deliver this record, or should it fail to hand it in the specified time limit, the user may initiate a complaint, according to what is established in the Directives for Complaints.

# Endnotes

35 The government will close the DINI for 180 days to reorganize it. *El Comercio*, February 9, 2015, available at: https://eff.org/r.v79d

36 See list of treaties of legal assistance on criminal matters signed by Peru, Judicial Branch, available at: https://eff.org/r.iofv

37 Government announces the closing of the National Intelligence Directorate for 180 days, Agenda País, February 5, 2015, available at: http://www.agendapais.com/?p+16718