State Communications Surveillance and the Protection of Fundamental Rights in Uruguay

By Fabrizio Scrollini, Ana Tudurí, and Katitza Rodríguez

March 2016

ELECTRONIC FRONTIER FOUNDATION

Fabrizio Scrollini is the chairman of Data Uruguay. He conducts research on public information access, transparency, and open data. He has a law degree from the Catholic University of Uruguay (UCU), a Masters in Public Policy at Victoria University of Wellington and is a PhD candidate at the London School of Economics and Political Science.

Ana Tuduri is a researcher and studies issues related to privacy, surveillance, intellectual property, and digital rights. She has a law degree from the University of the Oriental Republic of Uruguay (UDELAR). Ana previously worked on human rights issues within the Uruguayan prison system.

Katitza Rodríguez is the international rights director at the Electronic Frontier Foundation. She concentrates on comparative policy of international privacy issues, with an emphasis on law enforcement, government surveillance, and cross border data flows. Katitza holds a Bachelor of Law degree from the University of Lima, Peru.

We would like to thank Kim Carlson and David Bogado of EFF for their copy-editing and formatting contributions.

This report is part of a larger regional project conducted in eight Latin American countries by the Electronic Frontier Foundation, an international non-profit organization that has been defending freedom of expression and privacy in the digital world since 1990.

Table of Contents

I.

State Communications Surveillance in Uruguay

In July 2013, *El País* newspaper revealed Uruguay's secret purchase of the surveillance software "El Guardián."[1] According to media reports, "El Guardián" increases the Uruguayan government's capacity to spy on mobile phones, emails, and publicly available information posted on social media. This revelation sparked a reaction among civil society[2] and politicians alike about the software's use, reach, and scope, and the applicable legal framework that would restrict it to what is necessary and proportionate.

Uruguay is a country known for its stable legal framework and strong democratic institutions, but surveillance technologies have existed for more than a century in Uruguay,[3] and the lack of a clear legal framework surrounding such technologies leaves great room for improvement.

Traditionally, the confidentiality of communications is protected under the right to privacy. In exceptional cases, the interception of communications is allowed. But, like many countries in the region, there have been cases of abuse—in Uruguay, particularly during its last military dictatorship (1973-1985). During this period, the communications of many innocent individuals were illegally intercepted for the purpose of quelling political activity.

This report analyzes the constitutional and international framework of human rights in relation to communications surveillance. It examines the law, case law, and national doctrine that authorize it. The report also assesses whether national surveillance legislation complies with international human rights standards ratified by Uruguay, using the International Principles on the Application of Human Rights to Communications Surveillance as a guideline.[4] It concludes with a series of recommendations for the Uruguayan government and civil society.

Given the technical, legal, and political complexity of this issue, we define "communications surveillance" and "communications metadata" as follows:

- *Communications surveillance:* The monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.[5]

- *Communications metadata*: Information about an individual's conversation (e-mails, phone calls and text messages sent and received and posts on social networks), identity, online accounts, pages, websites visited, books, and other materials read, web searches conducted, resources used, or interactions (such as the origin and destination of communications, people interacted with, friends, family, acquaintances, places and time, or proximity to others).[6]

II.
Legal Framework

2.1 Constitutional Protection

Fundamental freedoms, such as the right to privacy, freedom of expression, freedom of association, and the right to information, possess extensive legal protections at both a national and international level. At a national level, these rights are protected by the Constitution of the Eastern Republic of Uruguay in Articles 7, 29, 72, 82, and 332. Specifically, freedom of expression is enshrined in Article 29 of the Constitution and establishes:

> *"The expression of opinion on any subject by word of mouth, private writing, publication in the press, or by any other method of dissemination is entirely free, without prior censorship..."*

Just as it's stated in Article 13 of the American Convention on Human Rights, the right to freedom of expression, as defined inUruguayan legislation, can be exercised through any means and may not be the object of prior censorship. In other words, it allows for free expression to occur first and, if the expression violates the legal framework, only then should appropriate action be taken.

Regarding communications privacy, Article 28 of the Constitution establishes, in an out-of-date fashion, that:

> *"The papers of private individuals, their correspondence, whether epistolary, telegraphic, or of any other nature, are inviolable, and they may never be searched, examined, or intercepted except in conformity with laws which may be enacted for reasons of public interest."*

Thus, communications may only be intercepted when a law authorizes it for public interest reasons.

2.2 International Treaties

Article 12 of the Universal Declaration of Human Rights protects the privacy of communications.[7] This right is also protected by Article 17 of the International Covenant

on Civil and Political Rights[8] and Article 11 of the American Declaration of the Rights and Duties of Man.[9] Uruguay has subscribed and ratified all of these treaties. However, unlike other countries in the region, human rights treaties are not automatically enacted into national legislation. Human rights treaties are only incorporated when they are adopted by the Parliament. The Uruguayan doctrine, however, states that these rights are recognized because of their *iusnaturalist* nature, in other words, they are inherent by virtue of human nature as reflected in Articles 72 and 332 of the Constitution. The national doctrine refers to the "self-enforceability" of the regulations on human rights; that is, the possibility to effectively rely on these rights even when Parliament or the Executive Branch have not regulated them.[10]

2.3 Legal Framework

2.3.1 Surveillance in the Uruguayan Legislation

The Uruguayan courts consider communications surveillance a legal means for obtaining evidence of a crime, if carried out according to the rule of law.[11] It was originally regulated in Article 212 of the Uruguayan Criminal Procedure Code (hereinafter, C.P.P.),[12] and Article 146.2 of the General Procedure Code.[13] Interception of communications can be carried out whenever there are serious reasons to believe that such a measure might provide sufficient evidence for the investigation of a crime. This regulation does not require that the person whose communications are under surveillance be notified after the surveillance measure is complete.

Electronic surveillance is also authorized as a means to investigate certain crimes that the law provides for, according to Article 5 of Law 18.494 on the control and prevention of money laundering and financing of terrorism.

This article indicates:

> *"Article 5º. (Electronic surveillance): In the investigation of any crime, all the available technological means may be used, in order to facilitate their clarification.*
>
> *The implementation of electronic surveillance shall be ordered by the Judge of the investigation upon the request of the Public Ministry. The development and collection of evidence shall be verified by the competent Judge. The competent Judge shall be in charge of selecting the material to be used in the case and the material to be discarded. The latter should have no relation to the evidentiary object.*

> *The result of the evidence shall be transcribed in the certified records in order to be added to the process and the Judge shall be compelled to preserve and protect the electronic forms that contain it, until the sentence has been served. Once the defense of the accused is assigned, the procedural acts shall be made available for their control and analysis, submitting the material to those under investigation for them to recognize voices and images. An exception to this includes the communications between the accused and his or her defense counsel and the communications that have are unrelated to the object of the investigation."*

This provision focuses on five important topics: the object of surveillance, due process, the means provided for, the role of the accused, and the crimes involved:

1. With regard to the *object of surveillance,* the provision makes clear that interception of telephone communications includes text messages, e-mails, satellite phones, video cameras and microphones, and the collection of communication data (metadata), among others.[14]

2. In relation to the *process*, the judge is who, operating under an inquisitorial criminal system,[15] decides what material is considered part of the process and what is not. The legislation explicitly excludes:

> "*...The communications between the accused and his or her defense counsel and the communications that are unrelated to the object of the investigation..."*

Counsel José Luis G. González[16] points out that the intercepted material can only be revealed when a copy of the transcription presented at the hearing is delivered to the defendant. Therefore, the affected individual won't be notified until the hearing takes place.

The judge's criteria when ruling on the discarding of information that is no longer needed for the investigation is unclear. According to Article 24 of Law 18.331, personal data stored for police purposes should be discarded whenever it is not relevant to the investigation that prompted its storage. In the legal process, a competent judicial authority determines the interception and oversees it upon the request of the Public Ministry (Public Prosecutor's Office).

The proceedings that allow surveillance require that: (i) the authorization of *electronic surveillance* be based on a justified decision made by the Judge; (ii) there be a police memo establishing the reasons for the investigation that justify the Prosecutor's request; and (iii) the Prosecutor justify his/her request. In short, this is a justified written decision that cannot be materialized in a judge's oral order.[17]

Upon the request of the Public Ministry (Public Prosecutor's Office), the Investigation Judge orders the implementation of electronic surveillance. The development and collection of evidence must be verified by the competent Judge. The competent Judge is in charge of selecting the material that shall be used in the case and the material that shall be discarded if it is unrelated.

3. Regarding the *means provided for*, the law seems to enable the use of "all available technological means." An extensive interpretation of the law could assure that this provision enables the authorization of several types of surveillance techniques and technologies, like the use of malware.

The Uruguayan legal framework must be interpreted in tandem with international human rights treaties—in particular, the American Convention on Human Rights (Pact of San José). The constitutional requirement for prior judicial authorization should also be applied.

4. Regarding the *role of those being investigated,* it is established that:

> *"...Once the defense of the accused is assigned, the procedural acts shall be made available to the defense for their control and analysis, submitting the material to those under investigation so they can recognize voices and images..."*

5. Regarding the *crimes that are included,* the law indicates that *surveillance* may be conducted "in the investigation of any crime," even minor ones. The implementation of surveillance mechanisms should be limited to a restricted list of serious crimes.[18] While the law refers only to crimes related to money laundering, it has been interpreted extensively to involve other crimes that were not originally provided for in this law. Juan Gómez, a prosecutor specialized in organized crime, assures, while commenting on this law, that "the deliberation with which judges deal with this measure is absolutely necessary in some types of investigations, like the ones linked to drug trafficking."[19]

The Ministry of Interior justifies the implementation of "El Guardián" based upon this broad provision, which, as we explained above, has broad and vague wording that explicitly authorizes the use of "all available technological means" to conduct electronic surveillance. It neglects to take into account the impact that revealing such sensitive information may have on a person's private life.

Uruguayan legislation provides for other circumstances in which electronic surveillance may be acceptable—for example, in cases where a person's rights are suspended (Article 31 of the

Constitution), or for security measures (Article 168, ord. 17). Both measures cause a general restriction of fundamental rights on assumptions of internal disturbance or external threats to the country. On the other hand, there is no provision in Uruguayan legislation that regulates surveillance authorizations in cases of emergency, where human lives may be at risk.

The Uruguayan Criminal Code (hereinafter C.P.) regulates the interception of communications in several articles.[20] In particular, the C.P. makes the interception, destruction or concealment of correspondence, including emails, illegal. This crime is aggravated when the offender is a public official. The C.P. also sanctions the disclosure of information. These regulations establish minimum penalties for those who commit these acts. In general, these penalties are not significant in the context of the Uruguayan Criminal Code. Occasionally, local courts have prosecuted individuals for these crimes.[21]

2.3.2 Computer-related Crimes

There is no specific legislation on "computer crimes" in Uruguay. Instead, we resort to referencing current criminal legislation. During the last parliamentary term, the Agency for E-Government and the Information and Knowledge Society (*AGESIC, in Spanish*) presented a bill on this issue. At present, policy-makers are reviewing this bill, which is facing categorical rejection by civil society.[22]

This bill includes a series of various crimes (acts) that are too broad. It contains a provision that would criminalize so-called "reverse engineering," meaning it would prohibit modifications of computer equipment made by users. While at first glance these computer crimes do not seem to be related to the surveillance agenda, the fact that users are not allowed to modify their equipment has strong implications for security protection measures.

2.3.3 Data Retention versus Data Protection

Article 35 of Law 18.331 establishes the Personal Data and Habeas Data Regulatory Unit (*URCDP, in Spanish*). The URCDP may apply sanctions to those responsible for databases whenever there is a violation of Uruguayan data protection law.

The Agency for E-Government and the Information and Knowledge Society (*AGESIC, in Spanish*)[23] considers that its necessary to ensure transparency and accountability. In particular, it references the protection of personal data established in Chapter V of Law 18.331[24] that regulates the processing of personal data for national defense or public security purposes:

> *"The processing of personal data with national defense or public security purposes by the armed forces, police or intelligence agencies, without the*

prior consent of its owners, is limited to those cases and data categories that are strictly necessary to accomplish the legally assigned missions of national defense, public security or the prevention of crimes. Databases, in these cases, shall be specific and established for those purposes, and must be classified into categories, according to their degree of reliability."[25]

On the other hand, Article 3 of this law excludes databases for public security, State defense, State security, and State's activities regarding crime and prosecution of crime.

Regarding ISPs and telecommunications companies' obligation to retain communications data for a certain period of time, Article 75 of Law 19.149 compels mobile telephone service companies to keep current records about the clients that have purchased their services in any of its forms. Databases are protected by Law 18.331 on the protection of personal data.

2.3.4 Communications Surveillance in Intelligence Activities

In Uruguay, there is a bill that aims to regulate the National Intelligence System. One of the bill's articles stands out for its rights-based nature:

"Article 14.- Every information search operation conducted by an agency belonging to the State Intelligence System involving special procedures that may affect the freedom and privacy of individuals must be authorized by the Judicial Branch. To this effect, the Supreme Court of Justice shall assign the competent judicial body that shall be in charge of these matters. All proceedings must be confidential."

At the same time, Article 15 provides a series of principles that must be followed by those who conduct these proceedings:

"Article 15.- During the collection and processing of information, the agencies that make up the State Intelligence System must adapt their actions to the following principles:

- *Legitimacy: they should act in full compliance with the law according to the agency's subordination and responsibilities;*
- *Efficiency: there should be an adequate relation between the available measures and the quality and appropriateness of the product obtained;*
- *Financing: origin and appropriate application of the monetary resources assigned to the services, including those which are confidential;*
- *Legality: strict compliance with the Constitution and the law when conducting the proceedings that, inescapably, require activities that invade*

individuals' privacy;

- *Necessity and dissemination: the information needed to properly and effectively conduct the functions in each of the areas mentioned above shall be required and safeguarded for those purposes;*
- *The information may not be used for the benefit of a particular person, private organization or political party whatsoever."*

However, in other sections, the bill imposes restrictions on the right to access public information.

Update: Uruguay set up a Response Unit for Security Incidents in the Ministry of Defense. The capabilities of this center are unknown to the public.

III.

Relevant Surveillance Cases

Unlike other countries, the Uruguayan Judicial Branch does not usually incorporate the judgments of the Inter-American Court of Human Rights into its own judgments. This means that even though there are international relevant cases, they are not used by the Judicial Branch.

The Uruguayan Supreme Court has ruled on the legality of communications surveillance.[26] In this case, the defendant filed a constitutional complaint[27] against Article 212 of the Criminal Procedure Code and Article 161 of the Criminal Code. He argued that these provisions do not establish the guarantees needed to protect the right to freedom of expression and due process protected by the Constitution.

The Supreme Court rejected the complaint alleging unconstitutionality on the following basis:

- The defendant did not duly justify which was the direct and personal interest presumably harmed, nor did he reference the concrete case—both of which are indispensable factors needed to file an unconstitutionality complaint;
- Article 212 of the C.P.P. does not violate Article 7 of the Constitution, nor does it leave the rights mentioned therein unprotected. Article 212 indicated that the interception of correspondence and other communications is only conducted in the cases of public interest, specifically to verify that a crime has been committed and the interception is subjected to a prior legal authorization;
- With regard to Article 161 of the C.P., the Court assured that it does not violate the principle of legality, given that it sets forth the acts classified in it and the sanctions that are imposed for their execution;
- Finally, on the topic of wiretaps, the Supreme Court suggested that the defendant should have filed the complaint in the pre-investigation stage, which made the complaint untimely.

Consequently, the highest domestic court considers that communications interception is consistent with the Constitution. Similarly, the Court of Appeals[28] indicates that those who, in principle, are not subjected to a criminal process may be the subjects of surveillance in certain procedures.

Another relevant case is Sentence 377/2013 of the Court of Appeals in Criminal Matters, Court 2.[29] This case solves an appeal lodged by the defendant against a sentence declaring the accused as the perpetrator of a crime related to illicit drug trafficking, association, and financing. This crime was committed in tandem with the offense of introducing and transporting drugs.[30] This was considered as an aggravating factor, because it was committed through the participation of an illicit organization or an organized criminal group.

The sentence confirms the appropriateness of the interception of telephone conversations in order to verify the commission of the crime. One section of the sentence explains the procedure that was followed in order to get the surveillance authorization:

- First, the Prosecutor considered that, pursuant to Article 20 of the United Nations Convention (also known as the Palermo Convention), which was ratified by Law 17.861 in Uruguay, and according to Article 212 of the Criminal Procedure Code and Article 5 of Law 18.494, it was appropriate to conduct electronic surveillance on the accused.
- Second, the trial judge ordered that electronic surveillance is reserved as is stated in the legal proceedings. In this way, the means of proof of the defendant and of the other individuals involved in the case, is not invalidated for a time period of 60 days.
- Third, the proportionality and necessity of wiretaps were considered by taking into account that there were no other effective means of collecting evidence. In order to reaffirm the analysis of these principles, it is necessary to quote the following portion of the sentence: "*The judge must assess its proportionality in order to breach the general rule and implement the measure in case extreme situations take place: more than two tons of cocaine were seized, thus, this principle is not only applicable to this justified electronic surveillance but also to any other measures that are not prohibited. This principle was born in the nineteenth century in continental Europe as a way to prevent police abuses; it was established in the twentieth century and it persists until today.*"
- Finally, the sentence clarifies that none of the non-entities invoked in relation to the wiretaps as evidence were proved. The Supreme Court is referred to, since it drew up Article 212 of the C.P.P., which authorizes the interception of communications held by third parties whenever there is a justified reason to suspect that they have participated in a crime.

3.1 El Guardián

"El Guardián" is an electronic surveillance system distributed by the Brazilian company, Digitro Tecnología Ltda. It allows 30 people to simultaneously access the location and traffic data of 800 cellphones and 200 fixed telephones in real time. It also allows for the

creation of 100 mirror accounts of e-mail subscriptions and the monitoring of public information on three social networks.[31] El Guardián was secretly purchased by the Ministry of Interior (*Ministerio del Interior*).[32] According to initial reports, "El Guardián" is an exclusive software that costs two-million dollars and whose maintenance cost is $200,000 USD per year.

"El Guardián" has three basic actors that must necessarily participate in its implementation: the Ministry of Interior, the Judicial Branch, and telecommunications companies. Since the government purchased this program secretly, no specific regulations have been established as to how "El Guardián" is implemented.

According to some press reports, the Ministry of Economy issued a reserved (not public) decree that establishes a need for Uruguay to acquire surveillance technology.[33] The decree, issued on March 28, 2014, would give tax exemptions to telecommunications companies that acquired new high-tech equipment requested by the Ministry of Interior. Thus, for the tax incentive, telecommunications companies indeed went onto purchase equipment that was requested by this Ministry.

Another decree, drafted by the Ministry of Interior and obtained by the newspaper, *El Observador*, would establish:[34]

- A protocol between the Ministry of Interior and telecommunications companies for them to know how to respond to electronic surveillance order requests from a judge. The document is clear that telecommunications companies are obliged to follow the procedures which involves connecting their computers to "El Guardián."
- That companies or communications service providers would be reimbursed for the cost of the interceptions;
- Specific data management and preservation requirements;
- Who (authorized staff) has access to the system;
- That companies are compelled to deliver geolocation information of the origin and destination of communications.

During an appearance before Parliament—which was prompted by a summoning from the opposition[35]—the Minister of Interior also supported the purchase of "El Guardián." He indicated that before "El Guardián" was purchased, there were at least 22 interception systems operating in the country with no oversight whatsoever. According to the Minister of Interior, "El Guardián" was a way to centralize the surveillance processes and ensure it was conducted in a legal, controlled manner.

He also noted that "El Guardián" can monitor subjects on "open" social networks, but it

does not interfere with users' activities. Authorities of the Ministry of the Interior assured that they would keep all collected data in a state-of-the-art data-center. The Ministry of Interior also told legislators that there would be white lists—that is, people who would not be subjected to this surveillance tool—that would include legislators themselves.

Uruguayan civil society questioned the policy of confidentiality in relation to the purchase and the protocols that regulate "El Guardián's" implementation.[36] Also, even when authorities pointed out that there should be prior judicial authorization and that, according to Law 18.494, this technology is a legal instrument of evidence, civil society criticized the lack of a regulatory framework that would guarantee respect for human rights and democratic values. The Supreme Court of Justice granted the go-ahead for this system through a memo of understanding with the Ministry of Interior.[37] In theory, the Ministry and the Court have established a secret protocol for its' implementation.

As part of this investigation, we requested the court give us a signed copy of the cooperation agreement, which it did. The agreement, however, did not establish a specific protocol of cooperation of how "El Guardián" shall be implemented. Its' content solely indicated the existence of a framework agreement—a general document that provided vague ideas as to how "El Guardián" would be overseen by the Judicial Branch.

This revelation prompted the executive director of the Center of Archive and Access to Public Information (*CAINFO, in Spanish*) to submit a request to access public information regarding the secret purchase of "El Guardián."[38] The Ministry of Interior, who purchased the software, did not answer the request. Thus, CAINFO sought justice by activating the legal mechanisms pursuant to the law of access to public information.

Their request was first denied by the Administrative Court Nº 1. It was then also rejected by the Court of Appeals on Civil matters Nº 5, making the Administrative Court's decision final. That is, the courts defended the thought that "the public dissemination of the system's strengths and weaknesses could foil its implementation during activities."[39]

The key arguments in the lawsuit for dissemination were based on the broad protection of the right to access public information and the principle of divisibility of public information. In particular, the applicant said:

> *"In the examination of the legal framework presented, the conclusion reached is that the requested information must be available to the public. Under no circumstances can we accept a generic classification of all the information in relation to 'El Guardián' that impedes none other than the public scrutiny of telecommunications surveillance systems implemented by the State. This would be a blatant violation of the human rights to*

> *information and civic participation and it would imply a disregard for all the standards and guarantees related to the classification of public information."*

However, the Court of Appeals on Civil Matters Nº 5 argued that the "plaintiff was wrong about the strategy used, since in the administrative stage and in the lawsuit, the plaintiff intended to gain access to information that was clearly protected by secrecy." The court added that "the right to access information is not absolute nor unrestricted, since the protection of other constitutional rights determines the possible existence of legal exceptions to the obligation to provide information."

In that regard, the Court emphasized that:

> *"It seems obvious that the secrecy of the purchase of the operating system 'El Guardián,' which was endorsed by the Court of Auditors, lies not only in the purchase itself (which was incidentally disclosed) but also in its technical characteristics, for security reasons and for the protection of individuals through the prevention and suppression of crimes, by implementing systems similar to the one purchased. This instrument aims at combating crime, and the public dissemination of its strengths and weaknesses may foil its implementation, leaving it to hackers and/or individuals who illegally try to obstruct or impede investigations or suppressions subjected to legal control, as presented by the defendant, with the support of specific legal and administrative legislation..."*

The civil society organization DATA filed an *amicus curiae* which was later rejected by the court. In its arguments, DATA explained:

- The secrecy of the administrative law that regulates the implementation of "El Guardián" is extremely troubling. In fact, to simply learn about an administrative protocol that should be public by default, it should not be required to turn to a law of access to information. The State should not implement a measure that interferes with the right to privacy if there is no publicly-available legislation surrounding it.[40]
- It is essential to have access to the regulations on the implementation of "El Guardián" and of any other surveillance system. This is necessary in order to know the guarantees that the Ministry of Interior, which has a prominent role in the new system, has provided for in relation to the collection, systematization, processing, protection, and destruction of data, which shall be obtained through the interception of phone calls and e-mails.
- The purchase of "El Guardián" exponentially increases the surveillance capabilities

> of the State. International experience indicates that this type of technological platform poses a high risk to privacy and may pave the way for potential abuses of power.

Today, thanks to the press and the Ministry's admittance, we know that there is a protocol that was originally kept secret from the public. However, little is still known about its nature and structure. Such a notion must be rejected by a State under the rule of law.

With such secrecy, how can we solve the potential problems that will arise from implementing such surveillance that may infringe upon human rights? Who will be in charge of overseeing administrative officials who operate this system and what procedures will they follow in order to hold them accountable? Are bodies also going to be secretly created by administrative decisions? All of these are queries that the Ministry of Interior should answer, apart from establishing the jurisdictional control of "El Guardián."

Such secrecy and uncertainties are not welcomed in democracies. In Uruguay, the important principle that allows for the publishing of legal regulations is violated. This creates a dire situation since the administration can only act as the law allows, and the only guarantee for the citizenry is the control of the regulations, which cannot be carried out if the content of the law is unknown.

3.2 Hacking Team

In July 2015, emails of the Italian company, "Hacking Team," were leaked revealing that Uruguayan authorities, along with a Paraguay businessman as mediator, met with Hacking Team.[41] Hacking Team sells invasive surveillance technology that is used to harm computer users. It works in many different ways including, but not limited to, disrupting computer operation, gathering sensitive information, impersonating a user to send spam or fake messages, or gaining access to private computer systems.[42]

IV.

International Principles on the Application of Human Rights to Communications Surveillance

This section analyzes Uruguayan regulations and practices vis-à-vis the International Principles on the Application of Human Rights to Communications Surveillance.

Principle 1: Legality

> *Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.*[43]

Uruguay, in general, complies with the Legality Principle since communications interceptions and electronic surveillance are established in Uruguayan law, analyzed above in this report.

However, the aforementioned laws are too vague and broad in scope when considering surveillance tools such as "El Guardián." The legislation neglects to establish specific procedures that authorize the use of invasive surveillance technology—such as malware—that is used to infiltrate electronic devices like cellphones or computers. Such surveillance practices are much more intrusive than the mere interception of communications, and should require a higher level of privacy protection.

Moreover, it is not clear how these technologies operate at an administrative level. The problem is exacerbated due to the lack of in-depth discussions on the legality of secret laws (such as the aforementioned secret decree of the Ministry of Economy).

Finally, the guidelines or agreements that regulate the State's ability to access the data collected by telecommunications operators are not publicly available. The secretive nature of the law violates the Legality Principle.

Principle 2: Legitimate Aim

> *Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.*
>
> *Any measure must not be applied in a manner that discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*[44]

On the basis of the analysis of the current laws, we conclude that the measures for the prevention and detection of crime correspond to a legitimate aim.

Uruguayan regulations establish that, in principle, it is the Ministry of Interior, the Public Ministry, and the Competent Judge who are able to carry out surveillance. However, there are other government agencies, not covered by law, that are capable of doing so as well. Consequently, these agencies have the ability to carry out surveillance that may not correspond to a legitimate aim–it is particularly worrisome when intelligence activities are not regulated.[45]

Principle 3: Necessity

> *Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim.*
>
> *Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.*[46]

It is impossible to thoroughly analyze compliance with this principle, since the protocols or guidelines of the actions taken by the Ministry of Interior in surveillance cases are unknown. The current practice indicates that, according to the Ministry of Interior, there are at least 22 wiretap systems operating simultaneously in Uruguay, but the Ministry has not yet justified the need for them.[47]

Principle 4: Adequacy

> *Any instance of communications surveillance authorized by law must be appropriate to fulfill the specific legitimate aim identified.*[48]

In order to determine whether telecommunications surveillance is adequate and

appropriate to achieve the corresponding legitimate aim, we should analyze each case individually. In any case, it is known that, currently, telecommunications surveillance is being used more frequently as key evidence in criminal investigations related to drug trafficking and corruption.

In an *El País* interview with Juan Gómez, a prosecutor specializing in organized crime, claimed that he did not notice an "exaggerated tendency in the implementation" of telephone interceptions.[49]

Gómez stated, *"The interception is ordered after a previous study and in the cases in which there are signs that determine that the person has been involved in an illicit activity."* On this topic, Counsel Fagúndez asserted that it is "very common" for the police to intercept telephones, and whenever the information obtained is of interest, [the police] requests judicial authorization."[50]

Principle 5: Proportionality[51]

> *Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society.*
>
> *Decisions about communications surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.*

System operators state that they "assess the necessity and rationality" of implementing surveillance measures, since it is a mechanism that invades individuals' privacy.[52] However, there are no additional criteria applied to national legislation that would assess the proportionality of a surveillance measure.

Upon examining the current regulatory framework, it appears that in order for a measure to be proportionate, the following requirements must be met: (i) the investigation must be related to a crime, (ii) there should be serious reasons to believe that the measure could guarantee sufficient evidence to verify the commission of a crime, and (iii) the measure must be requested by the Public Ministry to the Judge of the investigation.

Principle 6: Competent Judicial Authority

> *Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.*[53]

The Public Ministry (the prosecutor) requests authorization from the Judicial Branch to conduct surveillance. The Judicial Branch is in charge of authorizing that request. The

Ministry of Interior (the Uruguayan National Police) and the Judicial Branch have recently come to an agreement regarding the operation of "El Guardián," although the technology has not been implemented yet.

Assessment of the capabilities and resources of the Judicial Branch requires further analysis, which is outside the scope of this report.

Principle 7: Due Process

> *Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.*[54]

The legal framework that regulates surveillance in Uruguay is insufficient. In particular, the guidelines or agreements that regulate the State's access to data collected by telephone or Internet operators are not available to the public, which conflicts with both the Principle of Due Process and the Principle of Legality.

Principle 8: User Notification

> *Those whose communications are being surveilled should be notified of a decision authorizing communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstance:*
>
> *Notification would seriously jeopardize the purpose for which the communications surveillance is authorized, or there is an imminent risk of danger to human life; and the authorization to delay notification is granted by a Competent Judicial Authority; and the user affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.*
>
> *The obligation to give notice rests with the State, but communications*

> *service providers should be free to notify individuals of the communications surveillance, voluntarily or upon request.*[55]

This obligation is not included in Uruguay's national legislation. However, it does include a deferred notification in which the intercepted material is shared with the accused so they are able to exercise their right of defense during the hearing.

Principle 9: Transparency

> *States should be transparent about the use and scope of communications surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for communications surveillance, adhere to those procedures, and publish records of State requests for communications surveillance.*[56]

Even though the Personal Data Regulatory Unit[57] maintains that the appropriate measures to ensure transparency and accountability were taken when conducting surveillance, these measures do not keep up with the advances of surveillance techniques and technologies.

Upon the request of a senator, the Supreme Court revealed that between January 2009 and March 2014, the judges who were competent in criminal matters ordered a total of 6,150 wiretaps,[58] which averages to three wiretaps per day. During this same time period, the two law enforcement agencies that ordered the most interceptions both specialized in organized crime, while 2,192 interceptions were authorized by a judge.

Consequently, to date, there is incomplete data on the implementation of surveillance measures. There is no proactive publication of this information nor is there a standard to publish it.

Principle 10: Public Oversight

> *States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.*[59]

In Uruguay, there are a series of laws that could function as mechanisms that oversee telecommunications surveillance:

- Law 18.331, which establishes the protection of personal data and the petition of habeas data.
- Law 18.381, which protects the right to access public information and guarantees transparency in the State's public management.

However, the functions of these two mechanisms, in practice, is complex. Nonetheless, there are parliamentary commissions that partially monitor these matters in the Senate.

Principle 11: Integrity of Communications and Systems

> *In order to ensure the integrity, security, and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State communications surveillance purposes.*
>
> *A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users.*[60]

Article 20 of Law 18.331 establishes that operators that exploit public networks or that provide electronic communications services must guarantee the protection of personal data. In Uruguay, there is no specific law regulating mandatory data retention by telephone or Internet service providers for a certain period of time, but several of them conduct data retention voluntarily.

Principle 12: Safeguards for International Cooperation

> *In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from foreign service providers and States. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use*

> *mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.*[61]

Uruguay has signed and ratified the Inter-American Convention on Mutual Assistance in Criminal Matters (MLAT).[62] Article 2 of the Convention is the only provision of the treaty that is applicable to surveillance matters.

This article stipulates that "The state's parties shall render to one another mutual assistance in investigations, prosecutions, and proceedings that pertain to crimes over which the requesting state has jurisdiction at the time the assistance is requested (...) This convention applies solely to the provision of mutual assistance among states parties. Its provisions shall not create any right on the part of any private person to obtain or exclude any evidence or to impede execution of any request for assistance."

In relation to Uruguay's current commitments of international cooperation regarding data protection, we found:

- Agreements on cooperation in matters of personal data protection with several countries;
- Uruguay is a member of the Ibero-American Data Protection Network and of the Organizing Committee of the International Conference of Data Protection;
- Uruguay signed the Convention 108 before the European Council for the protection of individuals in relation to the automatized processing of personal data and its additional protocol for the supervisory authorities and the cross-border data flow.
- Uruguay has adapted to the standards set by the European Union in accordance with "Directive 95/46/CE," which means that it complies with the standards of data protection established by the European Union. However, this agreement is limited to the protection and transmission of personal data between Europe and Uruguay.

Principle 13: 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. Laws should*

> *stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence or otherwise not considered in any proceeding, as is any evidence derivative of such information.*
>
> *States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must not be retained, but instead be destroyed or returned to those affected.*[63]

All illegal communications interceptions are considered crimes in accordance with the Uruguayan Criminal Code. There is no legal provision for the protection of whistleblowers.

V.

Conclusion

This report has analyzed the current framework for communications surveillance in Uruguay. What follows is a series of conclusions and recommendations in order to move the debate, vis-à-vis the aforementioned Principles, forward.

5.1 New Regulations

- New technological developments in Uruguay need new regulations with regards to communications surveillance and human rights. The aim is to limit the State's surveillance capabilities and their access to individuals' data through telecommunications companies or third-party companies.
- Both "El Guardián" and the arrangements for the purchase of invasive technology (malware) show the government's tendency to buy and use modern technologies with the purpose of increasing the State's scope and capability to conduct surveillance on the population.
- The current regulations are not robust enough to clearly set limits for this activity. Consequently, our fundamental freedoms such as privacy, freedom of expression, and association are at risk.
- To this day, there have been no cases whatsoever in which the Uruguayan government used surveillance tools for political purposes or on specific groups of the population.
- Uruguay needs to reform its policies to guarantee the right to communicate without illegal and disproportionate interception by intelligence and security agencies. The Principles analyzed in this report may work as a guideline. The idea of protecting the integrity of communications is not new, as it has been present in the Uruguayan Constitution since 1830. However, the government's technical capabilities have expanded since, with the use of systems that facilitate surveillance on a large scale.
- Uruguay possesses a framework for a strong and general protection of human rights. Nonetheless, this framework is too broad to cover the new situations these emerging and rapidly changing technologies create.
- Uruguay's legal framework is unclear on the following issues: the objective criteria in order to conduct surveillance on an individual or a group of individuals; the objective criteria that determines the duration of a surveillance procedure and the

restricted rights of those subjected to surveillance; the rules that the State should follow in order to have access to the data stored by telephone and Internet service providers.

5.2 Necessity and Legitimate Aim

- The evidence found during this investigation shows that local authorities are extremely worried about the struggle against organized crime, and that the purchase of these tools is an outcome of this situation. However, the State has not justified the need for these tools.
- Neither has it justified the existence of 22 uncontrolled surveillance systems, apart from "El Guardián," which were presumably implemented by agencies to intercept public communications. This is worrying and calls for immediate action.
- The current framework, as we understand it, works in relation to a certain type of crime, despite the fact that the authorities argue that it enables surveillance for criminal offenses in general. The best way to proceed would be to determine a more comprehensive and consistent framework for this sensitive activity.

5.3 User Notification

- Uruguay should establish rules for the State to notify the user when the investigation is no longer at risk.

5.4 Judicial Authorization, Transparency, and Illegitimate Access

- The Uruguayan legal framework allows surveillance to be authorized through the Judicial Branch upon the request of a prosecutor. However, the current legal framework does not provide a means for overseeing how many people are subjected to surveillance, and what the conditions and reasons for it are. Even though it is possible to argue that there is constitutional protection for this right, the legal protections should be more specific.
- It is also difficult to know how the information obtained by surveillance is discarded, or how the people that have been exposed to surveillance by mistake are dealt with. This is a further aggravation, since, in principle, the regulations on the protection of personal data do not apply to databases in matters of defense and national security.
- Clear sanctions for those who use these technologies unlawfully should also be established. The current regulation of the Criminal Code is insufficient.

5.5 Due Process

- Authorities have not explained a way to proceed with nor the procedural protocol required for “El Guardián.” On the basis of the available evidence and separate lawsuits, we discoveredthat, in Uruguay, there is a secret administrative law. This is some sort of "secret regulatory framework," similar to the ones in the United States of America or Great Britain, and is not compatible with a constitutional State.
- Consequently, mechanisms, including publicizing the regulations under which they operate, must be created to oversee the implementation of such tools. Furthermore, knowing the technical details of the way in which they work may also be important, however such knowledge might foil the essential purpose of the tool. No one has requested information on this yet.

5.6 Transparency

- There is no periodic and aggregate information about the surveillance requests—from the requests for communications interception, to the requests related to the access to data stored by third parties—that are authorized and rejected. Although authorities have reported to Parliament on wiretaps, and responded to some specific requests on this subject, they do not regularly and systematically report on these activities.
- It is necessary to provide transparency for the Ministry of Interior and to pro-actively publish aggregate information of surveillance requests. Also, the legislative branch should be able to oversee the matter. Civil society should also play a role and be able to use the information to evaluate the fluctuation of surveillance powers over a certain period of time, and for which crimes. Publishing this information will probably prompt a more extensive and transparent debate on this topic. It will pave the way for a dialogue between authorities and Uruguayan civil society.

5.7 Transparency in Purchase Procedures

- More transparency is needed surrounding the purchasing of surveillance tools, since Parliament needs to exercise adequate control over them. The discussion on how to proceed can be guided by the 13 Principles analyzed in this report.
- Apart from the legal aspects, there are some factors linked to the capabilities of the State, and in particular to security agencies, when examining the technology that they want to purchase. The current solutions provided by the State are not related to free software or open-source software, which impedes their audit in case there are back doors.

5.8 Voluntary Data Retention

- Even though Uruguayan law does not compel service providers to conduct mandatory data retention, we know little about the *voluntary* retention these service providers carry out, or their compliance (or non-compliance) with the regulations on data protection.
- The legal requests submitted to telecommunications operators about text messages and geolocation of cellphones suggest that Uruguayan telecommunications operators retain their clients' information, but the duration and the type of data retained are unknown.

5.9 Encryption

- In Uruguay, encryption is not prohibited, and there are no regulations compelling encryption service providers to put back doors in their products. Human rights standards protect the use of encryption as a mechanism to exercise the right to freedom of expression and the right to privacy.

5.10 Intelligence Services

- Uruguayan legislation is incomplete when it comes to surveillance conducted by intelligence agencies. The bill related to this topic that was rejected, may have provided better guidelines for these agencies.

VI.

Bibliography

Cortizas, G: El Guardián: Super Spy Software Launched by the Government EL v. March 25, 2015. Available at: http://www.elpais.com.uy/informacion/guardian-gobierno-pone-marcha-super.html [Accessed on September 18, 2015].

Corujo Guardia, William, Acerca de las escuchas telefónicas como medios de prueba y el derecho constitucional a la intimidad. [On Wiretaps as Evidence and the Constitutional Right to Privacy]. Online: UY/DOC/250/2012

Joint Declaration on Surveillance, Security and Privacy: Uruguay Urged to Adopt Standards on Human Rights, 2014. Available at: https://eff.org/r.1dss [Accessed on September 6, 2015]

De los Santos, F., (2015). Who Surveils those who Conduct Surveillance? La Diaria. Available at: http://ladiaria.com.uy/articulo/2015/3/quien-vigila-a-los-vigilantes/ [Accessed on September 18, 2015].

Newspaper El Observador (2015). As of January, El Guardián is going to spy on e-mails and cellphones. Available at: http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757. [Accessed on September 29, 2015]

Newspaper EL PAÍS Uruguay. Regional Government Strengthen and Expand their Spying Capabilities (2015). Noticias Uruguay y El Mundo actualizadas - Newspaper EL PAIS Uruguay. Available at: http://www.elpais.com.uy/informacion/gobiernos-region-potencian-capacidad-espiar.html [Accessed on September 17, 2015].

Newspaper EL PAÍS Uruguay (2015). Bonomi: "El Guardián" provides more guarantees than the current system. Noticias Uruguay y el Mundo actualizadas, Newspaper EL PAIS Uruguay, 2015. Available at: http://www.elpais.com.uy/informacion/bonomi-guardian-garantias-sistema-actual.html. [Accessed on August 19, 2015].

Newspaper EL PAÍS Uruguay. Controversy around Wiretaps. Criminal attorneys Warn about Wiretaps without Judicial Authorization and Recording of Dialogs between the Accused and their Counsels, Newspaper EL PAÍS Uruguay, November 4, 2012.

EFF, ARTICLE19. Background and Supporting International Legal Analysis, 2014. Available at: https://es.necessaryandproportionate.org/analisislegal [Accessed on September 16, 2015], Access, Universal Implementation Guide, 2015. Available at: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf [Accessed on September 16, 2015].

Gomes, Santoro, Fernando. Prueba Ilícita y Prueba Irregular. [Illegal Evidence and Irregular Evidence] Admisibilidad de Grabación de Voz y/o Imagen Sin Autorización. [Admissibility of Unauthorized Recording of Voice and/or Image] Review on the sentence of the Court in Administrative Matters N° 591/2011 of August 16, 2011, Case of Francisco Casal C/ DGI. Published in: LJU volume 149. online: UY/DOC/38/2014)

González, José Luis. Control and Prevention of Money Laundering and Financing of Terrorism. Law N° 18.494, 2010. At: Magazine of Law School, 29, 137-159. Available at: http://www.fder.edu.uy/contenido/penal/pdf/2010/gonzalez.pdf [Accessed on August 1, 2015].

Gros Espiell, Héctor. La Constitución y los Tratados Internacionales, Revista del Colegio de Abogados del Uruguay Volumen II, Montevideo, 2da edición. [The Constitution and International Treaties, Magazine of the Uruguayan Lawyers Association, Vol. II, Montevideo, 2nd edition].

Kutz, Christopher. The Repugnance of Secret Law. Available at: https://www.law.upenn.edu/live/files/2398-kutz-the-repugnance-of-secret-law-full [Accessed on March 15, 2015].

La Rue, Frank. 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, page 3.

McMullan,Thomas (2015). The World's First Hack: the Telegraph and the Invention of Privacy. The Guardian. Available at: https://eff.org/r.xuol [Accessed on August 1, 2015].

Melendrez, P., 2014. Wiretaps are Implemented "Sensibly", Judges Claim. Newspaper EL PAIS, April 26, 2014. Available at: http://www.elpais.com.uy/informacion/jueces-disponen-escuchas-telefonicas-prudentemente.html [Accessed on April 30, 2015].

International Principles on the Application of Human Rights to Communications Surveillance (2014). Available at: https://es.necessaryandproportionate.org/text [Accessed on September 6, 2015].

Uruguayan Judicial Branch. Civil Court 5º Rejects Appeal on "El Guardián" and Notes Strategic Error by the Applicant, 2015. Available at: https://eff.org/r.qayy [Accessed on March 15, 2015].

Supreme Court of Justice, Sentence 58/2009. Available at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37359

Court of Appeals in Criminal Matters 2º, Sentence 377/2013. Available at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37314 Court of Appeals 2º, Sentence 80/2006. Available at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37359

Terra, Gonzalo (2013). The Government Purchased "El Guardián" to Spy on Calls and E-mails. Newspaper El País. Available at: https://eff.org/r.5fvk [Accessed on September 16, 2015].

Personal Data Control Regulatory Unit of the Eastern Republic of Uruguay, 2014. The Right to Privacy in the Digital Age: A/RES/68/167. Available at: http://www.ohchr.org/Documents/Issues/Privacy/Uruguay.pdf [Accessed on September 16, 2015].

1 Terra, Gonzalo (2013). *The Government Purchased "El Guardián" [The Guardian] to Spy on Calls and E-mails.* El País. Available at: https://eff.org/r.5fvk [Accessed on September 16, 2015].

2 *Joint Declaration on Surveillance, Security and Privacy: Uruguay Urged to Adopt Standards on Human Rights* (2014). Available at: https://eff.org/r.1dss [Accessed on September 6, 2015].

3 McMullan, Thomas (2015). The World's First Hack: the Telegraph and the Invention of Privacy. The Guardian. Available at: https://eff.org/r.xuol [Accessed on August 1, 2015].

4 *International Principles on the Application of Human Rights to Communications Surveillance,* 2014. Available at: https://es.necessaryandproportionate.org/text [Accessed on September 16, 2015], EFF, ARTICLE19. *Background and Supporting International Legal Analysis*, 2014. Available at: https://es.necessaryandproportionate.org/analisislegal [Accessed on September 16, 2015], Access, *Universal Implementation Guide,* 2015. Available at: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf [Accessed on September 16, 2015].

5 *International Principles on the Application of Human Rights to Communications Surveillance* (2014). Available at: https://es.necessaryandproportionate.org/text [Accessed on September 6, 2015]; See also, La Rue Frank, 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, p. 3.

6 Ibid., La Rue, p. 4.

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

8 Article 17: 1. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

9 Article 11 Protection of Honor and Dignity: 1. Everyone has the right to the respect of their honor and dignity; 2. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation; 3. Everyone has the right to the protection of the law against such interference or attacks.

10 Gros Espiell, Héctor. *The Constitution and International Treaties*, Magazine of the Uruguayan Lawyers Association, Vol. II, Montevideo, 2nd edition.

11 However, there is an area of the national doctrine that seems to accept evidence even when it has been originally obtained through illicit means. For instance, if the interception of a communication was conducted without judicial authorization by a private actor, the legality of the evidence would be questionable, and the court should evaluate whether it is acceptable or not. Consequently, electronic surveillance may, as a general rule, be used as an evidentiary means in a judicial court as long as the evidence is obtained in accordance with the national legislation.

12 A new Criminal Procedure Code will enter into force in 2017.

13 Article 146: 146.1) Documents, statements made by the parties, or by the wtinesses, expert's opinions, judicial reviews, and reenactments of the facts can be used as evidence. 146.2) Other evidentiary means not prohibited by law can be used; the same disciplinary regulations as those applied to the means provided for by law should be applied to them.

14 González, José Luis, *op. cit.*, p. 148.

15 Uruguay is one of the few Latin American countries that maintains a criminal procedure system based on an inquisitorial principle, unlike schemes that are more right-based, which rely on accusatory principle. Taking this into account, it is necessary to explain that the Uruguayan criminal procedure system is mixed: in the first stages (pre-investigation and investigation) it is inquisitorial; and in the last stages, (extension of the investigation and plenary) it is accusatory. The remaining characteristics of the inquisitive system are: written process, which is discontinuous and decentralized. The Investigating judge shall be the one to pass sentence. Refer to González and Patrón on this topic. *Manual Básico del Proceso Penal* (2010) [Basic manual of Criminal Procedure]. It is important to mention that Uruguay has already passed a new system based on the accusatory principle of the criminal process —which demands a correlation between the accusation and the sentence— although it has not been implemented yet. Available at: http://www.fder.edu.uy/material/gonzalez-maria-prato-magdalena_manual-basico-proceso-penal.pdf. [Accessed on September 20, 2015].

16 González, José Luis, *op. cit.*, p. 148.

17 Corujo Guardia, William, *On the Wiretaps as Evidence and the Constitutional Right to Privacy*. Online: UY/DOC/250/2012. Verbal orders are an accepted practice in the Uruguayan Judicial Branch for administrative acts within it.

18 Article 8.- Crimes classified in articles 54 - 57 of the Decree-Law Nº 14.294, of October 31, 1974. Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=14294&Anchor=, they shall be also classified when their material objects are goods, products or instruments coming from crimes classified by our legislation, linked to the following activities:

- Crimes of genocide, war crimes, crimes against humanity, as established by Law Nº 18.026, September 25, 2006. Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18026&Anchor [Accessed on September 16, 2015];
- Terrorism; financing of terrorism, contraband of more than US$20.000; illicit trafficking of arms, explosives, ammunition, or material destined to their manufacturing; illicit trafficking of organs, human tissues and medicines; human trafficking; extortion; abduction; proxenetism; illicit trafficking of nuclear substances; illicit trafficking of works of art, animals or toxic materials; fraud; embezzlement; crimes against Civil Service, included in Title IV of volume II of the Criminal Code and the ones established in Law Nº 17.060, of December 23, 1998 (crimes of public corruption). Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17060&Anchor [Accessed on September 16, 2015];
- Fraudulent bankruptcy; fraudulent insolvency; the crime provided for in Article 5 of law Nº 14.095, of November 17, 1972 (societal fraudulent insolvency). Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=14095&Anchor=#art5%C2%BA [Accessed on September 16, 2015];
- Crimes provided for in Law Nº 17.011, of September 25, 1998 and its amendments (trademark crimes) http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17011&Anchor [Accessed on September 16, 2015];
- Crimes provided for in Law Nº 17.616, of January 10, 2003 and its amendments (intellectual property crimes). Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17616&Anchor [Accessed on September 16, 2015];
- Crimes provided for in Law Nº 17.815, of September 6, 2004. Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17815&Anchor, in articles 77 - 81 of Law Nº 18.250 of January 6, 2008. Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?

Ley=18250&Anchor [Accessed on September 16, 2015],

- Crimes provided for in the Optional Protocol of the Convention on Children's Rights about trafficking in children, child prostitution, child pornography or any crime related to the trafficking and sexual exploitation of people. Available at: http://www.parlamento.gub.uy/htmlstat/pl/protocolos/prot17559.htm [Accessed on September 16, 2015] Available at: http://www.parlamento.gub.uy/htmlstat/pl/convenciones/conv16137.htm [Accessed on September 16, 2015];
- Currency counterfeiting and altering, provided for in articles 227 and 228 of the Criminal Code."

19 Meléndrez, P. *Wiretaps are Implemented "Sensibly", Judges Claim*. EL PAÍS. April 26, 2014. Available at: http://www.elpais.com.uy/informacion/jueces-disponen-escuchas-telefonicas-prudentemente.html [Accessed on April 30, 2015].

20 Uruguayan Criminal Code: Article 296. (Violation of written correspondence): Those who, in the attempt of getting knowledge about the content of correspondence, open a postal letter, or telephonic or telegraphic correspondence that was previously closed without them being the addressees, commit the crime of violation of correspondence. The punishment of this crime is a fine that ranges from 20 U.R. (twenty readjustable units) to 400 U.R. (four hundred readjustable units). Those who open, intercept, destroy or hide correspondence, parcels, and other postal objects in the attempt of taking possession of their content or of disrupting their course, shall be punished with one year of imprisonment or up to four years of penitentiary. Both crimes are aggravated whenever the offender is a public official belonging to the services of each case.

- Article 297. (Interception of telephonic or telegraphic notifications): Those who, using special devices, intercept, impede or interrupt a telephone or telegraphic communication shall be punished with a fine ranging from 20 U.R. (twenty readjustable units) to 400 U.R. (four hundred readjustable units).
- Article 298. (Disclosure of confidential correspondence and postal, telephonic and telegraphic communication): Whenever it causes harm, this is considered a crime, which is committed by: (i) Those who, without a rightful cause, reveal to others the knowledge they have acquired through any of the means mentioned in the previous articles. (ii) Those who, without a rightful cause, publish the content of postal, telegraphic or telephonic correspondence that was not addressed to them and which, by its very nature, should be kept confidential. The punishment for this crime is a fine ranging from 20 U.R. (twenty readjustable units) to 200 U.R. (two hundred readjustable units).
- Article 299. (Aggravating factors): The following are aggravating factors related to this crime:

    1. The offender is affiliated to the postal, telegraphic or telephonic service.

    2. The correspondence is official; The disclosure is carried out through the press.

21 See sentence of the Court of Appeals 1º 38/2005. Available at: http://www.jurisprudenciainformatica.gub.uy/jurisprudencia/ficha.jsp?id=81 [Accessed on September 16, 2015].

22 See the declaration of the Uruguayan civil society on this topic at: http://www.rga.com.uy [Accessed on September 16, 2015].

23 AGESIC is an agency that depends on the Presidency of the Republic. Its aim is to improve the services provided to the citizenry, by implementing the options that Information and Communications Technologies (ICT) give. Available at: http://www.agesic.gub.uy/ [Accessed on 16, 2015].

24 Law Nº 18.331, *Protection of Personal Data and Habeas Data*, 2008. Available at: http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor [Accessed on September 16, 2015].

25 Personal Data Control Regulatory Unit of the Eastern Republic of Uruguay (2014). *The Right to Privacy in the Digital Age: A/RES/68/167*. Available at: http://www.ohchr.org/Documents/Issues/Privacy/Uruguay.pdf [Accessed on September 16, 2015].

26 Sentence 58/209. Unconstitutionality Complaint. Available at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=46058

27 Judicial Branch - Eastern Republic of Uruguay. Unconstitutionality. Available at: http://www.poderjudicial.gub.uy/historico-de-noticias/140-articulos-explicativos/567-inconstitucionalidad.html [Accessed on October 8, 2015].

28 The Court states that: "subsection 2 of article 212 accepts the implementation of the interception of communications of any type, even in relation to third parties. Consequently, there cannot be a well-founding reason to sustain that the accused cannot be subjected to such measure, given that its scope also comprehends those who are not involved in the criminal process." (Court of Appeals for Civil matters, 2nd, Sentence 80/2006. Available at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37359).

29 Sentence 377/2013 Court of Appeals in Criminal Matters, 2 Court. Available at: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=37314

30 A co-occurring crime is an offense used as a means to commit the main offense.

31 See an initial report on the situation in Uruguay. Scrollini, Fabrizio. Uruguay: National Report in Global Information Society Watch, 2014. Available at: http://www.giswatch.org/2014-communications-surveillance-digital-age

32 Terra, Gonzalo. *The Government Purchased "El Guardián" [The Guardian] to Spy on Calls and E-mails*. El País, 2013. Available at: https://eff.org/r.5fvk [Accessed on September 16, 2015].

33 Newspaper El Observador (2014). *As of January, El Guardián is going to spy on e-mails and cellphones*. [ONLINE] Available at: http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757. [Accessed on September 29, 2015].

34 Newspaper El Observador (2014). *As of January, El Guardián is going to spy on e-mails and cellphones*. [ONLINE] Available at: http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757. [Accessed on September 29, 2015].

35 Legislative Branch, Senate. Available at: http://www.parlamento.gub.uy/indexdb/Distribuidos/ListarDistribuido.asp?URL=/distribuidos/contenido/senado/S20150196.htm&TIPO=CON [Accessed on September 29, 2015].

36 Joint Declaration: Surveillance, Security and Privacy: Uruguay Urged to Adopt Standards on Human Rights. Available at: http://www.cainfo.org.uy/2014/12/dia-internacional-de-los-derechos-humanos-declaracion-conjunta-vigilancia-seguridad-y-privacidad-llamamiento-para-que-uruguay-adopte-estandares-de-derechos-humanos/ [Accessed on October 23, 2015].

37 Newspaper El País. *Details Finalized before Implementing El Guardián*. http://www.elpais.com.uy/informacion/ultiman-detalles-implementar-sistema-guardian.html [Accessed on September 29, 2015].

38 De los Santos, F., (2015). Who Surveils those who Conduct Surveillance? *La Diaria*. Available at: http://ladiaria.com.uy/articulo/2015/3/quien-vigila-a-los-vigilantes/ [Accessed on September 18, 2015].

39 Judiciary of Uruguay (2015). Civil Court 5º Rejects Appeal on "El Guardián" and Notes Strategic Error by the Applicant. Available at: https://eff.org/r.qayy [Accessed on March 15, 2015].

40 This document indicates that "in other jurisdictions, the establishment of a secret legislation has been questioned due to jurisdictional and administrative processes that were completely devoid of transparency." The idea of a secret law, as established by Professor Kutz of Berkeley University, California, is "fundamentally repugnant." There can be mere secrets, but there cannot be meta-secrets in a democracy. Meta-secrecy refers to regulations, protocols and laws whose existence is only known by the State.

41 Newspaper El País. *Regional Governments Strengthen and Expand their Spying Capabilities. Noticias Uruguay y el Mundo actualizadas. EL PAÍS Uruguay, 2015*. Available at: http://www.elpais.com.uy/informacion/gobiernos-region-potencian-capacidad-espiar.html [Accessed on September 17, 2015].

42 EFF, Surveillance Self Defense, Tips, Tools and How-tos for Safer Online Communications. Available at: https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware [Accessed on September 17, 2015].

43 International Principles on the Application of Human Rights to Communications Surveillance, 2014. Available at: https://es.necessaryandproportionate.org/text [Accessed on January 21, 2016].

44 *Ibid.*

45 The authorities involved would be the DINACIE (National Intelligence Division of the State), the National Intelligence Coordinator and some departments that are not included within the structure of the several State forces (Land, Air and Sea).

46 International Principles, *op. Cit.*, Principle of Necessity.

47 *Bonomi: "El Guardián" Provides more Guarantees than the Current System.* Newspaper EL PAIS Uruguay, 2015. Available at: http://www.elpais.com.uy/informacion/bonomi-guardian-garantias-sistema-actual.html. [Accessed on August 19, 2015].

48 International Principles, *op. Cit.*, Principle of Adequacy.

49 Newspaper EL PAÍS Uruguay. Controversy around Wiretaps. Criminal attorneys Warn about Wiretaps without Judicial Authorization and Recording of Dialogs between the Accused and their Counsels. Newspaper EL PAÍS Uruguay. November 4, 2012. Available at: http://historico.elpais.com.uy/121104/pnacio-673703/nacional/escuchas-riesgo-en-interpretacion/

50 *Ibid.*

51 International Principles, *op. quote*, Principle of Proportionality.

52 Melendrez, Pablo, *op. Cit.*

53 International Principles, *op. Cir.*, Principle of Competent Judicial Authority.

54 International Principles, *op. Cit.*, Principle of Due Process.

55 International Principles, *op. Cit.*, Principle of User Notification.

56 International Principles, *op. Cit.*, Principle of Transparency.

57 Personal Data Control Regulatory Unit of the Eastern Republic of Uruguay, *op. cit.*

58 Melendrez P. C*riminal Judges Order Three Wiretaps a Day* Newspaper El País [Accessed on October 10, 2015] available at: http://www.elpais.com.uy/informacion/jueces-penales-ordenan-tres-escuchas.html

59 International Principles, *op. cit.*, Principle of Public Oversight.

60 International Principles, *op. cit.*, Principle of Integrity of Communications and Systems.

61 International Principles, *op. cit.*, Principle of Safeguards for International Cooperation.

62 OAS, Inter-American Convention on Mutual Assistance in Criminal Matters, 1992. http://www.oas.org/juridico/english/treaties/a-55.html [Accessed on July 22, 2015].

63 International Principles, *op. cit.*, Principle of Safeguards against Illegitimate Access and Right to Effective Remedy.