Comparative Analysis of Surveillance Laws and Practices in Latin America

Katitza Rodríguez Pereda

October 2016

ELECTRONIC FRONTIER FOUNDATION

The lead author of the "*Comparative Analysis of Surveillance Laws and Practices in Latin America"* is Electronic Frontier Foundation's (EFF) International Rights Director, Katitza Rodríguez Pereda. The legal review was done by EFF's Civil Liberties Director, David Greene. The technical review was done by EFF's Senior Staff Technologist, Seth Schoen. EFF's International Project Manager, Kim Carlson edited and formatted this report. EFF would like to thank Juan Camilo Rivera who consulted for EFF on this project, and Ana María Acosta, EFF Google Policy Fellow (2016), for their contributions to this report.

EFF would like to thank the following individuals for their valuable input, assistance, and feedback in the preparation of this paper:

Agustina Del Campo, Centro de Estudios en Libertad de Expresión y Acceso a la Información (Argentina)
Ana Tuduri (Uruguay)
Carolina Botero, Fundación Karisma (Colombia)
Daniela Schnidrig, Global Partners Digital (Argentina)
Dennys Antonialli, InternetLab (Brazil)
Fabrizio Scrollini (Uruguay)
Jacqueline Abreu, Internet Lab (Brazil)
Jorge Gabriel Jímenez (Guatemala)
Juan Carlos Lara, Derechos Digitales (Chile, Latin America)
Juan Diego Castañeda Gómez, Fundación Karisma (Colombia)
Leandro Ucciferri, Asociación por los Derechos Civiles (Argentina)
Luciana Peri, Fundación Acceso (Central America)
Luis Fernando García, R3D (Mexico)
Maricarmen Sequera, TEDIC (Paraguay)
Marlon Hernández Anzora (El Salvador)
Miguel Morachimo, Hiperderecho (Peru)
Verónica Ferrari, Centro de Estudios en Libertad de Expresión y Acceso a la Información (Argentina)

Thank you also to the following EFF staffers and consultants who contributed substantial time to the completion of this project:

Carlos Wertheman, EFF Spanish Editor
Danny O'Brien, International Director
David Bogado, former EFF Latin American Coordinator (Paraguay)
Justina Díaz Cornejo, translator
Sara Fratti, translator
Ramiro Ugarte, legal consultant

The following reports are part of a larger regional project conducted by the Electronic Frontier Foundation in 12 Latin American countries. They have been used as the main sources for the *"Comparative Analysis of Surveillance Laws and Practices in Latin America."*

Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, *"State Surveillance of Communications and the Protection of Fundamental Rights in Uruguay*," Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

Daniela Schnidrig and Verónica Ferrari, *"State Communications Surveillance and the Protection of Fundamental Rights in Argentina,"* Electronic Frontier Foundation & Centro de Estudios en Libertad de Expresión y Acceso a la Información, (2016). https://necessaryandproportionate.org/country-reports/argentina

Dennys Antonialli & Jacqueline de Souza Abreu, *"State Surveillance of Communications in Brazil and the Protection of Fundamental Rights,"* Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

Fundación Acceso, *"Privacy for digital rights defenders: a study on how the legal frameworks of El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance of human rights defenders,"* Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, (2015). https://necessaryandproportionate.org/files/2016/05/16/investigacion-privacidad-digital-fa.pdf

Jorge Rolón Luna & Maricarmen Sequera, "*State Communication Surveillance and the Protection of Fundamental Rights in Paraguay,"* Electronic Frontier Foundation & TEDIC, (2016). https://necessaryandproportionate.org/country-reports/paraguay

Juan Camilo Rivera & Katitza Rodriguez, *"State Communications Surveillance and the Protection of Fundamental Rights in Colombia,"* Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

Juan Carlos Lara and Valentina Hernández, *"State Communications Surveillance and the Protection of Fundamental Rights in Chile,"* Electronic Frontier Foundation & Derechos Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

Luis Fernando Garcia, *"State Communications Surveillance and the Protection of Fundamental Rights in Mexico,"* Electronic Frontier Foundation & InternetLab, (2016). https://necessaryandproportionate.org/country-reports/mexico

Miguel Morachimo, *"State Communications Surveillance and the Protection of Fundamental Rights in Peru,"* Electronic Frontier Foundation & Hiperderecho, (2016). https://necessaryandproportionate.org/country-reports/peru

Table of Contents

Introduction

In December 1992, following a hastily-drawn sketch of a map given to him by a whistleblower, the Paraguayan lawyer Martin Almada drove to an obscure police station in the suburb of Lambaré, near Asunción. Behind the police offices, in a run-down office building, he discovered a cache of 700,000 documents, piled nearly to the ceiling. This was "the Terror Archive," an almost complete record of the interrogations, torture, and surveillance conducted by the military dictatorship of Alfredo Stroessner. The files reported details of "Operation Condor," a clandestine program between the military dictatorships in Argentina, Chile, Paraguay, Bolivia, Uruguay and Brazil between the 1970s and 1980s.[1] The military governments of those nations agreed to cooperate in sending teams into other countries to track, monitor and kill their political opponents.[2] The files listed more than 50,000 deaths and 400,000 political prisoners throughout Argentina, Bolivia, Brazil, Chile, Paraguay, Uruguay, Colombia, Peru, and Venezuela.[3]

Stroessner's secret police used informants, telephoto cameras, and wiretaps to build a paper database of everyone that was viewed as a threat, plus their friends and associates. Almada had been tortured under this regime: his wife died from a heart attack shortly after the police played her, over the phone, the screams of her incarcerated husband. The Terror Archive shows how far a country's government might sink when unchecked by judicial authorities, public oversight bodies, and the knowledge of the general public.

A modern-day Stroessner or a revamped Operation Condor, however, would have far more powerful tools at hand than just ring-binders, cameras, and wiretapped phones. Today's digital surveillance technology leaves the techniques documented in the Terror Archive in the dust. New tech like the IMSI-catcher, a portable mobile cell-tower that lets its operator sweep up all the mobile phone calls and messages within a 200 meter radius, would let the authorities collect the identities of everyone at a protest. Mobile phones tell their providers where they are at all times: government orders could demand a mobile provider retain such data and hand it to the government. That would let the authorities track the movements of everyone who owns a cellphone. It would also allow them to "time travel": pick a target, and then look back in their history to see everywhere they had been for months or years.

For targeted intimidation and entrapment, governments could take advantage of the email, social media, and messages that dominate our lives. States could deploy for the purposes of

1 Paraguay's Archive Terror, http://news.bbc.co.uk/2/hi/americas/1866517.stm

2 Condor legacy haunts South America, http://news.bbc.co.uk/2/hi/3720724.stm

3 1992: Archives of Terror Discovered, http://nationalgeographic.org/thisday/dec22/archives-terror-discovered/

social control, the same malicious software, or malware, that petty Internet criminals use to take over innocent users' computers, by tricking them to click on fraudulent emails or websites. Some of this malware is also "spyware"—it can covertly record audio and video from the microphone and camera of a target's smartphone or laptop. Once installed, government malware could go much further: retrieving lists of contacts, or remotely planting incriminating evidence on the device. A net far wider and far more pervasive than any 20th century secret police project would be cast over the whole of society.

The disturbing truth is that these tools are not theoretical. Many governments are already using these techniques, with neither legislative constraints holding them back, nor any effective public oversight, as our research shows.

It took a leak from one of the world's most notorious malware providers, the Italian "Hacking Team," and careful detective work from investigative journalists, to reveal just how many Latin American governments were already using mass surveillance and other invasive tools such as commercial malware. IMSI catchers and worse are hinted at in court filings. On the rare and random occasions that courts are asked to sanction such super-spying, judges are often kept in the dark about the power and reach of these tools.

Twentieth century surveillance law mostly regulates the simple wiretapping of a single phone line, with no guidance on how to apply these laws to this growing menagerie of new spying capabilities. When new surveillance or cyber-security laws are passed, they are written primarily to legitimize existing practice, or widen existing powers—such as data retention laws that force phone and Internet companies to log and retain even more data for state use.

Each of these new powers is a ticking time-bomb, waiting for abuse. The only way to stop them being turned against the public is to create robust and detailed modern laws to constrain its use, an independent judiciary who will enforce those limits, and a public oversight mechanism that allows the general public to know what its country's most secretive government agents are up to in their name.

Unfortunately, legislators and judges within Latin America and beyond have little insight into how existing surveillance law is flawed, or how it might be fixed.

To assist in that imposing task, the Electronic Frontier Foundation has spent over a year working with our partner organizations across Latin America. Our intention was to hold a light up to current surveillance activities, in law, and in practice. We've carefully documented existing law in 13 countries, and gathered together the evidence of its misapplication whenever possible. Our aim with these papers is to compare existing practices to established human rights standards. Without that constraint, every country, within Latin America and without, not only risks violating the rights of their own citizens,

but places themselves in danger of being overthrown by illegitimate elements in their own society, powered by a tech-enabled secret police.

In our research, we have analyzed publicly available laws and practices. Given the deeply rooted culture of secrecy surrounding surveillance, it is far harder to judge the extent to which states comply with their own published legal norms. Ensuring that law not only complies with human rights standards but also genuinely governs and describes the states' real-world behavior is an ongoing challenge.

State officials and civil society must take care that written norms are translated into consistent practice and that failures to uphold the law can be discovered and remedied. That raises a second problem: the lack of adequate public oversight throughout the region. This is the main reason why even positive guarantees established by law—and there are many examples of good surveillance standards in the region—simply do not work. These can only be overcome if civil society demands transparency and accountability from the intelligence and law enforcement community.

Public oversight efforts are usually trumped by the secrecy which surrounds intelligence and law enforcement activities. However, the advances produced in the last decade in Freedom of Information laws throughout the region provide an opportunity to pierce through these obstacles and strengthen citizens' control over a part of the state which remains in the dark.

Our message is not entirely pessimistic. Our analysis has uncovered rights-preserving procedures in the books that are a step ahead of the rest of the world. Now we need to ensure that those procedures are actually enforced. In summary below, we list both the good and bad of modern Latin American surveillance law. Every state can improve, but many might benefit from imitating the positive experiences of other jurisdictions.

Technology cannot entirely defend us from the misuse of these new tools and capabilities. We need strong rule of law, robust statutes that are actually prescribed by law, necessary, adequate and proportionate. We need judicial guidance, due process, transparency and a right to be notified of the surveillance decision with enough time and information to enable them to challenge the decision or seek other remedies whenever possible. We need avenues for redress for those affected by the surveillance measure. Besides having a better institutional design for overseeing and controlling surveillance activities, the region should commit to implementing public oversight mechanisms that are carefully matched in resources and authority over those who wield these powers. We also need a strong civil society coalition working on these issues. With the help of watchful and informed judges and legislators, we hope that digital technology will be used wisely to protect, not violate human rights. We must ensure that we build a world where the Terror Archive remains a grim record of past failings, not a low-tech harbinger of an even darker future.

Executive Summary

The constitution of every Latin American country recognizes a right to privacy in some form, most commonly as a general right to private life or intimacy. Sometimes, it is protected as multiple, specific rights: a right to the inviolability of communications; a data protection right; or habeas data, which varies from country to country, but in general, habeas data protects the right of any person to find out what information is held about his or her person.

Unfortunately, despite this consensus, most states do not implement those rights in a way that fully complies with international human rights standards.

The Necessary and Proportionate Principles provide a touchstone for assessing whether a state's communications surveillance and interception practices comply with its human rights obligations. In this paper, we assess how closely each state's practices reflect those Principles. Using this analysis, we identify good practices that should serve as a model for all states, as well as specific reforms that will bring law and practice into compliance with human rights standards.

Our report also identifies deficiencies that are widespread throughout the region and are in need of special and immediate attention. Latin America appears to lag behind the rest of the world in permitting regulations that require private companies to retain data about the communications of the entire population. It stands in stark contrast to Europe, for example, whose own European Data Retention Directive was declared invalid after a successful human rights-based legal challenge. Nor has Latin American law kept up with the ever-broadening scope of "communications surveillance." As a result, new surveillance technologies such as cell-site simulators or IMSI catchers (which intercept cell phone signals by imitating cell towers)[4] and malware (software that is used to harm computer users)[5] are in widespread use without any specific authorization or human rights protections in place. States, too, have failed to broaden the scope of their surveillance laws to eliminate the outdated distinctions between the content of communications and other communications

4 Cell-site simulators, also commonly known as IMSI catchers or Stingrays, are devices that masquerade as a legitimate cell phone tower, tricking phones nearby into connecting to the device in order to log the mobile subscriber identity of mobile phones in the area or capture the content of communications. Learn more at: https://www.eff.org/sls/tech/cell-site-simulators

5 Malware 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, and gaining access to private computer systems. Learn more at: https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware

metadata.

Beside these general concerns, we can categorize the failings, reforms, and occasional successes of Latin American surveillance law under the individual principles of the Necessary and Proportionate standard.

The Principle of Legality

The Legality Principle requires that any limitation to human rights be prescribed by law, and that the law be public, precise, and unambiguous. Thus, the state must not interfere with the right to private communications in the absence of an existing public law that is sufficiently clear to ensure that individuals can foresee its application. History shows that imprecise intelligence laws are prone to abuse.

Our review of practices by Latin American governments found that many states only specifically authorize wiretapping—listening to or recording telephone conversations—and do not have precise legal authorization to conduct newer forms of surveillance, such as geolocation tracking, cell tower monitoring, or using IMSI catchers or malware. Like wiretapping, these technologies are invasive and surreptitious, but also raise far different privacy concerns and legal questions than traditional wiretapping. Despite a lack of legal footing, there appears to be widespread use of these technologies by authorities. Malware, for example, is known to be used in Mexico, Panama, Venezuela, Colombia, Brazil, Chile, Ecuador, Honduras, and Paraguay with insufficient legal authorization.

We also found that many communications interception and surveillance practices were authorized solely by the executive branch in the form of administrative decrees and administrative resolutions. These include data retention mandates in Brazil, Colombia, Peru, and Honduras: regulations that are paired with provisions allowing public investigators broad access to these stores of private information. Executive orders authorizing surveillance or mandating data retention are typically issued without any public discussion or input from the legislature or judiciary. Some guidelines regarding the collaboration between the private sector and the government remain secret, including confidential regulations and guidelines in El Salvador, Uruguay, and Peru. Although data retention is inherently an unnecessary and disproportionate measure, Mexico provides a hint of a best practice here—its controversial data retention mandate, which was adopted by a public legislative act, at least limits the data it requires companies to retain to a precise list.

Even when surveillance was encoded in legislative acts and other public laws, those regulations frequently suffered from vagueness and ambiguity. These laws are insufficiently clear about the specific powers that intelligence agencies and law enforcement have to surveil communications. The laws often fail to identify the appropriate situations when

surveillance may be conducted or which specific agency is empowered to conduct a specific form of surveillance or to access collected communications. Outside of Mexico, data retention mandates do not clearly specify what data must be retained. For example, laws in Peru that authorize location tracking typically do not describe which crimes may be investigated using that technique. Laws in Honduras do not describe which agencies have access to retained data, while in Colombia the data retention decree authorizes "other competent authorities" access; however, as a result of a citizen complaint, the phrase "other competent authorities" was repealed. A 2016 State Council's decision closed this loophole.[6] Now only the general prosecutor (*Fiscalía de la Nación*), through judicial police agencies, may access retained data.

Colombia's Law 1621, which regulates intelligence activities, also contains a vague definition of communications surveillance, leaving a large margin for potential abuse. Subsequently, the Constitutional Court of Colombia interpreted this vague language as granting intelligence agencies power to monitor the entire electromagnetic spectrum, regardless of the technological means employed.[7] But this law does not explicitly authorize mass surveillance: Under the case law that approved the new Colombian Intelligence Law, the Constitutional Court emphasizes that interception is only allowed during a criminal investigation and with judicial authorization. Under this law, intelligence agencies are only allowed to monitor the spectrum, which in theory is different from intercepting communications according to the Court. The law does not define what constitutes "monitoring the spectrum." But because Law 1621 clearly states that "monitoring does not constitute interception," a phrase that can be interpreted broadly, it's rather likely that the law can be used for that very purpose. Indeed, this may have already occurred: over the past several years, without any apparent legal authorization, several mass surveillance programs have been devised. These programs are supposed to be rolled out through mechanisms such as the Unified Platform of Monitoring and Analysis [Plataforma Única de Monitoreo y Análisis] (PUMA) and the Comprehensive System of Digital Recording [Sistema Integral de Grabación Digital, SIGD].

There is also a lack of clarity in the privacy safeguards that some laws provide. These legal frameworks use very broad legal provisions and can be interpreted as authorizing a wide range of both existing surveillance technologies, such as malware and IMSI catchers, and any future surveillance technology. For example, in Paraguay, Article 200 of the Criminal Procedural Code establishes that a judge can order the interception of the communications of any accused persons, "regardless of the technical means used" to achieve it. In Guatemala,

6 "Tumban polémico decreto sobre acceso a datos privados," Semana Económica, (2016). http://www.semana.com/nacion/articulo/consejo-de-estado-solo-la-fiscalia-podra-tener-acceso-a-datos-privados/465546

7 European Commission, Scientific Committee, Technical Terminology – Glossary. http://ec.europa.eu/health/opinions/es/lamparas-bajo-consumo/glosario/def/espectro-electromagnetico.htm

the Control and Prevention of Money Laundering Law authorizes the use of any technological means available for the investigation of any offense to facilitate clarification. Argentina's intelligence framework allows for significant exceptions to constitutional privacy protections in “states of emergency,” a phrase that is not adequately defined.

The Principle of Legitimate Aim

This Principle requires that any interference on human rights serve a specified Legitimate Aim that corresponds to an important legal interest that is necessary in a democratic society. Discrimination is categorically an illegitimate aim. Thus, the Principle requires that any measure infringing on a human right not be enacted for the purpose of discrimination or 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. The Legitimate Aim must operate to limit the state's restriction of rights, not be used as an excuse to grant the state wider leeway.

With respect to infringements on the right to private communications, the investigation of serious crimes and real, concrete threats to national security are recognized legitimate aims. Communications surveillance cannot be justified by reference to a general interest, such as “safety,” or a nonspecific or abstract concern for “national security.” The best practices in this area involve surveillance legislation that contains exhaustive lists of enumerated crimes (or some other clear and objective definition) and other legal constraints to ensure no human rights violations occur.

The report identifies several positive examples. Nicaragua, Guatemala, and Peru limit the interception of communications to the investigation of specific serious crimes that are listed in the statute. Other states, however, such as Argentina and Chile, do not adequately define terms such as “terrorism” nor specify how severe a suspected crime must be before communications surveillance is permitted. As a result, subjective, arbitrary, and/or improper political considerations may dictate when such measures are used.

Colombia adequately defines the crimes in which communications surveillance may be used in order to aid their investigations, but it fails to provide the same specificity and clarity with respect to intelligence operations.

The Principles of Necessity, Adequacy, and Proportionality

The Necessity Principle requires all laws, regulations, and activities that interfere upon human rights be limited to what is strictly and demonstrably necessary to achieve a Legitimate Aim. Surveillance must be conducted only when it is the only means available to achieve a Legitimate Aim or, when there are multiple means, is the means least likely to

interfere upon human rights. The onus of establishing this justification is always on the state. The Adequacy Principle requires that any interference with human rights that is authorized by law be an effective means of fulfilling the specific Legitimate Aim identified. The Proportionality Principle requires that infringement decisions consider the severity of the human rights violations and other competing interests on a case-by-case basis, and only allow infringement if the public interest gains appropriately balance the human rights losses. Moreover, any measure that interferes with human rights must be the least invasive means for actually accomplishing a Legitimate Aim.

A State must establish, at a minimum, the following to a Competent Judicial Authority, prior to conducting communications surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

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

Compliance with these conditions must be assessed with respect to each aspect of the surveillance process: the decisions to surveil, the means of surveillance chosen, and requirements for data retention and access to stored data.

These Principles are deeply embedded in the region's constitutions. However, the development of new surveillance technologies and the increasing amount of data that can be obtained by way of communications surveillance have complicated the application of these Principles, resulting in some government surveillance activities that lack necessity, adequacy, or proportionality.

As the most striking example, data retention laws, since they require the infringement of the

rights of all users of a communications service regardless of particularized suspicion, are inherently disproportionate. Yet, as discussed above, data retention mandates are widespread throughout Latin America.

There are also good practices. The surveillance laws of El Salvador, Brazil, Colombia, Chile, and Guatemala incorporate rigorous necessity, adequacy, and/or proportionality analyses, though it remains to be seen whether these laws will be implemented in a privacy protective manner. Some states, such as Chile and Honduras, set time limits on surveillance operations, reflecting a concern for proportionality. Peru's law specifically limits the retention of data obtained by state agencies to ensure that it is destroyed once it is no longer useful. Some states, such as Paraguay, Uruguay, Mexico, Colombia, Nicaragua, and Chile, appropriately prohibit the surveillance of certain communications, most commonly attorney-client communications.

The Principles of Transparency and Notification

States should be transparent about the use and scope of laws, regulations, activities, powers, and techniques that infringe on human rights. Without transparency, civil society is unable to hold governments accountable, and persons are not accorded the dignity of knowing when their rights are violated. Secrecy prevents meaningful public debates on these matters of extreme importance.

Transparency is especially important with respect to communications surveillance, because of a reflexive perceived need for secrecy by investigators and intelligence agencies. These actors unfortunately commonly confuse a need for secrecy in a specific situation with an overarching reticence to describe operational capacities and legal authority. Even if an agency has a good reason to keep a specific investigation confidential, it does not need to keep secret the fact that, for example, it uses malware and has been authorized to do so as a general matter. Without transparency, the public is denied the opportunity to debate whether malware should be used at all and, if so, under what specific conditions.

There are several methods states (and telecommunications companies) can implement in order to increase transparency about communications surveillance. States can publish information about the purchases they have made of surveillance technologies. States can comply with Freedom of Information laws when faced with requests for records regarding their surveillance laws and capabilities. States can issue transparency reports in order to provide useful information to citizens and users and require or encourage telecommunications providers to issue them as well. Telecommunications companies can establish and publish law enforcement guidelines: a set of rules that set forth the circumstances under which they will or will not deliver information to law enforcement, and states can agree to abide by them. States should also permit providers to inform users

that they are or were surveilled.

We found that, unlike other regions, Latin America has yet to develop a culture of transparency reporting by communications providers. Several countries have yet to see transparency reports published by state entities, telecommunications firms, and major communications application providers. In Nicaragua, Guatemala, and Honduras, for instance, neither the state, nor local telecommunications firms, nor Google, Twitter, nor Facebook publish transparency reports. In other countries such as Chile, Peru, Colombia, and Brazil, Google, Twitter, and Facebook have published transparency reports but telecommunications firms have not done so, and, in El Salvador, only Twitter and Facebook have published reports. Mexico is the only country where local telecommunication companies have published transparency reports. Iusacell, Movistar, Nextel, and Telcel have published a transparency report through ANATEL (Asociación Nacional de Telecomunicaciones). This is an important first step. However, this transparency report only provides readers with a general number of requests made by authorities; it does not provide detailed information about which type of requests have been received, which authorities made the requests or what reasons authorities gave to make the requests. Overall, the secrecy surrounding even basic information on the extent of surveillance is widespread in the region. Indeed, since many of the intelligence regimes in the region were formed during dictatorships, there remains a general default to secrecy in matters of surveillance. Secret laws authorizing surveillance exist, however the advances produced in the last decade throughout the region with Freedom of Information laws should provide an opportunity to pierce through these obstacles. Still, broad legal exceptions for intelligence and police investigative information still exist and the secrecy surrounding state surveillance prevents citizens from learning how these laws are applied in this context.

Our survey did not find any best practices in the region, but a few states do employ some good practices worth replicating with some specified improvements. In Mexico, governmental agencies must regularly disclose statistical information about the requests they've made to telecommunications service providers for communication interceptions, access to communications records, and access to location data in real time. A guideline that regulates the collaboration between the government and the private sector requires telecommunications companies to submit transparency reports to the Telecommunications Federal Institute. Brazil, Chile, and Colombia require agencies to report to another governmental agency, but not the public, unless a record is specifically requested. The benefits of Freedom of Information laws in El Salvador, Honduras, Nicaragua, and Guatemala are limited and uncertain because of ambiguities and exceptions in those laws.

The Principle of Notification also requires that users be notified to the greatest extent possible when they are surveilled. In all but exceptional situations users should have the opportunity to contest planned surveillance or seek other remedies. Any delay in notification must be judicially approved and only upon proof that notification would

seriously jeopardize the purpose for which the surveillance was authorized, or the existence of an imminent risk of danger to human life. Notification must take place when those conditions no longer exist.

The report identifies some good practices for user notification. Peru and Chile require notification of those affected by surveillance, but only after the investigation closes, and with some exceptions. Peru allows the user to seek judicial re-examination of the surveillance order. Some states, such as Colombia and El Salvador, provide for user notification but only if the user is a criminal defendant and the surveillance yields evidence to be used against them. Many other states lack requirements for user notification. Indeed, Nicaragua and El Salvador place an affirmative duty of confidentiality upon telecommunications providers that prevents them from notifying anyone about governmental requests for information.

The Principles of Competent Judicial Authority and Due Process

The Judicial Authority Principle requires that the judicial oversight authority be: (i) separate and independent from the authorities restricting human rights; (ii) conversant in relevant issues and competent in making judicial decisions; and (iii) adequately resourced in exercising the functions assigned to it.

The Due Process Principle addresses many of the same concerns and advances many of the policies established in the Competent Judicial Authority Principle. 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 public. In cases of emergency, when there is imminent risk of danger to human life, retroactive authorization must be sought within a reasonable time period. Retroactive authorization may not be justified solely by concerns of a flight risk or concerns about destruction of evidence.

As a result, communications surveillance must be formally authorized on a case-by-case basis by an independent and impartial judiciary, with access to the appropriate technological expertise. This ensures that the state is not acting beyond its authority and that due consideration is given to the human rights of those affected by the surveillance. It ensures that the subject's human rights are protected at every step in the authorization process. By requiring the state to justify each act of surveillance to a judge, this principle ensures that communications surveillance is conducted only when necessary and when the effect on human rights is eliminated or minimized. It also ensures that when possible, the subject of surveillance has an opportunity to challenge the state's intended action.

The report finds mixed compliance with these Principles throughout the region. For example, the constitutions of Mexico and Peru require judicial authorization for every interception of a private communication, and courts have interpreted these requirements so that they are applied broadly. But the requirement does not appear to be used when obtaining location data. Peru allows access to location data in real time without a court order in cases of serious crimes. While Mexican constitutional interpretation has considered that communications metadata is protected in the same way that communications content is protected (meaning accessing them requires judicial authorization), the Supreme Court of Justice has stated that it's not necessary to obtain judicial authorization to monitor location data in real time. In Argentina, Guatemala, and Chile, most surveillance, both for criminal and intelligence investigations, requires judicial approval. In Colombia, prior judicial authorization is required for any legal measure that affects human rights, except in surveillance cases for criminal matters. In those cases, the Attorney General may authorize surveillance subject to subsequent review. Brazil requires judicial approval for the interception of the content of communications, but not subscriber information.

The Mexican Supreme Court (SCJN), in particular, has made some positive steps to ensure judicial review of Mexico's surveillance programs in certain cases. It has also determined, for example, that accessing and analyzing data stored on a mobile phone without a judicial order is an infringement on the right to the inviolability of private communications. Likewise, the SCJN recently decided that access to communications metadata stored by telecommunications companies must have prior judicial authorization. The same court has stated that an email counts as being "intercepted" (in such a way that it infringes upon the right to inviolability of communications) the moment that the password of an account has been taken without judicial order or the user's consent, regardless of whether the content of the email was analyzed.

The Principle of Public Oversight

The Principle of Public Oversight requires that states establish independent oversight mechanisms to ensure transparency and accountability for infringements on human rights. This oversight mechanism should be available to the public, either in the form of public investigations or, at a minimum, periodic reporting. Public oversight promotes checks and balances within the government.

With respect to infringements on the privacy of communications, public oversight usually comes in the form of judicial oversight as described above. However, these systems rarely provide the public oversight the Principle requires. In some legal systems, public, civil grand juries can provide oversight and auditing functions for various types of governmental operations to review surveillance programs. The judiciary may also appoint a Special Master to oversee and monitor a program, particularly when the program is in need of significant

reform.

There is almost no tradition of public oversight mechanisms in place in the region. El Salvador, Chile, Colombia, Brazil, and Argentina require various forms of audits, but offer no apparent public access to them.

Most of the intelligence agencies in Latin American were formed at a time when such a division of powers was nonexistent—meaning under military rule in which governmental operations were embedded in the executive power.[8] Because these intelligence agencies were part of the militarized dictatorships, most of the governments transitioned into democracies through a negotiation process with the military junta, and thus were formed without well-placed controls or oversight mechanisms. Intelligence organizations in Latin America were formed at a time when democratic regimes were either weak or non-existent. So the few oversight mechanisms that were placed *on top* of the inherited non-democratic culture are inherently ineffective.

Furthermore, the *enhanced* nature of Latin American presidentialisms also explains why oversight mechanisms were inadequate.[9] In the region, presidents are formally more powerful than, for example, their United States peers (they can declare emergencies, can introduce legislation in Congress, and so on). Furthermore, it has been argued that the political dynamics in the region usually create a situation where Congress *delegates* power to presidents, either *de jure* or *de facto,* at least during the initial moments of a presidency.[10] If these analyses are correct, they could explain why legislative oversight mechanisms do not work. Intelligence agencies in Latin America have been powerful tools in presidential politics, specially used to spy on dissident groups, opposition politicians or independent journalists.[11] These abuses have been widely documented: from the Peruvian scandals involving Vladimiro Montesinos in the 1990s to the DAS' former Colombia Intelligence Agency wire-tapping revelations of the 2000s in Colombia, to the more recent upheaval involving intelligence agencies in Argentina. The use of intelligence agencies to support presidential politics and wishes is a strong argument for why oversight mechanisms in the region do not work. The *delegative* nature of presidential politics explains, furthermore, why legislative oversight mechanisms usually approach their task with a *laissez faire* doctrine

8 José Manuel Ugarte. El control público de la actividad de inteligencia en América Latina. Ediciones CICCUS, Buenos Aires, 2012.

9 Mainwaring, Scott. "Presidentialism in Latin America." Latin American Research Review 25, no. 1 (1990): 157–179, 160.

10 O'Donnell, Guillermo A., ed. Counterpoints: Selected Essays on Authoritarianism and Democratization. First Edition edition. Notre Dame, Ind: University of Notre Dame Press, 2003.

11 *See* Ramiro Álvarez Ugarte and Emiliano Villa. El (des)control de los organismos de inteligencia en la Argentina. Asociación por los Derechos Civiles (ADC). January 2015. Available at: http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

which is incompatible with the demands of modern democratic societies.

These institutional weaknesses can only be overcome if a strong civil society demands transparency and accountability from the intelligence community.

The Principle of Integrity of Communications and Systems

These Principles seek to preserve the integrity of communications infrastructures by limiting states' ability to compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for communications surveillance purposes. The Principles also incorporate the right of individuals to express themselves anonymously, by preserving the integrity of anonymization tools. These Principles thus require states to refrain from compelling the identification of users and to acknowledge the right to use encryption.

Unfortunately, threats to systems integrity abound in the region. Brazil prohibits anonymity in its Constitution. Colombia has an extremely broad prohibition on encryption and, like Nicaragua and Peru, requires telecommunications providers to provide access and the capacity to intercept for states wishing to surveil their users. El Salvador requires providers to decrypt or be able to decrypt communications upon demand.

The Principle of a Right to an Effective Remedy

The Principle of the Right to an Effective Remedy requires that there be a readily available legal remedy for every infringement of human rights. Compliance with this Principle thus requires that every state prohibition or limitation on communications surveillance be accompanied by a penalty against the government and compensation to the affected persons.

Good, but incomplete, examples are found throughout the region. A key problem remains, though—private communications are offered insufficient protections in the region. For example, in Argentina and Colombia, criminal penalties may be imposed on members of the intelligence services who unduly intercept or divert communications and who fail to destroy communications records when required to do so. Chilean criminal law generally penalizes those who violate the right to privacy, but the deficiency in user notification requirements means that the violations may never be discovered.

Final Recommendations

What do our studies suggest could be done to improve the state of surveillance law and practice in the Americas? To improve clarity and aid the public's understanding, states

should have dedicated communications surveillance laws rather than a jigsaw puzzle of numerous provisions spread throughout various legislation. Surveillance laws should not distinguish between different kinds of communications data and should afford equal and equally strong protection to content, metadata, geolocation data, subscriber information, real-time communications, and stored data. And all infringements on the right to private communications must comply with the Necessary and Proportionate Principles.

In many areas, Latin American states have favorable practices that can be replicated throughout the region. But in other cases, a major shift in traditional practices is necessary. Nevertheless, these changes are all achievable.

First, we urgently need to end the culture of secrecy surrounding communications surveillance. We need the ensure that civil society, companies, and policy makers understand the importance of transparency in the context of surveillance, and why transparency reporting from the companies and the state is crucial to preventing abuses of power.

Second, we need to fix the lack of adequate public oversight mechanisms. That is the *main* reason even good guarantees established by law—and we have many in the region—simply do not work.

Finally, besides having a better institutional design for overseeing and controlling surveillance activities, the region should commit to building a strong civil society coalition to work on ensuring strong legal safeguards are in place and enforced.

Our hope is that, through our research, states can draw from the best, and learn from the worst, that Latin American surveillance law has to offer.

1.
Laws or Lawlessness

The Legality Principle requires that 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.

Not all rules limiting the right to privacy and communications surveillance in the region are prescribed by formal laws passed by legislatures. Rather, privacy rights are often limited by various types of administrative decrees, regulations, and other executive powers. Some of these administrative rules were adopted without any public discussion in the legislative branch. In some cases, these norms remain secret.

Other countries' laws are vague, inconsistent, or contain large loopholes that fail to safeguard individuals' fundamental freedoms. They provide little clarity about the powers of intelligence and law enforcement agencies, and the circumstances under which these agencies may conduct investigations. Surveillance laws often fail to specify to which agency each law applies, and who is authorized to surveil. Some laws include data security rules and impose usage conditions. However, they do not identify who is entitled to access the data that are subject to those rules.

In other cases, the legal loopholes are so broad that they can be interpreted as authorizing a full range of both existing surveillance technologies, including malware and IMSI-catchers, and any future surveillance technology. Although we did not find any legislation in the region that explicitly authorized the use of malware or IMSI-catchers, it is well known that these devices are widely used.

The following are some of the most egregious examples of surveillance laws in terms of both criminal and intelligence legal frameworks that fail to comply with the Legality Principle.

1.1 Surveillance Laws, Protocols, and Statues Are Often Not Prescribed by Law

Some communications surveillance laws, protocols, and statutes are kept secret, and secret installations of surveillance technology occur under their authority. Such secret

authorizations allow unchecked and unregulated spying. This pattern exists across the world. Moreover, law enforcement and governments exploit new technologies. They gain more invasive surveillance capabilities and enact secret procedures for employing them.

We found secret guidelines in El Salvador, Uruguay, and Peru.

EL SALVADOR: Article 31 of the Special Law on Telecommunications Intervention establishes the cases in which communication interceptions can be authorized. Article 31 of this law requires that the Office of the General Prosecutor (Fiscal General) enact public regulations and guidelines for police operations (including communications surveillance). It also requires them to establish a process for selecting and overseeing the director, officials, staffers, and members of the national civil police.[12] The specific regulations and guidelines pursuant to this law are classified as "confidential" according to the Unit for Access to Public Information of the Prosecutor's Office, per a Freedom of Information Act request.[13] For now, the people of El Salvador have no way of knowing how and why they are being surveilled or how that surveillance is being overseen.

URUGUAY: The government secretly purchased *El Guardián*, an electronic surveillance system created by the Brazilian company, Digitro Technology Ltda. The government has yet to set any public regulations governing its use.[14] According to the Uruguayan press, the Ministry of Economy issued a secret decree establishing the government's need to purchase surveillance technology. The decree also gave tax incentives to any telecommunication company that could provide the Interior Ministry with such technology. The newspaper, *El Observador*, revealed that the government also issued a secret collaboration protocol between the Interior Ministry and local telecommunication companies governing the use of *El Guardián*.[15] The document indicated that telecommunication companies were obliged to

12 El Salvador, Ley Especial para la Intervención de las Telecomunicaciones, Asamblea Legislativa, (2010). http://www.oas.org/juridico/PDFs/mesicic4_slv_telecom.pdf

13 Resolution 128-UAIP-FGR-2015. Freedom of information request submitted by Marlón Hernández, researcher at Fundación Acceso, Costa Rica. Cited in Fundación Acceso (coord. by Luciana Peri), "¿Privacy for Digital Rights Defenders: A Study on how the Legal Frameworks of El Salvador, Guatemala, Honduras and Nicaragua Can be Used for Protection"(¿Privacidad Digital para Defensores y Defensoras de Derechos: un Estudio Sobre Cómo los Marcos Legales de El Salvador, Guatemala, Honduras y Nicaragua Pueden ser Utilizados Para la Protección, Criminalización y/o Vigilancia Digital de Defensoras y Defensores de Derechos Humanos), (2015). https://necessaryandproportionate.org/files/2016/05/16/investigacion-privacidad-digital-fa.pdf

14 For more in-depth research, see Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "State Surveillance of Communications and the Protection of Fundamental Rights in Uruguay," Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

15 Leonardo Pereyra, "As of January, El Guardián is going to Spy on e-mails and cellphones," El Observador, October 12, (2014). http://www.elobservador.com.uy/el-guardian-espiara-

connect their computers to *El Guardián*.[16] Information about the purchase and regulation of *El Guardián* remains secret.

PERU: The protocol in Peru used to access geolocation data is kept secret from the public. In October 2015, under Ministerial Order 0631-2015-IN, the Ministry of Interior, authorized by Legislative Decree 1182, approved a protocol that regulates access to geolocation data of cellphones and electronic devices. Based on the national security exception of the Freedom of Information Act, the Ministry categorized this protocol as "reserved information."[17] Therefore, Peruvian citizens cannot obtain information about the protocol, even if the procedure is being applied to them. This is especially curious because a different protocol, the Protocol on the Interception and Recording of Communications, approved in November 2014 by Ministerial Order Nº 0243-2014-JUS, is public.

1.2 Data Retention Mandates Lack Legislative Authorization

The following countries have passed data-retention obligations that are not prescribed by law, but by an executive or administrative authority.

BRAZIL: Several data-retention mandates were established through administrative resolutions issued by the Brazilian telecom regulator, ANATEL, rather than actually being adopted into formal law. ANATEL's Resolution 426/05 requires service providers to retain phone records and other data processed by landline service providers. ANATEL's Resolution 477/07 compels mobile telephone service providers to retain billing documents that contain data of the incoming and outgoing calls of its subscribers for at least five years. Such data include the time, duration, and price of the calls, as well as the account information of the subscribers. Additionally, ANATEL's Resolution 614/13 compels Internet service providers to retain connection logs and subscriber account information pertaining to Internet connections for at least one year.[18]

COLOMBIA: In the criminal context, Decree 1704 of 2012 establishes several surveillance measures that infringe upon human rights. These include a data-retention obligation for

enero-mails-y-celulares-n289757

16 Leonardo Pereyra, "As of January, El Guardián is Going to Spy on e-mails and Cellphones," *El Observador*, (2014). http://www.elobservador.com.uy/el-guardian-espiara-enero-mails-y-celulares-n289757

17 NGO Hiperderecho issued a freedom of information request which was then denied. For a more detailed analysis, see Miguel Morachimo, "Peru: State Surveillance of Communications and the Protection of Fundamental Rights in Peru," Electronic Frontier Foundation & Hiperderecho, (2016). https://necessaryandproportionate.org/country-reports/peru

18 For the purposes of this report, account information refers to information included in the user's records with the telephone company, autonomous system operator, or application provider.

ISPs and network providers. This decree was adopted by an administrative agency—the Ministry of Information Technology and Communications—rather than the Legislature.

PERU: Peru's executive power adopted Legislative Decree 1182 (also known as Ley Stalker) one day before Peru's Independence Day, when most of the country was on holiday. Legislative Decree 1182 creates a data-retention obligation for telecommunication providers (concesionarios de servicios públicos de telecomunicaciones) and public entities that provide telecom services (such as airports that provide Wi-Fi).[19]

HONDURAS: Pursuant to administrative resolution NR 004/11, which approved the regulation for service providers in Honduras, ISPs (Servicio de Internet o Acceso a Redes Informáticas) are obligated to retain the "IP addresses of the users of the service that serve as a source for judicial or other relevant authorities' investigations for one year only." This resolution was issued by the country's telecom regulator, CONATEL[20]

In contrast, Mexico's data-retention mandate was adopted by a legislative act. It has been in force since 2009 in what is now known as the repealed Federal Telecommunications Law (LFTR); the new LFTR extends the data-retention period to 24 months.

In Brazil, there are two additional legal provisions that create data retention mandates. Law 12,850 of 2003 requires fixed and mobile phone providers to retain call records for a period of five years, and the Marco Civil compels "autonomous systems" who provide Internet to retain connection logs for one year. Learn more about data retention in section 1.3.2.

1.3 Vague or Broad Legal Frameworks Are Prone to Abuse

Throughout the region, we find several surveillance laws that are vaguely worded, inconsistent, or contain large loopholes. They fail to safeguard individuals' fundamental freedoms. Many of them do not clarify the appropriateness of the surveillance request, who can access the data, or the circumstances and conditions under which they may do so.

1.3.1 Location Tracking

Most people today walk around with a device that transmits their location. Mobile phones register to a nearby tower as the owner moves from location to location. The phone company can collect that data in real time or retrospectively to physically place the phone with varying degrees of accuracy. Companies can also determine the owner of every handset within range of a particular tower. GPS-enabled phones permit far more precise location

19 Criminal Procedural Code of Peru, art. 259. http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=default-nuevocodprocpenal.htm&vid=Ciclope:CLPdemo

20 Honduras, Resolución NR004/11, Comisión Nacional de Telecomunicaciones, CONATEL, (2011). http://www.tsc.gob.hn/leyes/Reglamento%20del%20Servicio%20de%20Internet%200%20Acceso%20a%20Redes%20Inform%C3%A1ticas.pdf

placement. At EFF, we advocate that the law protect location information by requiring police to get a search warrant before obtaining this sensitive data. We also work to ensure that location-based service providers do not abuse the information they collect or hand it over to the police without strong legal safeguards.

Although individuals might not realize all the implications continuous monitoring of their locations may have, it can be extremely sensitive because of its tendency to reveal personal relationships (such as the identities of those who live or spend the night together), religious practices, friendships and associations, medical consultations, participation in political organizations and events, and many other relationships and activities of daily life. While a few of these might be discovered or revealed in other ways, location tracking can reveal them systematically and on a large scale—like creating a record of every mobile device that was present at a political rally or protest.

PERU: Peru does not provide strong legal protection for location privacy. Legislative Decree 1182 grants the National Police warrantless 24/7 access to real-time location data of mobile phones or electronic devices in criminal instances when the following three requirements occur simultaneously: (i) there is a blatant crime (*flagrante delicto*), (ii) the punishment for the crime under investigation is more than four years in prison, and (iii) access to this information is necessary to the investigation.[21] Article 259 of the Criminal Procedural Code defines "blatant crime" very broadly. Its definition includes emergency procedures (when there is an imminent risk to human life). It also includes any crime that is being committed or has just been committed, and up to 24 hours after the crime has been committed.[22] Legislative Decree 1182 also fails to define location or geolocalization data, and to limit the entities obliged to implement this obligation. It compels not only telecommunication providers but also any public or private entities who provide Internet access to retain location data of users. Moreover, the same entities are obliged to develop and provide the National Police with "exclusive access" to these data.[23]

COLOMBIA: Decree 1704 of 2012 requires telecommunication services (Claro and Movistar) and network providers to hand over location data to authorities. Such location data includes geographic coordinates, signal potency, and "other information" that helps to determine the geographic location of the terminal, equipment, or devices. The location data must be handed over in real time or online to the Prosecutor's Office upon request. Content

21 Criminal Procedural Code of Peru, art. 259. http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=default-nuevocodprocpenal.htm&vid=Ciclope:CLPdemo

22 For a detailed analysis of the legal problems regarding location tracking, see Miguel Morachimo, "Peru: State Communications Surveillance and the Protection of Fundamental Rights in Peru," Electronic Frontier Foundation & Hiperderecho, (2016). https://necessaryandproportionate.org/country-reports/peru

23 Decree Legislative 1182 of Peru, art. 4, and Final Complementary Dispositions (Disposiciones Complementarias Finales), first article.

and Internet application providers (Mercadolibre.com and Tappsi.com) are excluded from this provision.

The real-time location-tracking provisions in Article 4 are unclear about the type of data that should be turned over in real time to the General Prosecutor's Office. According to this article, the data should be "the specific information contained in the companies' databases, such as sectors, geographic coordinates, and signal potency, among others." The use of the words "among others," like "such as," opens the door for these companies to turn over unspecified types of information to the authorities.

MEXICO: The new Federal Telecommunications and Broadcasting Act (LFTR) lacks clarity regarding which authorities can access geolocation data. Article 190, Section I of the LFTR compels telecommunication companies to "collaborate with the security agencies, law enforcement and administration of justice authorities to obtain the geographical location of mobile communication devices in real time." This provision grants power "to authorities who did not, and do not, have this power in an enabling law, such as the "security agencies" or the "administration of justice authorities" (*instancias de administración de justicia*, in Spanish) which are defined neither in the LFTR nor in any other law."[24] However, a 2016 Mexican Supreme Court decision[25] recently established that the only authorities who are authorized to access location data are the Federal and State Prosecutors, the Federal Police, and the Center for Investigation and National Security (CISEN).[26]

1.3.2 Data retention mandates

BRAZIL, COLOMBIA, CHILE, MEXICO, PERU, and HONDURAS all have data-retention obligations that require certain technology companies to log vast amounts of intrusive data about their users and provide law enforcement access to this stockpile on demand. Government-mandated data retention impacts millions of ordinary users and is an inherently disproportionate measure. Data retention compromises online anonymity, which is crucial for whistle-blowers, investigators, journalists, and those engaging in political expression. It also compromises the privacy of certain protected communications. These include those between an attorney and his or her client, a doctor and his or her patient, and a journalist and his or her sources.

24 For a detailed analysis of the legal problems regarding data retention, see Luis Fernando Garcia, "Mexico: State Communications Surveillance and the Protection of Fundamental Rights in Mexico," Electronic Frontier Foundation & InternetLab, (2016). https://necessaryandproportionate.org/country-reports/mexico

25 Second Chamber, Supreme Court, Amparo in Revision 964/2015.

26 Luis Fernando Garcia, "Mexico: State Communications Surveillance and the Protection of Fundamental Rights in Mexico," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/mexico

Data-retention obligations force ISPs and telecommunication companies to create large databases of information about their users' communications. Because these databases are vulnerable to theft and accidental disclosure, such data-retention obligations actually increase privacy risks.

Legal frameworks for mandatory data retention, which are usually paired with legal provisions that allow investigators to access such data, are unclear about the type of data companies are obligated to retain, who is authorized to access it, and for what purposes.

In recent years, more and more dangerous data retention mandates have been introduced in Latin America. Paraguay is the only country in the region that has rejected a mandatory data-retention bill. Its rejection was fairly aligned with the Grand Chamber of the European Court of Justice judgment that invalidated the EU Data Retention Directive in 2014 for seriously interfering with the right to privacy.[27]

HONDURAS: The data-retention obligation established in Article 20 of the Service Provider or Access to Networks Regulation (Resolution NR004/11) does not indicate which entities may access retained data. The CONATEL Resolution established that service providers are obliged to retain IP addresses for one year in order to serve as a source for "judicial investigation" or other "competent authorities'" investigations of illegal activities "when appropriate." The resolution fails to specify the standards for accessing data or any other limitations on the types of crimes for which this data can be retrieved. It also broadens the purpose for retrieving data beyond judicial investigations.

COLOMBIA: In the criminal context, Decree 1704 of 2012 establishes a data-retention obligation for telecommunication services (*servicios de telecomunicaciones*), such as ISPs and network providers (*proveedor de redes*),[28] to retain up-to-date "subscriber information" for a period of five years and to provide the prosecutor's office with this information upon request.[29]

The data-retention obligation provides examples of the types of data telecommunication services and network providers are obliged to retain. These data consist of "subscriber information, 'such as' billing information, identity, and type of connection." However, the use of "such as" (*tales como*) demonstrates that it is not an exhaustive list; this open-endedness creates ambiguity regarding what other types of subscriber data must legally be

27 Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others. http://curia.europa.eu/juris/documents.jsf?num=C-293/12

28 In the Colombian legal framework, Internet companies and Internet applications are considered content and applications providers, and are hence excluded from Decree 1704. See Resolution 000202 of 2010.

29 Colombia, Decree 1704 of 2012, art. 4.

retained.

The article is also unclear about which authorities can access the retained data and under what conditions. Originally the decree stated that the General Prosecutor (*Fiscalía de la Nación*) or "other competent authorities" (for example, the Directorate of National Taxes and Customs of Colombia and the Office of the Comptroller General) could access data through the judicial police designated to investigate the case. However, this vagueness failed to identify specifically who these authorities were. As a result of a citizen complaint, the phrase "other competent authorities" was derogated; a 2016 State Council's decision closed this loophole.[30] Now only the general prosecutor (*Fiscalía de la Nación*), through judicial police agencies, may access the retained data.

In the intelligence and counter-intelligence context, Law 1621 of 2013 pose similar problems. Article 44 of Law 1621 compels telecommunication service providers to give intelligence and counterintelligence agencies "communication history"—technical data that identify subscribers and their cell locations, and "any other information" that contributes to subscribers' locations. Information is provided upon request of intelligence agencies under an "authorized operation," whenever it is technically feasible. The intelligence agencies must limit to a maximum of five years their request to access data. This means that this provision does not explicitly impose a data-retention obligation on all companies, but only on those that already have the data.[31] However, mobile companies and network providers, including ISPs, are already obliged to retain data under Decree 1704 of 2012.

The law provides immunity to network providers and telecommunication services. It states that they are not responsible, under any circumstances, for what the intelligence and counterintelligence agencies do with the data in compliance with this law.[32]

MEXICO: Article 190 of the Federal Telecommunications and Broadcasting Act (LFTR) of 2014 ordered telecommunications providers to retain data for 12 months on systems that allow law enforcement agencies to access and obtain the data electronically, in real time. After this one-year period, telecommunications providers must keep the data for an additional 12 months and, upon request, deliver it to authorities within 48 hours. The Mexican Supreme Court recently declared this law constitutional, stating that this data-retention obligation does not constitute an interference with the right to the inviolability of

30 "Tumban polémico decreto sobre acceso a datos privados," Semana Económica, (2016). http://www.semana.com/nacion/articulo/consejo-de-estado-solo-la-fiscalia-podra-tener-acceso-a-datos-privados/465546

31 Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

32 Act 1621 of 2013, art. 44

communications.[33]

In contrast to other countries' data-retention mandates, the Mexican data-retention law provides a precise although expansive list of data that telecommunications companies are compelled to retain:

a) The name, business name or corporate name, and address of the subscriber;

b) The type of communication (voice transmissions, voicemail, conference, data), supplementary services (including call forwarding and transfers), or messenger or multimedia services used (including the services of short messaging, multimedia and advanced services);

c) The data necessary to track and identify the origin and destination of mobile communications: destination number and type of line service—lines with a contract or a flat rate plan, like the lines of prepaid credit;

d) The data necessary to determine the date, time and duration of the communication, as well as the messaging and multimedia service;

e) The date and time of the first service activation and localization tag (Cell ID);

f) When appropriate, the identification and technical characteristics of the device, including, among others, the international ID codes of the subscriber and the manufacturer of the device;

g) The digital location of the geographical position of the lines; and

h) All the data that have been generated since the date the first communication was produced.

The language in Article 190, Section III of the LFTR is highly ambiguous regarding the authorities who are entitled to access the retained data. This article authorizes the delivery of the retained data to "the requesting authorities referred to in Article 189 of this Law." Article 189 of the LFTR creates the obligation for telecommunications companies and online service, application, and content providers to comply with all "written requests that are well founded and justified by the competent authority," among which "security and law enforcement bodies" are mentioned without clearly establishing which authorities fit into those categories:[34]

[S]everal authorities have considered that Article 189 of the LFTR sufficiently

33 Second Chamber, Supreme Court, Amparo in Revision 964/2015.

34 Luis Fernando Garcia, "Mexico: State Communications Surveillance and the Protection of Fundamental Rights in Mexico," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/mexico

empowers them to use covert surveillance tools and that this power does not need to be detailed in any other law. For instance, the "Financial Intelligence Unit" of the Ministry of Finance and Public Credit is considered a "security body" pursuant to Article 189 and to an instrument that is not a formal or material law known as the "Guidelines for Collaboration."[35] *[...] Furthermore, there are reports that claim that authorities like the National Electoral Institute may have sent these types of requests in order to access the personal data of telecommunication services users.*[36]

Recently the Mexican Supreme Court[37] solved this problem by ruling that the Federal and State Prosecutors, the Federal Police, and the Center for Investigation and National Security (CISEN) are the only authorities entitled to access the retained data.[38]

CHILE: Article 222 of the Criminal Procedure Code (*Código Procesal Penal de Chile*) states that telecommunications providers must retain a list of their subscribers' IP addresses and connection logs for one year and make that data available to the Public Ministry. Providers who refuse to cooperate are punished.

Regulations controlling the interception and recording of telephone calls (*Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones*) do not require judicial authorization. Rather, they require the retained information to be available to public prosecutors and any other institution that is authorized by law to request it, without requiring specific judicial authorization for each interception or request.

ARGENTINA: In the 2009 *Halabi* decision, the Supreme Court declared a 2004 Act that sought to provide the government with ready access to telecommunications records unconstitutional. In February 2004 Act 25,873 modified the Telecommunications Act of 1972. It required telecommunications companies and service providers to establish technological and human resource measures that would allow for the remote observation of communications by the Judiciary or the Public Ministry (Article 1). It also required providers to create a 10-year registry of users that included information about communications traffic. The president suspended the law through Decree 357/05 after it

35 Agreement/016/2014 through which the Head of the Financial Intelligence Unit appoints the public servers mentioned herein for the purposes of the provisions established in Federal Telecommunications and Broadcasting Law in the Diario Oficial de la Federación (newspaper), art. 189, (2014).

36 Christine Murray and Joanna Zuckerman Bernstein, "Mexico Ramps up Surveillance to Fight Crime, but Controls Lax," Reuters, (2015). http://www.reuters.com/article/2015/10/12/us-mexico-surveillance-idUSKCN0S61WY20151012

37 Supreme Court. Second Chamber. Amparo in Revision 964/2015.

38 Luis Fernando Garcia, "Mexico: State Communications Surveillance and the Protection of Fundamental Rights in Mexico," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/mexico

faced criticism.[39]

Resolution 5/2013, Article 8 forces all telecommunications service providers to preserve all data gathered by their systems electronically for at least three years for quality assurance purposes only. However, under this article, law enforcement may request data in "partial or full delivery and store it for as long as it deems necessary."[40] Also, for quality assurance purposes, telecommunication providers must allow law enforcement "full access to their networks and information."[41] Finally, the *Ente Nacional de Comunicaciones* (ENACOM), with the purpose of meeting quality standards, may "request any information deemed necessary from telecommunications service providers."[42]

All these measures are disproportionate, as they grant ENACOM access to user data under a broad premise of "quality." Even further, there are no protections in place that prevent abusive actions by law enforcement authorities.[43]

PARAGUAY: Telecom regulator CONATEL issued a resolution that compelled companies to retain phone call and text messaging data for a six-month period for electronic commerce reasons. It clearly prohibits access to such data for any other purposes.

PERU: Decree 1182 compels local ISPs and telephone companies to retain communications and location details of the entire Peruvian population for a period of three years. The retained data could be accessible to law enforcement with a court order for possible use in the future.

Peruvians dubbed the decree #Leystalker ("Stalker Law"), which was meant to evoke an image of someone who uses technology to spy on a person's every movement online. The decree is very broad regarding the entities who are compelled to retain the data. It includes not only large and small Internet Service Providers (ISPs), but also any public entities that provide Internet access to end users, such as public schools, public libraries, airports and

39 Beatriz Busaniche, Breaking News About Data Retention, Electronic Frontier Foundation, https://www.eff.org/node/81911

40 Ministry of Federal Planning, Public Investment and Services, Department of Communication, Resolution 5/2013, (2013). http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

41 Ministry of Federal Planning, Public Investment and Services, Department of Communication, Resolution No 5/2013, art. 5, section 2, (2013), http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

42 Ministry of Federal Planning, Public Investment and Services, Department of Communication, Resolution No 5/2013, art. 3, (2013). http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm

43 Verónica Ferrari and Daniela Schnidrig, "State Communications Surveillance and the Protection of Fundamental Rights in Argentina," (2016). https://necessaryandproportionate.org/country-reports/argentina

other government entities. The decree does not specify the type of data that should be logged, the limitations on access and usage conditions, or the data security rules that should apply.

BRAZIL: Brazil is the only country in the region that has developed different data-retention rules depending on the kind of service: fixed line, mobile phones or Internet services.

Article 22 of the Fixed Telephone Service Regulation (ANATEL's Resolution 426/05) states that telecommunications companies must retain data related to the provision of services, including call logs, for a minimum of five years. The article does not describe specifically the type of data that should be retained, who can access it, and for what purposes.

Similarly, the Regulation on Personal Mobile Service (ANATEL's Resolution 477/07) requires fixed telecommunications providers to retain "at the disposal of ANATEL and other parties, tax documents (*documentos de natureza fiscal*) that contain data on incoming and outgoing calls, dates, time, duration and price, as well as account information of subscribers [...]" for a minimum of five years. It must make this information available to the National Telecommunications Agency and other interested parties:

> *[T]hat law requires legal entities to retain and keep billing/tax documents at the disposal of Brazil's Federal Revenue Department, for the period set forth in tax legislation to bring disputes to court (prazo decadencial), which is five years. Articles 42 and 58 also establish "the minimum amount of personal data" that users need to disclose in order to join a mobile telephone service (name, identity card number, and taxpayer number). In practice this makes registering for a mobile phone service dependent on a taxpayer number, which compromises anonymity.*
>
> *The rationale of the five-year data-retention obligation for telephone services, and justification of billing auditing and oversight by ANATEL, are outlined in Article 10, XXII of Resolução no. 477/07. However, both rules that establish data-retention obligations for fixed and mobile telephone service providers have long allowed for the convenience of keeping such records for the state's investigatory and prosecution purposes.*
>
> *Law no. 12.850/13 (Criminal Organizations Law), which requires telephone companies to retain data expressly to that end, dates back to only 2013. Moreover, provisions of these resoluções establish data-retention obligations even for services providing flat-rate plans, where a call's duration or the number dialed does not affect the amount a user pays. It is thus reasonable to suppose that ANATEL's data-retention regulations are used for purposes that go well beyond those associated with its responsibilities.*[44]

44 For a detailed analysis of the legal problems regarding data retention, see Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and

Article 53 of the Regulation of Multimedia Communication Services (ANATEL's Resolution 614/13) requires Internet service providers to retain subscriber records and account data for one year:

> *[T]he definition of connection logs is established in Article 4, XVII (the set of information referring to date and time of use of a connection to the Internet and a given IP address used at the terminal for incoming and outbound data packets, among other data that permit identification of the access terminal used). The shorter retention term compared to data-retention obligations for telephone services, as well as the clear description of what data need to be retained, might be attributed to the fact that the regulation was drafted while discussions on Law no. 12.965/14 (Marco Civil da Internet) were ongoing and to publicity concerning international decisions against data retention, which received particular attention from the academic community and civil society.*[45]

Several interpretations of the Criminal Organizations Law 12.850 of 2013 have led to confusion and have resulted in retained logs from phone companies being used for the purpose of identifying a person under criminal investigation.[46]

Article 17 of Law 12,850 of 2003 requires fixed and mobile phone providers to retain call records (*registros de identificação)* of the origin and destination of national and international calls for a period of five years, and make such records available to the Chief of Civil Police and the Attorney General's Office. Although this obligation is included in a law aimed at combatting criminal organizations, the law does not contain a provision that limits the use of the retained data for other types of criminal activities. The provision does specifies neither the type of data that should be logged, the limitations on access and usage conditions, nor the data security rules that should apply. This provision also states that the Chief of the Civil Police and the attorney general can access a defendant's account information without a judicial order. The constitutionality of this provision is being challenged through an *Ação Direta de Inconstitucionalidade* procedure, ADI 5063/DF, and is awaiting trial.[47]

---

the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/brazil

45 For a detailed analysis of the legal problems regarding data retention, see Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/brazil

46 For a detailed analysis of the legal problems regarding data retention, see Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/brazil

47 For a detailed analysis of the legal problems regarding data retention, see Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab

Article 15 of the same law allows the Chief of Civil Police and the Public Attorney's Office to get an accused's registration data (*dados cadastrais*) without a judicial authorization in order to "obtain information that uniquely informs the individual's qualifications, parents, and addresses retained by electoral courts, telephone companies, financial institutions, Internet providers, and credit card administrators."[48]

Article 21 criminalizes the refusal to provide "account information (*dados cadastrais*), logs, documents, and information requested by the judge, Public Attorney's Office, or the Chief of Civil Police during the course of the investigation or proceedings," and establishes penalties ranging from six months to two years of incarceration, plus a fine. According to the authors of the report State Surveillance of Communications in Brazil and the Protection of Fundamental Rights, these authorities have, without court orders, demanded companies' telephone logs and location data under the threat of punishment.[49]

Article 13 of the Marco Civil only requires operators of an "autonomous system" who provide Internet access to retain connection logs for one year. Here, "autonomous system" is a technical term that refers to those who administer specific IP address blocks and the corresponding autonomous system for routing purposes. This implies that the obligation to retain applies only to the largest ISPs and not to each entity that provides Internet access to end users, such as a school, library, café, or small local ISP that does not administer its own IP address blocks. Article 15 requires that commercial operators of Internet "applications" retain logs related to access to their own applications for a period of six months. Non-commercial operators of such applications may also be ordered by a court or public authority to retain such logs.

1.4 Monitoring the Spectrum or Mass Surveillance?

COLOMBIA: Law 1621, which regulates intelligence activities, contains a vague definition of communications surveillance, leaving a large margin for potential abuse:

> *[T]he intelligence and counterintelligence activities include the monitoring of the electromagnetic spectrum duly incorporated into operational orders or the work mission. The information collected under the monitoring of the electromagnetic spectrum in pursuit of the activities of intelligence and counterintelligence, that does not serve to fulfill the purposes set out in this Act, shall be destroyed and*

(2016). https://necessaryandproportionate.org/country-reports/brazil

48 Criminal Organizations Law 12.850 of 2013, art. 15. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

49 For a detailed analysis of the legal problems regarding data retention, see Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab (2016). https://necessaryandproportionate.org/country-reports/brazil

cannot be stored in intelligence or counterintelligence databases. Monitoring does not constitute interception of communications.

Intercepting mobile or fixed telephone private conversations and private data communications should be subject to the requirements of Article 15 of the Constitution and the Code of Criminal Procedure and may only be carried out within the framework of judicial proceedings.

The Constitutional Court of Colombia interpreted this vague language as authorization to allow intelligence agencies to monitor the entire electromagnetic spectrum,[50] without a judicial order regardless of the technological means employed.

Moreover, this provision does not explicitly authorize mass surveillance: under the case law that approved the new Intelligence Law, the Constitutional Court emphasizes that interception is only allowed during a criminal investigation and with judicial authorization. Under this law, intelligence agencies are allowed only to monitor the spectrum, which in theory is different from intercepting communications according to the Court. This law doesn't define what constitutes "monitoring the spectrum." But because Law 1621 clearly states that "monitoring does not constitute interception," a phrase that can be interpreted broadly, it's rather likely that the law can be used for that very purpose.

Indeed, this may have already occurred: over the past several years, without any apparent legal authorization, several mass surveillance programs have been devised. These programs are supposed to be rolled out through mechanisms such as the Unified Platform of Monitoring and Analysis [*Plataforma Única de Monitoreo y Análisis*] (*PUMA*) and the Comprehensive System of Digital Recording [*Sistema Integral de Grabación Digital, SIGD*].

Context

For a brief period starting in the early 2000's, Colombians were subject to surveillance under a platform called Esperanza, which was designed to spy on targeted telephone communications. In 2009 Colombians were shocked when they learned about the surveillance, and how intelligence agencies (DIPOL and DAS) had intercepted the telephone communications of journalists, political opposition parties, human rights activists, and even justices that had ruled under Alvaro Uribe's government.[51] This scandal led to the restructuring of the intelligence agencies, including the dismantling of the DAS.

50 European Commission, Scientific Committee, Technical Terminology – Glossary. http://ec.europa.eu/health/opinions/es/lamparas-bajo-consumo/glosario/def/espectro-electromagnetico.htm

51 Privacy International, "Shadow State: Surveillance, Law and Order in Colombia," (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

DAS members were prosecuted under the crime of illegal interception.[52]

In addition to Esperanza, there is a communications interception program called PUMA that was purchased in 2007 and is administrated by the Directorate of Criminal Investigation and Interpol (DIJIN)—the criminalistics branch of the police.[53] With the aim of collecting and registering personal information that concerns criminal investigations, this platform is connected directly to the Internet backbone and has the capability to mass surveil Internet and telephone traffic.[54]

The DIPOL (classified as an intelligence agency) has operated its own surveillance program since 2005: *The Integrated Recording System of the Directorate of Police Intelligence* is a program that combines biometric data, social media public records and other available data to create profiles.[55]

According to Article 43 of the Intelligence Law, intelligence agencies are able to access records belonging to the judicial police for reasons of national security. Still, such actions must be in accordance with the Colombian human rights legal framework. This means that these agencies could actually gain access to the data intercepted by PUMA and Esperanza, since they're currently managed by the Colombian judicial police.[56]

The Public Prosecutor's Office has questioned the legality of these tools. It believes that increasing the interception capacity of PUMA (by adding up to 20,000 telephone lines more than they have now) "may violate privacy rights."[57] In the same interview General Prosecutor Eduardo Montealegre told Colombian newspaper, El Tiempo:

> *[I]t may lead to the indiscriminate use of interception tools in cases where such an*

52 Privacy International, "Shadow State: Surveillance, Law and Order in Colombia," (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

53 Privacy International. "Shadow State: Surveillance, Law and Order in Colombia." (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

54 Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

55 Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

56 Colombia, Law 1621 of 2013, art. 43, http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

57 "Fiscalía le dice 'no' a sistema de interceptación 'Puma' de la Policía" [General Prosecutor Says 'No' to Police's 'Puma' Interception System], El Tiempo, (2014), http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

invasion of privacy is not even necessary to the investigation and to fight against crime [...] No other government agency (other than the Prosecutor's Office) is empowered to order the interception of communications or manage the equipment used for this. That all people have a right to intimacy and privacy is a legitimate guarantee.

Last year, one particular email from the Hacking Team leaks suggested that the US Drug Enforcement Agency was conducting mass surveillance on Colombia by installing equipment in the US Embassy in Colombia "that would receive all the traffic from Colombians ISPs."[58]

1.5 Imprecise Intelligence Laws Are Prone to Abuse

ARGENTINA: The regulatory framework for intelligence activities includes Law 25,520 on National Intelligence,[59] passed in 2001, and Law 27,126, passed recently, both of which substantially amended the previous law.[60] These laws require Argentina's intelligence system to function in strict accordance with the provisions of the National Constitution and the legal and regulatory norms in force. However, the intelligence regulatory framework allows for discretionary activities by the State. For instance, the national intelligence law establishes that the "highest authority" in each agency of the intelligence system is in charge of ordering surveillance activities.[61] However, the law also indicates that in "states of emergency," these activities may be initiated by others, provided they are immediately reported to the highest authorities. The fact that there is no exhaustive definition of "state of emergency" means that activities infringing upon fundamental rights may occur. This situation is only made worse by the lack of adequate oversight of intelligence activities.

From the Legality Principle perspective, a decree issued by the Presidency called the New Doctrine of National Intelligence *(Nueva Doctrina de Inteligenica Nacional)* is also questionable. Its purpose is to set the new objectives and tasks of the newly created Federal Intelligence Agency in the context of the reorganization of intelligence services in the country. As mentioned above, this new doctrine stems from a decree issued by the executive

58 Ryan Gallagher, "Hacking Team Emails Expose Proposed Death Squad Deal, Secret UK Sales Push and Much More," The Intercept, (2015). https://theintercept.com/2015/07/08/hacking-team-emails-exposed-death-squad-uk-spying/ See also Hacking Team email leak. https://www.documentcloud.org/documents/2160947-dea-amp-hacking-team-surveillance-in-colombia.html

59 Argentina, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001.

60 Argentina, Republic, Law No. 27,126 on the creation of the Federal Intelligence Agency, Official Journal of March 5, 2015.

61 Argentina, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, art. 5.

power and, as such, it was neither discussed in Congress, nor publicly debated. This new doctrine broadens the definitions of "attacks against the constitutional order." This may be problematic in terms of legality, since the definitions are rather vague.[62] It should be noted that the new administration which entered office in December, 2015, has issued several regulations which modify the previous framework. Even though the administration stands at the opposite end of the ideological spectrum of the previous government, it has not expressly revoked the New Doctrine of National Intelligence nor has it replaced it with a similar document stating purposes. However, the new administration did do away with oversight mechanisms which the previous government had created towards the end of its term.[63]

COLOMBIA: Law 1621 of 2013 regulates intelligence and counterintelligence activities. The law does not precisely define the purposes for which intelligence activities are legal (as discussed below with respect to legitimate aim). In addition this law gives the executive branch the power to issue decrees that set the parameters for the declassification of information.[64] Furthermore, judges may not be granted access to classified information if it poses a threat to national security (this is at the discretion of the intelligence agencies).[65] The Constitutional Court of Colombia endorsed this delegation of power, arguing that in all cases the law provides clear criteria on which to base the regulations.[66] Thus, having been delegated the power to alter the levels of classification, the executive branch is empowered to define the criteria used to classify intelligence information. The intelligence and counterintelligence agencies are in charge of applying such criteria in concrete cases.[67] However, the confidentiality of information, whenever it represents a limitation of the right to access information, should be clearly defined by a formal law, pursuant to the Legality Principle, not left to executive discretion.[68]

BRAZIL: Law 9,883 of 1999 created the Brazilian Intelligence System *(SISBIN)*, which involves different state agencies, including its principal body, the Brazilian Intelligence Agency *(ABIN)*.[69] *ABIN* is in charge of planning, executing, monitoring, and overseeing intelligence activities. As such, it has access to information obtained by other Brazilian

62 Argentina, Decree No. 1311/15, Official Journal of July 6, 2015, Annex 1.

63 On this point, see ADC. Ciberseguridad en la era de la vigilancia masiva. (2016). https://adcdigital.org.ar/wp-content/uploads/2016/06/ciberseguridad-argentina-ADC.pdf

64 Colombia, Law 1621 of 2013, art. 37.

65 Colombia, Law 1621 of 2013, art. 34.

66 Colombia, Constitutional Court, sentence C-540 of 2012.

67 The Colombian government established regulations on the levels of classification of intelligence and counterintelligence information through Decree 857 of 2014.

68 Colombia, Law 172 of 2014.

69 Abstract of the Brazilian surveillance report. For an in-depth analysis see Dennys Antonialli, Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

authorities through *SISBIN*.

It is not clear how the exchange of information between *SISBIN* and *ABIN* occurs.[70] The law does not specify an exchange, and there are no transparency mechanisms set in place that would allow the public to monitor the process. For instance, *ABIN* does not have the power to intercept communications, because neither the Constitution of Brazil nor the law on interceptions empower it to do so. However, *ABIN* may be able to get data obtained by communications interception through a mechanism of cooperation with other State entities.[71] In 2008, *Folha de São Paulo* disclosed that *ABIN* has indirect access to intercepted communications from the Federal Police System *(Guardião)*.[72] Also, if Brazil's Federal Revenue Department holds billing documents of telephone companies in its database, *ABIN* would have access to users' telephone logs.

MEXICO: The National Security Law authorizes the Center of Investigation and National Security *(CISEN)* to intercept private communications if an "imminent threat to national security" exists.[73] "Threats to national security" are broadly defined in Article 5 of the National Security Law, which can be used to target foreign international NGOs involved in privacy activism. The text reads:

1. Actions aimed at carrying out espionage, sabotage, terrorism, revolt, treason, or genocide against the United Mexican States within its national territory;

2. Actions of foreign interference with national issues that may have a negative impact on the Mexican State;

3. Actions disabling authorities to take action against organized crime;

4. Actions aimed at disrupting the unity of the Federation, described in Article 43 of the Political Constitution of the United Mexican States;

5. Actions aimed at hindering or obstructing military or navy operations against organized crime;

6. Actions against aviation security;

---

70 Abstract of the Brazilian surveillance report. For an in-depth analysis see Dennys Antonialli, Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

71 Brazil, Judge Adilson Vieria Macabul, Supreme Court of Justice, habeas corpus 149250-SP, (2012). http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

72 Folha de São Paulo, "Access to the Guardian by the Abin Causes Controversy," (2008). http://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm

73 Mexico, National Security Law. Articles 33 - 49.

7. Attacks against diplomats;
8. Actions aimed at carrying out illegal trafficking of nuclear materials, chemical weapons, bioweapons, and conventional weapons of mass destruction;
9. Actions against maritime navigation;
10. Actions financing terrorist practices or organizations;
11. Actions aimed at hindering or obstructing intelligence or counterintelligence activities, and;
12. Actions aimed at destroying or disabling the strategic or needed infrastructure for the provision of public goods and services.[74]

1.6 No Precise Legal Authority to Use Malicious Software, Cell-site Simulators, or Other New Spying Technologies

New technologies have raised legal questions about the circumstances under which Latin Americans can expect their data to be safe from access by government surveillance. At one point in time, "communications surveillance" consisted almost exclusively of wiretapping—the listening to and/or recording of telephonic communications. Thus, many of the laws governing electronic surveillance remain focused on wiretapping. They rarely refer to any of the more recent technological advancements in either electronic communications—such as the Internet—or surveillance techniques.

One of the more common techniques that are significantly different from wiretapping is the use of malware to infect a person's computer and gain access to the communications stored on and passed through it. Another is the use of IMSI-catchers, which are devices that mimic cell phone towers and are capable of detecting the presence of mobile devices and intercepting calls made in a geographic area. Like wiretapping, these technologies are invasive and surreptitious, but also raise far different privacy concerns and legal questions than traditional wiretapping.

These and other developments mean that the term "communications surveillance" encompasses a much larger range of techniques and activities today than it did at the time wiretapping laws were written. This can include a range of other new technical means and data sources that are used to interfere with communications privacy, like location tracking, IP address logs, government hacking and malware, and attacks against mobile phones. Older legislation often maintains strict distinctions among different categories of protected (or unprotected) information, even when new information sources and analysis techniques can readily be used to make sensitive inferences about individuals and groups.

74 Argentina, National Security Law, art. 5.

Recognizing the broad scope of today's surveillance landscape, an international group of experts, of which EFF was a part, proposes to define communications surveillance to include "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."[75] However, the laws that are used to authorize such new spying technologies in Latin America are outdated or were crafted piecemeal, and the various legislatures in the region have not, for the most part, carefully considered when, and under what circumstances, new techniques should be used, if at all. Therefore, new spying techniques may be adopted with minimal legal oversight based on explicit or implicit interpretations that exempt them from privacy controls or indicate that the data they obtain is not fully protected.

We've found that many Latin American states acquire new spying technologies under such legislation. This includes the purchase of malicious software. The Citizen Lab and Canada Centre for Global Security Studies Munk School of Global Affairs revealed the existence of command and control servers from FinSpy, Gamma International's FinFisher remote intrusion surveillance software, in several countries including Mexico[76] and Panama in 2013,[77] and Venezuela and Paraguay in 2015.[78] This spyware is developed by German-based Gamma International, and marketed and sold to law enforcement and intelligence agencies by the UK-based Gamma Group.[79]

---

75 Necessary and Proportionate Coalition, Necessary & Proportionate, (2014). http://necessaryandproportionate.org/principles; Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (2014). http://necessaryandproportionate.org/global-legal-analysis

76 Bill Marzcak, Claudio Guarnieri, John Scott-Railton, and Morgan Marquis-Boire, "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab and Canada Centre for Global Security Studies Munk School of Global Affairs, University of Toronto, (2013). https://citizenlab.org/wp-content/uploads/2009/10/You-Only-Click-Twice-FinFisher's-Global-Proliferation.pdf

77 Morgan Marquis-Boire et al., "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab and Canada Centre for Global Security Studies Munk School of Global Affairs, University of Toronto, (2013). https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

78 Adam Senft, Bill Marczak, Irene Poetranto, John Scott-Railton, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," Citizen Lab and Canada Centre for Global Security Studies Munk School of Global Affairs, University of Toronto, (2015). https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

79 Bill Marzcak, Claudio Guarnieri, John Scott-Railton, and Morgan Marquis-Boire, "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab and Canada Centre for Global Security Studies Munk School of Global Affairs, University of Toronto, (2013). https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

New insights into the wider market of surveillance technologies were also revealed by two important leaks. The first leak, pertaining to Finfisher/FinSpy, was revealed in August 2014.[80] Forty gigabytes of internal data were published, including release notes, price lists, and source code. The second leak, pertaining to the notorious Italy-based spyware vendor Hacking Team, was published in July 2015. Attackers compromised the company's servers and released over 400 GB of internal data and communications with clients. The documents revealed that Brazil, Colombia, Chile, Ecuador, Honduras, Mexico, and Panama purchased licenses for Hacking Team's remote control system.[81] The leaks also revealed that Argentina, Guatemala, Paraguay, Peru, Uruguay, and Venezuela had started negotiating with Hacking Team. However, the leaks did not reveal if any of those countries actually made any purchases.[82]

The use of these surreptitious and intrusive technologies should not occur without specific legal authorization and is permitted only if there is no less invasive way to obtain the information. A statement by the Organization for American States' Office of the Special Rapporteur for Freedom of Expression declared:

> *[A]ccording to international standards, the use of programs or systems for the surveillance of private communications should be clearly and precisely established by law, genuinely exceptional and selective, and must be strictly limited to the needs to meet compelling objectives such as the investigation of serious crime as defined in legislation. Such restrictions must be strictly proportionate and consistent with the international standards of the right to freedom of expression. This Office has stated that the surveillance of communications and the interference in privacy that exceeds what is stipulated by law, which are oriented to aims that differ from those that the law permits or are carried out clandestinely, must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media.*[83]

---

80 Joseph Cox, "A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher," (2014). http://motherboard.vice.com/read/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher

81 Gisela Perez de Acha, "Hacking Team malware para la vigilancia en America Latina," Derechos Digitales, (2016). https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf. See also Juan Diego Castañeda, "When the State "Hacks," An Analysis of the Legitimacy of the Use of Hacking in Colombia," Fundación Karisma, (2015). https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf

82 Gisela Perez de Acha, "Hacking Team malware para la vigilancia en America Latina," Derechos Digitales, (2016). https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf. See also Juan Diego Castañeda, "When the State "Hacks," An Analysis of the Legitimacy of the Use of Hacking in Colombia," Fundación Karisma, (2015). https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf

By comparing the domestic laws in the surveyed countries, we learned:

1. In Chile, Paraguay, Guatemala, Honduras, and Uruguay, large legal loopholes exist and can be interpreted as authorizing the use of any kind of existing or future surveillance technology, such as malware or IMSI catchers, or any technology still to be developed;

2. Even though many of the States studied in this report have purchased malicious software, there exist no specific legal provisions that authorize government authorities to use malicious software or IMSI catchers in any of the 13 surveyed countries;

3. In at least one of the countries surveyed, government authorities and state-owned companies have illegally purchased surveillance tools, including malware, even though they do not have constitutional or legal authorization to conduct surveillance; and

4. Mexico has used malicious software to target political opposition parties and journalists.

The following examples highlight concerning practices in the region.

MEXICO: Mexico does not have any law that precisely authorizes the use of malware. Recent leaks revealed that Mexico is Hacking Team's top client.[84] Even worse, it was revealed that governors from the states Querétaro, Puebla, Campeche, Tamaulipas, Yucatán, Durango, and Jalisco purchased and stockpiled powerful malware designed to attack personal computers and phones despite not having the legal authority to conduct surveillance of any kind. Likewise, Mexican state-owned oil company PEMEX *(Petróleos Mexicanos*) was also identified as a customer of Hacking Team's.[85] Authorities that have the power to intercept private communications in Mexico are the Public Prosecutor's Office

83 Special Rapporteur for Freedom of Expression, "The Office of the Special Rapporteur Expresses Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere," (2005). http://www.oas.org/en/iachr/expression/showarticle.asp?

84 Arturo Angel, "Mexico, the main client of a company that sells software to spy." Animal Político, (2015). http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

85 Daniel Hernandez and Gabriela Gorbea, Mexico Is Hacking Team's Biggest Paying Client — By Far, VICE, https://news.vice.com/article/mexico-is-hacking-teams-biggest-paying-client-by-far, Sebastián Barragán, "Equipo de espionaje en México: sin control legal suficiente ni transparencia", Aristegui Noticias, (2016). http://aristeguinoticias.com/1804/mexico/equipo-de-espionaje-en-mexico-sin-control-legal-suficiente-ni-transparencia/, PEMEX, Mexican intelligence and governments, outed as clients of spy company, El Universal, http://www.eluniversal.com.mx/articulo/english/2015/07/6/pemex-mexican-intelligence-and-governments-outed-clients-spy-company

(Public Attorney's Office) plus the Procurators' Offices/Prosecution Offices of the 31 federative organizations and the Federal District, the National Security Commission (Federal Police), and the Center for Investigations and National Security (Executive Branch).[86]

Adding insult to injury, the government of Puebla used Hacking Team's malicious software to spy illegally on political opponents—including the National Action Party (*Partido Acción Nacional, PAN*)—in 2014. In addition the governor of Puebla conducted surveillance in 2013 during State elections when mayoral and congressional posts were being appointed. He also spied on academics, journalists, and political opponents during Puebla's last federal election.[87]

COLOMBIA: Colombia does not have any laws that precisely authorize the use of malware.[88] Yet the Hacking Team leaks revealed that the Colombian National Police acquired Hacking Team's Galileo software for use between 2013 and 2016.[89] The police previously denied any association with Hacking Team, but the leak showed that the police indeed purchased the malware through an intermediary, Robotec.[90] In response to the leaks, the Colombian police stated that they had no relationship with Hacking Team, but with Robotec, and that "the purpose of this purchase was to enable the ability to detect threats of terrorism and organized crime in Cyberspace."[91]

In 2015, Vicky Davila, a journalist who reports on police corruption, uncovered a sex scandal that was deeply rooted in the Colombian police system and involved several high-ranking police officers.[92] After the scandal broke, Ms. Davila claimed that her work devices, and

86 Luis Fernando Garcia, "Mexico: State Communications Surveillance and the Protection of Fundamental Rights in Mexico," Electronic Frontier Foundation & R3D.mx (2016). https://necessaryandproportionate.org/country-reports/mexico

87 Ernesto Aroche, "El gobierno de Puebla usó el software de Hacking Team para espionaje político," Animal Politico, (2015). http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

88 Carolina Botero and Pilar Sáenz, "In Colombia, PUMA is Not What it Seems," Digital Rights Latin America & The Caribbean, (2015). http://www.digitalrightslac.net/en/en-colombia-el-puma-no-es-como-lo-pintan/

89 Privacy International, "Shadow State: Surveillance, Law and Order in Colombia," (2015). https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

90 For a more in depth research see, Juan Diego Castañeda, "When the State "Hacks," An Analysis of the Legitimacy of the Use of Hacking in Colombia," Fundación Karisma, 2015. https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf

91 Semana, Cuando hackean a los hackers, http://www.semana.com/nacion/articulo/los-lios-de-hacking-team-por-informacion-hackeada/434391-3, Diana Carolina Durán Núñez, El software espía de la Policía, El Espectador, July 2015, http://www.elespectador.com/noticias/investigacion/el-software-espia-de-policia-articulo-571980

92 El Tiempo, "Las investigaciones pendientes en el escándalo de la Policía," (2016). See also Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the

those of her coworkers, became infected with malware.[93]

ARGENTINA: Argentina does not have any laws that precisely authorize the use of malware.[94] Argentina's legislation allows only for the interception of communications when there's a warrant issued by a judge and for a period of no more than 30 days. The Criminal Procedure Code establishes that communications can be intercepted to investigate a crime, but only under the principles of necessity, proportionality, reasonability, and adequacy.[95]

Based on publicly available information, there is no evidence that Argentina purchased products from Hacking Team. However, leaks revealed that the Argentinean government contacted Hacking Team on several occasions, and the Italian company presented its products to the Ministry of National Security, the National Criminal Intelligence Directorate, the Public Prosecutor, and the Complex Investigations Unit, among others.[96] As of now, the Argentinean government has not issued an official statement acknowledging or denying these meetings.

There are some anecdotal indications that malware has been used in Argentina. Attorney Alberto Nisman was a federal prosecutor known in the country for investigating Argentina's deadliest bombing, a 1994 attack in Buenos Aires on a Jewish Center, which, to this day, remains unsolved. In 2015 Nisman was found dead in his home, and, according to a technical analysis, malware was found on Nisman's phone.

However, because the malware was meant for Nisman's computer, the phone was not

---

Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

93 Fundación Karisma, "El tal 'hackeo' sí existe," (2015). https://karisma.org.co/el-tal-hackeo-si-existe/

94 For a more in-depth research, read Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/argentina

95 Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/argentina

96 Hacking Team, Meetings in Argentina, https://wikileaks.org/hackingteam/emails/emailid/587154, and Report onArgentina, https://wikileaks.org/hackingteam/emails/emailid/765194, and Report on Argentina, visit with final agenda attached, https://wikileaks.org/hackingteam/emails/emailid/596983 See also, Asociación por los Derechos Civiles, La ADC alerta: software de interceptación y vulneración a los derechos humanos, (2015). https://adcdigital.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf

infected.[97] The expert who analyzed the malware on Nisman's phone concluded that whoever was behind the malware attack was the same person who conducted surveillance on the independent Argentinean journalist, Jorge Lanata, due to the common characteristics in the software that was being deployed in both instances. While there is a strong indication that a government actor was behind these attacks, there has been no direct attribution to a particular government as of this time.[98]

HONDURAS: Honduras has a specific law that regulates the interception of private communications.[99] Under this law, communications interception may be carried out by way of "special investigative techniques." This definition is so broadly defined that one could interpret it as authorizing the use of malware and perhaps any other surveillance technology:

> *[I]t is a special investigative technique that involves the process through which an authority accesses, captures, records, stores, retains or monitors, without the consent of the participants, a communication that was made by transmission, emission, or reception of signs, symbols, written signs, images, sounds, emails or information of any nature or wire, radio electricity, optical or other means, electromagnetic systems, telephony [...] information technology or telematics or similar or analogous natures, as well as the communication that takes place through any means or transmission type.*[100]

The only authorized governmental agencies who can request a warrant from a judge to intercept communications are the Public Ministry, the National Police, and the Attorney General's Office (Article 7). The only governmental body authorized to intercept communications is the Unit of the Intercepting of Communications (*Unidad de*

97 Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/argentina

98 Morgan Marquis-Boire, "Inside The Spyware Campaign Against Argentine Troublemakers," The Intercept, (2015). https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/ See also Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/argentina

99 For an in-depth analysis of surveillance law in Honduras, read Fundación Acceso "¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utiizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos," 2015. http://acceso.or.cr/files/investigacion-resumen-ejecutivo.pdf

100 Honduras, Ley de intervenciones de las comunicaciones, section 3, no. 11. http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas%20(8,2mb).pdf

Interceptación de Comunicaciones).

The National Intelligence Law (*Ley de Inteligencia Nacional*) authorizes the *Dirección Nacional de Investigación e Inteligencia* (DNII) to carry out surveillance for the purposes of protecting the rights of citizens and national security.

In 2014 Honduras' intelligence agency, DNII, acquired Galileo software from Hacking Team.[101]

BRAZIL: There are no specific regulations on government hacking in Brazil. However, Article 158 of Law 13.097 does allow authorities to avoid public bidding. This means that authorities do not need to publicly disclose whether they have purchased surveillance technology that will be used in police investigations.[102]

In May 2015 Brazil Federal Police purchased Hacking Team's RCS software through an intermediary company, YasniTech.[103] The Brazilian agency paid 75 thousand reals to the intermediary, and Yasnitech paid Hacking Team 25 thousand euros for a three-month trial of the software.[104] According to the Hacking Team leaks, a judge authorized the Federal Police to use a "special application to collect data from telephones under investigation" for 15 days.[105] The Brazilian Federal Police neither confirmed nor denied the agreement with Hacking Team.[106]

---

101 Gisela Perez de Acha, "Hacking Team malware para la vigilancia en America Latina," Derechos Digitales, (2016). https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf.

102 Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

103 See Hacking Team's client list: https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/5%20-%20Analisi%20Fatturato/2015/Customer%20History.xlsx See also Re: Brazil - POCs and Demos - Feedback first meeting with Civil Police - SP Department of intelligence: https://www.wikileaks.org/hackingteam/emails/emailid/440130

104 *See* Hacking Team's Leaked Invoice: https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/1%20-%20Commesse/5%20-%20Commesse%202015/Commessa013.2015%20Yasnitech.xls

105 Felipe Ventura, The References To Brazil In Leaked Emails Of Hacking Team, July 10, 2015, http://m.gizmodo.uol.com.br/brasil-e-hacking-teamSee also Natalia Viana, Hacking Brasil, http://apublica.org/2015/07/hackeando-o-brasil/Dennys Antonialli, Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

106 Redação Linha Defensiva, "PF was to close espionage million dollar contract," Linha Defensiva, (2015).http://www.linhadefensiva.org/2015/07/pf-estava-para-fechar-contrato-milionario-de-espionagem/

PARAGUAY: There are no specific regulations on government hacking in Paraguay. However, Article 200 of the Criminal Procedural Code contains a large legal loophole that can be interpreted as authorizing any kind of surveillance technology and techniques. This provision establishes that a judge can order the interception of the communications of any accused persons, "regardless of the technical means used" to achieve it.

According to research conducted by ABC Color, a Paraguayan newspaper, the National Anti-Drug Secretariat (SENAD) purchased FinFisher in November 2012. ABC Color revealed the receipt of purchase, as well as a record of the delivery of the system.[107] In May 2016, two weeks after the release of the report, *State Communications Surveillance and the Protection of Fundamental Rights in Paraguay* by EFF and TEDIC, [108] the Minister of SENAD referenced the report's findings and finally confirmed that Paraguay did indeed purchase the malicious software in 2012. The Minister claims that the software is used as a "security system for location tracking *(georeferenciamiento)*."[109]

GUATEMALA: Guatemala's legislation also provides an astoundingly broad power that can be interpreted as authorizing any kind of surveillance technology and techniques. Article 48 of the Law Against Organized Crime provides that any communication that is oral, written, carried out on the telephone, radio, or on software that uses the electromagnetic spectrum, as well as "any other means" that exist in the future, can be intercepted, recorded, and reproduced with judicial authorization.

The Hacking Team leaks revealed the government of Guatemala was in conversation with Hacking Team, though no evidence of an actual purchase was disclosed.

URUGUAY: Article 5 of Law 18.494 on the Control and Prevention of Money Laundering and Financing of Terrorism Surveillance authorizes the use of any technological means available for the investigation of any offense to facilitate clarification. A broad interpretation of the rule essentially authorizes various types of surveillance techniques and technologies such as malware or IMSI-catchers. The law does not designate an express, clear, and precise legal authority—something that is necessary in order to comply with the Organization of

---

107 ABC Color, Senad gastó casi G. 200 millones solo en "montaje y configuración," (2013). http://www.abc.com.py/edicion-impresa/judiciales-y-policiales/senad-gasto-casi-g-200-millones-solo-en-montaje-y-configuracion-590062.html?fb_comment_id=419236824858112_2094744#f1c83727667f9fc

108 Jorge Rolón Luna and Maricarmen Sequera, "State Communication Surveillance and the Protection of Fundamental Rights in Paraguay," Electronic Frontier Foundation & TEDIC, (2016). https://necessaryandproportionate.org/country-reports/paraguay

109 TEDIC, "Más preguntas y dudas sobre software malicioso adquirido por SENAD," (2016). https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/

American States' international human rights standards.[110]

110 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: State Surveillance of Communications and the Protection of Fundamental Rights in Uruguay," Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/uruguay

2.
Legitimate Aim

This Principle states that laws should only permit specified State authorities to conduct communications surveillance with 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.

Our analysis of the legal frameworks for conducting surveillance in the countries studied makes clear that communications surveillance is acceptable as a legitimate aim if it is conducted for evidentiary purposes, the investigation of a serious crime, or national security. However, digital surveillance is a powerful temptation for investigators and police officers. To prevent misuse, the law must specify the situations in which it serves a truly legitimate aim. The Legitimate Aim Principle should also be applied when a judge has been requested to authorize a specific surveillance measure.

Legitimate Aim, as defined by the International Principles on the Application of Human Rights to Communications Surveillance, is founded on a high standard established by the German Constitutional Court in 2008:[111]

> *[I]n particular, the German Constitutional Court has ruled that deeply intrusive measures such as a search of a computer by law enforcement agencies cannot be justified merely by reference to some vaguely defined general interest. The German Constitutional Court held that such a measure had to be justified on the basis of evidence that there is "a concrete threat to an important legally protected interest," such as a threat to the "life, limb or liberty of a person" or to "public goods, the endangering of which threatens the very basis or existence of the state, or the fundamental prerequisites of human existence."*[112]

The best practices in this area involve surveillance legislation that contains exhaustive lists of specific crimes (or some other clear and objective definition) and other legal constraints to ensure no human rights violations occur.

Although the Legitimate Aim Principle requires that any act of communications surveillance must have a legitimate aim, the following section only explores which

111 Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (2014). http://necessaryandproportionate.org/global-legal-analysis

112 Dictum in the Constitutional Court Judgment of 27 February, 2008 (1 BvR 370/07 and 1 BvR 595/07).

governmental aims are in fact "legitimate" and the extent to which the laws governing communications surveillance in the region incorporate this principle.

Most of the countries that were surveyed have laws that limit surveillance practices to serious crimes, but in many cases the laws fail to adequately specify which crimes fall under this category. Terms, such as "terrorism" and "cybercrime" that appear in many of the region's laws are so vaguely defined that most of the invasive surveillance techniques can be applied beyond their legitimate aim.

In accordance with this concern, the UN Special Rapporteur on the Right to Freedom of Expression and Opinion, called attention to the vague and nondescript term "national security," which is so often seen in legislation governing communications surveillance:

> *60. The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists, or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.*[113]

When it comes to legislation governing surveillance for intelligence purposes, several nation States define specific legitimate aims—a practice that should be more widely adopted. All States should follow the lead of those who expressly prohibit the use of intelligence surveillance 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.

2.1 Legitimate Aim Constraints

It is a good practice for States to limit the offenses for which the use of surveillance may be authorized. Four examples follow:

NICARAGUA: Articles 213 and 214 of the Criminal Procedural Code limit the interception of communications to a detailed list of serious crimes. These include terrorism, kidnapping, drug-related crimes, money laundering, and international weapons trafficking.[114]

---

113 Frank La Rue, Special Rapporteur on the Right to Freedom of Expression and Opinion, A/HRC/23/40, (2013, para. 58). http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

114 Nicaragua, Procedural Penal Code 406, (2001), and La Gaceta 243 y 244, (2001). http://legislacion.asamblea.gob.ni/Normaweb.nsf/%28$All%29/5EB5F629016016CE062571A1004F7C62

GUATEMALA: The Law Against Organized Crime limits communications interception to cases where the prevention or investigation of a crime is necessary. These include specified organized crimes and offenses that have major social impact.[115]

PERU: Pursuant to criminal law, judicial authorities can authorize a prosecutor to take control of those communications under preliminary or jurisdictional investigation, and for a specific list of offenses. These include kidnapping, trafficking, child pornography, aggravated robbery, extortion, drug trafficking, crimes against humanity, violations of national security and treason, embezzlement, corruption, terrorism, tax and customs offenses, money laundering, and cybercrime.[116]

BRAZIL: Law 9,296 of 1996 allows communications to be intercepted for purposes of a criminal investigation or discovery in a criminal proceeding by court order, *ex-officio,* or upon request of a law enforcement official or the Public Attorney's Office.[117] The interception of communications is prohibited in cases where there is no reasonable evidence of criminal responsibility or conspiracy to commit a crime, where evidence can be obtained by other means, or where the suspect, if convicted, faces no more than a detention-type sentence (*detenção),* which is common for misdemeanors.

2.2 Some Latin American Surveillance Laws Incorporate Some Aspects of the Legitimate Aim Principle but Fail to Satisfy It Completely

Instead of restricting intrusive surveillance measures to certain crimes, some States deal with their authorization differently according to the type of offense that is being investigated.

ARGENTINA: Argentina's legal framework permits communications interception to occur only if it is proved to be useful for combatting a crime. However, it does not specify the severity of the crime:

> *[I]n principle, the Argentinian law that provides for the interception of communications complies with this requirement, since it establishes that interceptions must be conducted in exceptional circumstances, with an aim to prove the commission of a crime or to protect national defense and domestic security.*[118]

115 Guatemala, Ministry of Interior, Law Against Organized Crime, art. 48, (2006). http://leydeguatemala.com/ley-contra-la-delincuencia-organizada/interceptaciones/10468/

116 Peru, Law 27697, Penal Code and Procedural Penal Code.

117 Brazil, Law 9,296, art. 3, (1996).

118 Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016).

CHILE: Chile's legal framework imposes fewer restrictions on surveillance involving terrorism and drug trafficking than it does on surveillance involving common crimes.[119] Compounding this problem, "terrorism" remains vaguely defined in the law. This allows judges to apply the rules established in the Terrorism Act at their discretion. In contrast, more protective provisions apply to surveillance carried out for the investigation of common crimes. In fact, for the investigations of common crimes—ones that would result in less than five years of imprisonment—no surveillance may be conducted:

> *[O]ne common critique of the [Terrorism Act] is that it defines "terrorist acts" in a vague and unclear manner[120] [...] Moreover, since acts classified as "terrorist acts" are especially dangerous, the law is lax when it comes to setting standards for telephone communications and other types of communications interception. It removes several of the requirements established in the Criminal Procedure Code, and forbids only the interception of the communications between the accused and his or her lawyer.*[121]

Indeed, the UN Office of the High Commissioner for Human Rights points out that subjective, arbitrary, and/or political considerations have played a role in the selection of cases where anti-terrorism legislation has been applied:

> *[T]he various justifications put forward have been subjective and lacking in legal rigor. A comparison of the cases that have been charged as terrorism with those that have not demonstrates this. It is impossible to distinguish any clear and consistent dividing line between cases that have been charged as common criminal offenses (such as arson, murder and firearms offenses) from those in which the counter-terrorism legislation has been invoked in order to aggravate the sentence and provide additional procedural advantages to the prosecutor. The Special Rapporteur reluctantly concludes that subjective, arbitrary and/or political considerations have played a role in the selection of those cases in which the anti-terrorism legislation is*

---

https://necessaryandproportionate.org/country-reports/argentina

119 *See* Law 18.314, which determines terrorist conducts, Law 20.000, which sanctions the illicit trafficking of narcotics and psychotropic substances, and the Criminal Procedure Code, art. 222

120 National Institute for Human Rights of Chile (INDH, in Spanish.) "Report on Issues to Consider in the Amendment of the Antiterrorism Law in Light of the Observation of Cases by the National institute for Human Rights." Passed by the Council of the National Institute for Human Rights on July 22, 2014. pp. 4-7. http://bibliotecadigital.indh.cl/bitstream/handle/123456789/655/Informe%20Ley%20Antiterrorista.pdf?sequence=1

121 Valentina Hernández and Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," Derechos Digitales and Electronic Frontier Foundation (2016). https://necessaryandproportionate.org/country-reports/chile

invoked.[122]

COLOMBIA: Although there is not a specific list of crimes to which communications interception is limited, the criminal procedural law authorizes communications interception only for the purpose of collecting evidence in criminal investigations. Pursuant to Article 222 of the Criminal Procedural Code, the judge shall, at the request of the public prosecutor, allow for the interception and recording of communications in criminal proceedings if a person has committed or participated in the preparation or commission of a crime, or if he or she is facing an associated penalty of at least five years and one day in prison.

In the intelligence context, Law 1621 of 2013 lists the aims to which intelligence and counterintelligence activities must be confined, but it fails to define them adequately. Specifically, Article 4 sets forth the following as legitimate aims:

a) To ensure the attainment of the State's essential aims, the life of the democratic regime, national integrity, sovereignty, and national security and defense;

b) To protect the democratic institutions of the Republic, as well as the rights of the people living in Colombia—in particular the rights to life and personal integrity—and of Colombians at any time and in any place against threats such as terrorism, organized crime, drug trafficking, kidnapping, weapons, ammunition and explosives trafficking, among other similar materials, money laundering, and similar threats; and

c) To protect the natural resources and economic interests of the Nation.

These aims are not clearly defined by law, and there are no examples that give context to scenarios in which the intelligence and counterintelligence services should be applied. This lack of specificity could allow intelligence agencies to self-define the events that give rise to intelligence and counterintelligence tasks, rendering all surveillance activity subject to the agencies' discretion.

2.3 The Legitimate Aim Must Limit the State's Surveillance Powers, Not Expand Them

ARGENTINA: The New Doctrine of National Intelligence is problematic and could

122 United Nations, Human Rights, Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, (2013). http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=13598, as cited Valentina Hernández and Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," Derechos Digitales and Electronic Frontier Foundation (2016). https://necessaryandproportionate.org/country-reports/chile

encourage Argentinian States to implement practices that violate human rights.[123] The New Doctrine identifies several legitimate aims of intelligence surveillance, but does so with such breadth that it seems to expand, rather than narrow, constitutional standards. It states that intelligence agencies must focus their information collection on a series of issues related to national defense and domestic security.

This new doctrine defines domestic security ambiguously as "criminal phenomena violating the freedoms and rights of individuals and of the constitutional, social, and democratic State governed by a rule of law."[124] In particular, it states that intelligence activities in this context shall tackle issues like terrorism and organized crime, with a focus on drug and human trafficking. Among the intelligence activities it authorizes is the monitoring of communications linked to "attacks against constitutional order and democratic life."

Included in this group of actions, according to this new doctrine, are activities carried out by economic or financial groups conducting bank runs and boycotts that may result in "market coups." This authorization may well prove problematic because it goes beyond the definition of "acts of force against the constitutional order and the democratic system" that is already provided for in the National Constitution. As *Asociación por los Derechos Civiles* cautions, it could "encourage State practices that might result in a violation of a citizen's human rights. Attacks against constitutional order are clearly defined in the Constitution, and the Executive Branch should not broaden this definition by regulatory means."[125] As mentioned before, even though there was a presidential turn over on December 2015, the new administration has not expressly revoked the New Doctrine nor has it replaced it with a similar document.

Argentina's telecommunication framework also violates the Legitimate Aim Principle:[126]

> *[W]ith regard to the telecommunications framework, the requirement that service providers must retain information is not duly justified,[127] nor does the legislation adequately describe the aims.*
>
> *Similarly, telecommunications legislation does not comply with this principle. This*

123 Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/argentina

124 Argentinean, Decree No. 1311/15, Official Journal of July 6, (2015), Annex 1.

125 Asociación por los Derechos Civiles, Comments on Decree 1311/15, (2015, p. 2). http://www.adc.org.ar/wp-content/uploads/2015/07/Apuntes-sobre-el-decreto-1311-15.pdf.

126 Daniela Schnidrig and Verónica Ferrari, "State Communications Surveillance and Protection of Fundamental Rights in Argentina," Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/argentina

127 Argentina, Communications Secretariat, art. 8.

law compels users to allow authorities to access information so they can conduct "all kinds of tasks and necessary verifications" without specifying the kinds of tasks, the types of verifications or their purposes.[128] *It also compels mobile service providers to report "all information" about users and clients, without giving a reason for such measures.*[129]

2.4 Safeguards Against Discrimination

Legislation that authorizes surveillance should stipulate that intelligence measures may not be used for discriminatory purposes. Many laws in the region do just that.

ARGENTINA: The law favorably specifies that intelligence agencies may not store information on the basis of race, religion, private actions, political activities or memberships.[130]

COLOMBIA: The law favorably contains an extensive list of criteria that may not be used to justify surveillance. These include: sex, race, national or family origin, language, religion, political or philosophical opinion, membership in a union, in a social or human rights organization, or in an organization promoting the interests of any political party or movement or affecting the rights and safeguards of opposing political parties.[131]

CHILE: The law stipulates that certain procedures to obtain information (which in Chile are called "special procedures for the collection of information") may be carried out with the sole purpose of safeguarding national security and protecting Chile and its people from threats related to terrorism, organized crime, and drug trafficking.[132] The implication that the surveillance shall not be used for discriminatory purposes should be explicitly stated.

128 Argentina, Law 27,078 Argentina Digital, art. 60, section D.

129 Argentina, Law 25,891 on Mobile Communications Services, art. 8.

130 Argentina, Law 25,520 on National Intelligence, Official Journal of December 6, 2001, art. 16f, incorporated by Law 27,126, art. 15

131 Colombia, Law 1621 of 2013, art. 4.

132 Chile, Law 19,974, art. 23.

3.
Necessity, Adequacy, & Proportionality

The Necessity Principle requires all surveillance laws, regulations, and activities to be limited to what is strictly and demonstrably necessary to achieve a Legitimate Aim. Surveillance may only be conducted when the measure is the only means available to achieve the 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.

The Adequacy Principle requires communications surveillance authorized by law to be an effective means of fulfilling the specific Legitimate Aim identified.

The Proportionality Principle requires that communications surveillance be regarded as a highly intrusive act that interferes with human rights and threatens the foundations of a democratic society. Decisions about communications surveillance must consider the sensitivity of any accessed information and the severity of the human rights violations and other competing interests on a case by case basis.

This assessment requires that a State, at a minimum, establish that:

1. There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been, or will be, carried out;

2. There is a high degree of probability that relevant and material evidence of such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the protected information sought;[133]

133 The 13 Principles has defined protected information as any "information that includes, reflects, arises from, or is about a person's communications and that is not readily available and easily accessible to the general public. Traditionally, the invasiveness of Communications Surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider. However, these distinctions are no longer appropriate for measuring the degree of the intrusion that Communications Surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications—metadata and other forms of non-content data—may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analyzed collectively, reveal a

3. Other, less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option;

4. Accessed information will be confined to that which is relevant and material to the serious crime or a specific threat to a Legitimate Aim;

5. Any excess information that is collected will not be retained, but instead promptly destroyed or returned;

6. Information will be accessed only by the specified authority and used only for the purpose and duration for which authorization was given; and

7. The surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or fundamental freedoms.

These principles should be assessed at different stages of the communications surveillance process: assessing the necessity of the means of surveillance, assessing the necessity of retaining the specific collected information, and assessing whether or not the surveillance measure has minimized the impact on protected information and human rights.[134]

As outlined in the Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance,[135] government agents who want to conduct surveillance to obtain protected information:

> *[M]ust clearly demonstrate that communications surveillance is the least intrusive means that can be used to achieve a Legitimate Aim. [...] [I]t is not enough that the communications surveillance be related to the target, Legitimate Aim, account, device or repository to be searched [...] but the [government agent] must narrowly tailor [its request] to minimize the impact on other protected information.*

---

person's identity, behavior, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time, or of all people in a given location, including around a public demonstration or other political event. As a result, all Protected Information should be given the highest protection in law." Necessary and Proportionate Coalition, Necessary & Proportionate, (2014). http://necessaryandproportionate.org/principles See Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (2014). http://necessaryandproportionate.org/global-legal-analysis

134 Access Now, "Universal Implementation Guide For The International Principles On The Application Of Human Rights To Communications," (2015). https://en.necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf

135 Access Now, Universal Implementation Guide For The International Principles On The Application Of Human Rights To Communications, (2015). https://necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf

All applications to conduct communications surveillance should explain what the Legitimate Aim of the communications surveillance is, along with the exact information that is needed to achieve the Legitimate Aim. The application should explain why communications surveillance and any access to personal, private information is necessary. The application should also identify, to the fullest extent possible, the target of the communications surveillance. [...]

Finally, an application must precisely describe the scope of the communications surveillance that has been requested. A proper description of the scope should describe the account, device, or repository subject to communications surveillance, the particular database thereon, any extraneous protected information expected to be accessed, the methodology to be used, the relevance of the necessary information to the identified Legitimate Aim, and the specific timetable, either in the time span over which they can acquire data or the period for which they have access to a certain account, device, or repository.[136]

Again, in Latin America, the Necessity, Adequacy, and Proportionality Principles are traditionally reflected in international human rights treaties that each State has ratified and recognized in its constitution.[137] Moreover, the interests protected by these Principles are deeply embedded in the region's constitutions. States have also adopted legal provisions that restrict which communications can be placed under surveillance. However, the development of new surveillance technologies and the increasing amount of data that can be obtained by way of communications surveillance have complicated the application of these Principles, resulting in some government surveillance activities that lack Necessity, Adequacy, and Proportionality.

The following section provides a few interesting examples of the legal provisions intended to limit the use of communications surveillance to what is adequate and proportionate. We do not, in this section, provide a detailed comparison of the proportionality rules for wiretapping. A detailed analysis of those can be found in the national country reports. We also do not explore how these laws are applied. Such analysis is, for the most part, included in the analysis of the Legality Principle, above. However, we do provide a brief analysis of the proportionality of data retention laws, since they are inherently disproportionate.

136 Necessary and Proportionate Coalition, Necessary & Proportionate, (2014). http://necessaryandproportionate.org/principles; Necessary and Proportionate Coalition, Necessary & Proportionate Global Legal Analysis, (2014). http://necessaryandproportionate.org/global-legal-analysis

137 Valentina Hernández and Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," Derechos Digitales and Electronic Frontier Foundation, (2016). https://necessaryandproportionate.org/country-reports/chile

3.1 Communications Surveillance Must Be Limited to Situations in Which It Is Necessary, Adequate, and Proportionate

Some countries in the region have surveillance laws that include promising language, though it remains to be seen whether they will be implemented in privacy-protective ways. Other countries confine surveillance to the least intrusive means. Many laws accomplish some aspect of proportionality by placing time limits on surveillance orders. Most alarmingly, some countries' laws have purportedly implemented the Necessity and Proportionality Principles, but in such a way as to have actually weakened the Principles.

EL SALVADOR: Article 2 of the Special Law for the Interception of Telecommunications incorporates a rigorous proportionality analysis. It defines surveillance as an exceptional measure that may be used if it is useful to a criminal investigation. However, its necessity must be justified sufficiently, and it must be the least onerous way to investigate the crime.

The law also creates a Principle of Temporality in which any intervention may be carried out only for the period of time allowed by the judge. The law appropriately defines intervention as an authority who listens, captures, or records a private communication without the consent of its participants. By its language, El Salvador's law governing the interception of telecommunications is promising, favoring privacy and the secrecy of communications.[138] It remains to be seen whether the law will be applied in a privacy-protective manner.

BRAZIL: Telephone Interception Law 9,296 of 1996 has promising language in theory but is extensive in practice. Article 1 has expanded the scope of the regulation beyond telephone interception to include "interception of communications flowing through information technology and telematics."

> *[W]ithin the context of the controversy about the proper interpretation of the constitutional provision protecting the secrecy of communications, the constitutionality of this provision was challenged based on the understanding that only the flow of telephone communications, not other kinds of communications, could be intercepted and limited to criminal investigation purposes. However, the [Unconstitutional Direct Action] was dismissed on procedural grounds. Currently, Article 7, subsection II, of the Marco Civil Da Internet, allows for the interception of the flow of communications over the Internet, by court order, "in the form required by law" (in reference to the Interception law).*
>
> *Interception of the flow of communication occurs, pursuant to the provision of the main clause of Article 1 of Law 9.296/96, for the purposes of a criminal*

138 El Salvador, Special Law for the Interception of Telecommunications, art. 3.

investigation or discovery in a criminal proceeding, by court order, sua sponte ("ex officio") or upon request from a law enforcement officer or the Public Attorney's Office. [...] Interception requests by authorities not expressly designated, such as [...] ABIN, are prohibited."[139]

Article 2 of the law prohibits communications interception when there exists no reasonable evidence of criminal responsibility or conspiracy to commit a crime, when evidence can be obtained by other means, or when the act under investigation is subject to no more than a "*detenção*-type" sentence.[140] Articles 2, 4, and 5 outline that communications interception may occur if justified:

[T]he interception request must be supported by a clear description of what is being investigated, including identification of the subjects, unless this is proved to be impossible. The request must also specify the grounds for the investigation and propose a means to be employed," which will be established in the court order.[141]

[T]he maximum period of time for interception should not exceed 30 days. Prevailing court precedents[142] *are of the opinion that an interception order may be renewed for as long as it is required. [...] Article 8 requires confidential treatment of records of interception, and Article 9 requires their destruction if they are not useful, or cease to be useful for evidentiary purposes.*[143]

GUATEMALA: Another promising provision can be found in Article 50 of the Law Against Organized Crime, which requires that the request to intercept communications include a justification for the interception, including an explanation of the necessity and adequacy of the investigation:

---

139 Dennys Antonialli and Jacqu eline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

140 Brazil, Law 9,296 of 1996, art. 2. Abstract from Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

141 Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab, (2015). https://necessaryandproportionate.org/country-reports/brazil

142 See Justice Joaquim Barbosa, Federal Supreme Court, habeas corpus 84.301, ruling of 9 Nov. 2004. (http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79542, and Justice Nelson Jobim, habeas corpus 83.515-RS, ruling of 16 Sept. 2005. http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79377

143 Dennys Antonialli and Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," *Electronic Frontier Foundation & InternetLab*, (2015). https://necessaryandproportionate.org/country-reports/brazil

Authorization requests for communications interception covered by this Act shall be submitted in writing to the competent judge. The following requirements must be included:

a) A description of the event under investigation, along with the offense or offenses under which they fall;

b) Telephone numbers, frequencies, email addresses, as appropriate, or any other data that are useful for determining the electronic or computer means intended to be intercepted [...];

c) A description of the investigative means and measures that have been carried out thus far;

d) Justification for the use of this measure based on its necessity and appropriateness; and

e) When available, the names and other information identifying the person or persons who will be affected by the measure.

Article 51 defines the "necessity and adequacy of the investigation":

> *[I]t will be understood that there is a need for the interception of communications when the investigation shows that members of organized criminal groups have used, or are using, the media established by this Act when committing a crime. The interception of communications is considered adequate if it can be determined that such a measure is effective in obtaining investigative elements that prevent, interrupt, or clarify the commission of the crimes carried out by members of organized criminal groups.*

International human rights standards define "necessity" differently. This provision must be interpreted both with the Constitution and the international human rights treaties that the Guatemalan government has ratified.

Article 51 of the Law Against Organized Crime states that communications interception is an effective measure for gathering evidence to stop the commission of an organized crime. This same law also includes a promising legal provision: destruction of surveillance records must occur in front of a judge after the conclusion of a case.

A judicial request to intercept communications must include a description of the measures and means of the investigation that have already been exhausted.[144]

144 Guatemala, Law Against Organized Crime, art. 50 [*Ley Contra la Delincuencia Organizada*], Ministry of Interior [*Ministerio de Gobernación*], (2006).

HONDURAS: Honduras has a mixed model. Article 5 of the Special Law of the Intervention of Communications allows communications surveillance for any crime, provided there are no less onerous measures of intervention.[145]

Article 6 establishes that communications interception may occur only during criminal investigations, and the Office of the Prosecutor or attorney general must reasonably establish that a criminal act has been, is being, or is about to be committed.

The application that is submitted to request surveillance authorization must contain any known information about the person whose communications will be targeted. If the person's identity is unknown, the application should explain the circumstances under which an investigation is required and provide basic elements of the person's identification (Article 9). The application should also include information about the surveillance devices that will be used and information that can identify the person who is to be surveilled, such as a phone number or email address (Article 9).

A communications interception request must include the duration of the surveillance measure (Article 9). The authorized measure must not exceed three months. However, it may be extended for an additional three months according to a special law (Article 12). This law expressly states that when the objective has either been fulfilled or has been deemed unsuitable, unnecessary, disproportionate, or unenforceable, surveillance must cease at the request of the prosecutor or authorizing judge (Article 16).

COLOMBIA: Colombia's legislation that governs intelligence activities explicitly states that they must be governed by the Principle of Necessity. Article 5 of Law 1621 of 2013 stipulates: "Intelligence and counterintelligence activities must be necessary to accomplish the constitutional aims pursued; that is to say, they can be used only when there exists no less invasive technique to reach such aims."

Colombia's legislation also incorporates the Principle of Adequacy when it comes to conducting intelligence activities. Article 5 of Law 1621 of 2013 establishes:

> *[I]ntelligence and counterintelligence activities must make use of measures that are adequate for the accomplishment of the aims identified in Article 4 of this law; that*

---

http://leydeguatemala.com/ley-contra-la-delincuencia-organizada/requisitos-de-la-solicitud-de-autorizacion/10470/

145 Republic of Honduras, *Special Law for the Intervention of Communications [Ley de intervencion de las comunicaciones]*, Decree No. 243-2011, (2011). http://www.conatel.gob.hn/doc/Regulacion/leyes/Ley_especial_comunicaciones_privadas.pdf

is to say, only the adequate measures to achieve such aims must be implemented, and not others.[146]

Article 5 also recognizes the Principle of Proportionality in the operation of intelligence agencies, stipulating:

> *[I]ntelligence and counterintelligence activities must be proportionate to the pursued aims and their benefits must exceed the restrictions imposed on other constitutional principles and values. Particularly, the implemented measures and methods must not be disproportionate in comparison to the pursued objectives.*

Moreover, Legislative Decree 1141 provides that intelligence activities may be requested by the national intelligence director only, and that the request must contain: (i) the identification of the person(s) affected by the measure; (ii) the description of the requested measures; and (iii) the justification and duration of such measures.

CHILE: Article 222 of the Criminal Procedure Code regulates telephone and other telecommunications interception:[147]

> *The provision stipulates that in cases of reasoned suspicion, based on particular facts that suggest a person has committed or participated in a crime or its organization, or that the person is currently organizing the commission of or participation in a punishable act sanctioned as a crime (that would be punishable by at least five years and one day of imprisonment), and if the investigation so requires, the supervising judge, upon the Public Ministry's request, may order the interception and recording of this type of communications.*
>
> *The requirement of having "reasoned suspicion" refers to the fact that considering the specific circumstances of the case and concrete punishable crimes, there should be a justified belief that the person under investigation has participated in the organization or commission of a crime, or that he or she will do so in the future. Moreover, a requisite of necessity is established in order to proceed with the interception. It must be crucial to the process of the investigation.*[148]

As a prerequisite for authorizing the interception of communications, the supervisory judge (*juez de garantías*) must assess whether the interception of communications is required for the purpose of the criminal proceedings.

146 Article 4 was included in the Principle of Legitimate Aim section.

147 For a detailed legal analysis of surveillance laws in Chile, *see* Valentina Hernández and Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," *Derechos Digitales and Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

148 Valentina Hernández and Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," *Derechos Digitales and Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

[T]he legislation does not specifically reference these principles, but they are underlying in the text. For instance, Article 222 of the Criminal Procedure Code outlines time limits for the intrusive measure, a scope that limits the intrusion to obtain only the data strictly necessary to the investigation, a required certain level of probability ("well-founded suspicion"), and a required minimum penalty or special qualification linkable to the criminal act; all of these factors determine the appropriateness of such measures, delimiting what can be intercepted and recorded. [...]

The Principle of Necessity is implicitly complied with, since the supervising judge shall authorize these measures only when they are essential to the investigation. Once again, it is possible to see these principles recognized and effectively applied in the legislation on the interception of communications by the supervising judge.[149]

Chile is among those States that incorporate some aspect of the Proportionality Principle into their legislation by placing time limits on surveillance orders. Communication interception for the investigation of an ordinary crime may be authorized for a 60-day period only; and drug trafficking communications may be intercepted for 120 days, with the orders renewable for successive 60-day periods.

Chile's intelligence legislation also incorporates the Principle of Necessity into its language. Article 23 of Law 19,974 establishes: "Whenever certain information is strictly required for the achievement of the objectives of the System, and it cannot be obtained from publicly available information, the special procedures for the collection of information may be carried out." The special procedures set out in Article 23 include:

a) The interception of telephone, computer, and radio communications, and of correspondence in any of its forms;

b) The interception of computer systems and networks;

c) Wiretapping and electronic recordings, including audiovisual recordings; and

d) The interception of any other technological system used for the transmission, storage, or processing of communications or information.[150]

Chile's law also respects the Principle of Proportionality by outlining that the special intelligence procedures mentioned in Article 24 of Law 19,974—which have the potential to greatly infringe upon the right to privacy—are limited to intelligence activities that aim at safeguarding national security, and protecting Chile and its people from threats related to

149 Valentina Hernández, Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," *Derechos Digitales and Electronic Frontier Foundation* (2016). https://necessaryandproportionate.org/country-reports/chile

150 Chile, Law 19,974, art. 24.

terrorism, organized crime, and drug trafficking.[151] As always, vague definitions of crimes to which this applies create potential opportunities for abuse.

PERU: Peru's law requires that all the intelligence information that the National Intelligence System *(SINA*) obtains that is private and not required for system objectives must be destroyed by the responsible officials under subpoena of disqualification, irrespective of the corresponding civil and/or criminal penalties.[152]

Similarly, Peruvian legislation establishes that all natural or legal persons are legally compelled to cooperate with the National Intelligence System (SINA) by providing them with any information related to intelligence investigations required by the governing body of the system at no cost.[153] The same article stipulates that whenever the requested information is protected by some obligation of secrecy, its delivery will not violate that obligation so long as it adheres to this principle, to which all intelligence personnel are compelled. However, there are exceptions to this obligation, including information protected by professional secrecy, personal and familial privacy, bank secrecy, tax confidentiality, and constitutionally recognized items.

ARGENTINA: A similar provision to the one found in Peru is found in Argentina's legislation.[154] The law stipulates that intelligence organizations may not disseminate information that is obtained during performance of their duty and that such information may not be disclosed unless authorized by a judicial order.[155] Furthermore, as the Principle of Competent Judicial Authority will clarify, intelligence organizations may not autonomously authorize the interception of communications.

A judicial authorization must be requested whenever such measures are deemed necessary. If the judge grants this authorization, the Argentinian legal system limits it to a maximum period. The period may be extended for an additional 60 days, at most, as long as the extension is indispensable to the completion of the investigation.[156]

3.2 Prohibition to Surveil Certain Types of Communication

Several States in the region have laws that prohibit communications interception in certain circumstances. The most common exception is for attorney-client communications.

151 Chile, Law 19,974, art. 23.

152 Peru, Legislative Decree 1141, art. 35.

153 Peru, Legislative Decree 1141, art. 41.

154 Argentine, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, art. 16f.

155 Argentine, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, art.16c.

156 Argentine, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, art. 19.

PARAGUAY: Paraguay maintains a clear list of exceptions. Interception cannot be carried out against the accused with his or her witnesses who have been excused from testifying due to kinship or confidentiality, including lawyers and doctors. The law prohibits obtaining lawyers' notes, medical records, or information from close family members. This means that if these witnesses take notes on the communications they shared with the accused, the government cannot surveil them. This limitation applies only to the communications of witnesses who have been granted the ability to abstain from testifying.[157]

CHILE: Communications between the accused and their lawyers generally cannot be intercepted, except in cases where a *juez de garantías* believes a lawyer is criminally liable in the matter under investigation and specifically orders surveillance. The judge shall include all supporting information in the order.[158]

URUGUAY: The law expressly prohibits the interception of communications between the investigated and his counsel, and any concerning questions that are not related to the object of investigation.[159]

MEXICO: The federal judicial authority shall not authorize surveillance for electoral, fiscal, mercantile, civil, labor, or administrative issues. Nor may it authorize the surveillance of communications between a detainee and his or her counsel.

COLOMBIA & NICARAGUA: The Colombian Code of Criminal Procedure[160] and the Criminal Procedural Code of Nicaragua[161] prohibit the interception of communications between the accused and his or her counsel.

157 Paraguay, Law 1286-98, *Criminal Procedural Code*, art. 198 & 200. https://www.imolin.org/doc/amlid/Paraguay/Paraguay_Código_Procesal_Penal.pdf.

158 Chile, Ministry of Transport and Communications, Regulation about interceptions and Recording of Telephone Communications and Other Telecommunications Means, 2005.

159 Uruguay, Law 18.494, Control and Prevention of Assets Laundering and Terrorist Financing, art. 5.

160 Colombia, Law 904 of 2004, *Criminal Procedural Code*, art. 235.

161 Nicaragua, Law 406, *Criminal Procedural Code*, (2001), La Gaceta 243 & 244 (2001). http://legislacion.asamblea.gob.ni/Normaweb.nsf/%28$All%29/5EB5F629016016CE062571A1004F7C62

4.
A Culture of Secrecy and the Right to Know

States should be transparent about the use and scope of communications surveillance laws, regulations, activities, powers, and techniques.

Understanding government actions is the first step in ensuring that a government respects the civil liberties of its citizens. Transparency especially is important when law enforcement agencies adopt new technology for national security purposes. Without transparency, society is unable to hold government accountable for its use of surveillance technologies, such as cell phone location, tracking devices, and malware. Secrecy prevents meaningful democratic scrutiny of surveillance laws, which can allow intelligence agencies and law enforcement agencies to be their own lawmakers.

The UN Special Rapporteur on the Right to Freedom of Expression and Opinion and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) have called for transparency within governments:

> *[A]ll persons have the right to access information held by the state, including information having to do with national security. The law may establish specific exceptions as long as those exceptions are necessary in a democratic society. The law must ensure that the public can access information on private communications surveillance programs, including their scope and any regulation that may be in place to guarantee that they cannot be used arbitrarily [...]. Consequently, public information should be available concerning regulatory framework of surveillance programs; the procedures for authorizing surveillance, selecting targets, and the purpose for the data collected [including aggregate information on their scope].*

States and telecommunications companies can implement several methods to increase transparency on communications surveillance:

1. States can publish information about surveillance technology purchases they have made.

2. Freedom-of-information laws can be used to obtain additional governmental records. In Latin America, NGOs have begun to use these laws to learn more about surveillance in their countries.

3. States and private companies can issue transparency reports to provide useful information to citizens and users.

4. Telecommunications companies can establish public law enforcement guidelines, which are a set of rules that set forth the circumstances under which they will or will not deliver information to law enforcement.

5. Investigative journalists who receive documents or sources from whistle-blowers describing the capabilities or targets of governmental surveillance programs can publish their findings.

Although many governments are capable of surveilling their own citizens unilaterally, they often compel third-party telecommunications companies to carry out surveillance on their behalf. Telecommunications providers, Internet companies, and ISPs often are compelled to assist governments by either providing direct access to their user data or facilities, or sharing specific user data that the government requests in accordance with the law.

In the United States, many telecommunications companies issue transparency reports in which they disclose how many requests for user data they have received from the government. These corporate transparency reports typically are divided into categories based on the type of requests received:

1. government requests to remove content;

2. government requests for user data;

3. government requests about copyright; and

4. statistics on malware and phishing attack detection.

Some companies further disclose how many government requests they have complied with, and how many they have rejected. This type of reporting is limited to instances when companies give governments direct, unsupervised access to systems such as optical splitters on fiber-optic backbones. Otherwise, the companies would be unaware of the scope or volume of the government's access.

While publishing transparency reports has become a best practice for the telecommunications and Internet industries, transparency reports have yet to be widely adopted in Latin America, where the concept of transparency reporting in the context of communications surveillance is unfamiliar. Most Latin American intelligence agencies were formed during the Cold War, when many countries were under dictatorships[162] and governments were operating under a culture of secrecy. A culture of secrecy exists in the region in the context of communications surveillance:

162 Samanta Curti, "Reforms in South American Intelligence agencies" *[Reformas de los Sistemas de Inteligencia en América del Sur]*. http://www.kas.de/wf/doc/17940-1442-1-30.pdf

1. As explained in the Legality Principle section, many governments have used secret laws to justify their surveillance practices.

2. Although freedom of information requests allow obtaining information about governmental communications surveillance activities, such as in Brazil, many countries classify all intelligence information—including information related to communications surveillance—as confidential and extend the term of confidentiality for as long as possible.

3. Latin American ISPs and the countries included in this report (except for Mexico, which has adopted guidelines requesting companies to issue transparency reports) maintain total secrecy about their use of communications surveillance: Investigatory authorities do not release annual reports about how they use their surveillance powers.

Below is a detailed analysis of the transparency practices we found in the context of communications surveillance in the region.

MEXICO: In 2014, the Federal Telecommunications and Broadcasting Law (LFTR) expanded the scope of authorities' surveillance powers significantly. It also imposed more obligations on telecommunications service providers and ISPs to cooperate in matters related to State communications surveillance (for example, Article 189 of the LFTR, in order to establish safeguards related to transparency, requires the Federal Telecommunications Institute [IFT, in Spanish] to issue "Guidelines for Collaboration in Security and Justice").[163] Article 18 of those guidelines requires telecommunications services and ISPs publish a biannual report that includes:

> *(i) The total number of requests by law enforcement for geolocation information and communications data records...the communications received, processed, and rejected, (ii) the number of cancelled and erased records, once the purpose for which they were requested has been accomplished."*[164]

Three ISPs in Mexico have set an important precedent for transparency by issuing some statistics on government requests for data that they have received. Iusacell, Movistar, Nextel, and Telcel have jointly published transparency reports through ANATEL (*Asociación Nacional de Telecomunicaciones*). However, these reports often lack sufficient detail. According to EFF and R3D, they "only provide a general number of requests made by authorities for the prosecution of crime, without providing detailed information about the

163 Federal Telecommunications Institute, *Guidelines for Collaboration in Security and Justice*. Published on the Official Gazette on December 2, 2015. http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

164 Luis Fernando Garcia, "Mexico: State Communications Surveillance and the Protection of Fundamental Rights in Mexico," *Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales* (2016). https://necessaryandproportionate.org/country-reports/mexico

type of requests they have received, which authorities made the requests, and the reasons authorities gave in order to make the requests."[165]

To address transparency in governmental agencies, Mexico enacted the Law on Transparency and Access to Public Information in 2015. Article 70, item XLVII of that law requires federal agencies to publish statistical information about the list of requests they have made to telecommunications service providers for communication interceptions, access to communications records, and access to location data in real time. The list must include the scope and legal basis for the requests and specify whether the requests require judicial authorization. Nevertheless, the same law classifies any information that could jeopardize national security, public security or national defense as confidential (Article 113). In the intelligence context, Article 51 of the Mexican National Security Law describes confidential information as "information whose application entails a revelation of laws, procedures, methods, sources, technical specifications, technology and equipment that are useful for the production of intelligence for National Security, regardless of the nature or origin of the documents that contain it."

BRAZIL: Resolution *(Resolução)* No. 59 of 2008 requires that public prosecutors, including the police and judges, inform the Inspector General of the Office of the Public Prosecutor and the Inspector General of the Office of the National Judiciary, respectively, of the number of communications interception operations underway in the country. This data must be delivered monthly for statistical purposes and contain data related to wiretapping and IT and telematics interceptions used in the National Interceptions Control System.

While this data is not posted publicly, it is available upon request. For example, InternetLab,[166] through an Access to Information Law request, obtained the following information: On average, 18,000 telephone lines are wiretapped, and 50,265 interception notices are sent to telecommunications companies each month.[167]

URUGUAY: No regulation compels intelligence and criminal investigation agencies to publish data about their surveillance activities.[168] Furthermore, there is no obligation for

165 Luis Fernando Garcia, Katitza Rodriguez, New Report Shows Which Mexican ISPs Stand With Their Users, EFF, (2016), https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isps-stand-their-users

166 InternetLab, http://www.internetlab.org.br/en/about/

167 Dennys Antonialli & Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," *Electronic Frontier Foundation & InternetLab,* (2015). https://necessaryandproportionate.org/country-reports/brazil

168 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: State Surveillance of Communications and the Protection of Fundamental Rights in Uruguay," *Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-

telecommunications and ISPs to publish statistics, or aggregated data, about the requests they receive from law enforcement to intercept communications or access data.[169]

Authorities have reported on their wiretapping activities to Parliament and have responded to other specific requests, but they do not regularly and systematically report on their surveillance activities. For example, a presidential candidate recently requested information about whether his communications were intercepted by a criminal investigation agency. The request was addressed to the Uruguayan Supreme Court of Justice and stated that a total of 6,150 wiretaps occurred from 2009 to 2014, but the Court did not address the candidate's specific concern.[170]

Uruguay requires more transparency about its purchase of surveillance tools. For example, authorities have not explained under which procedure they purchased the software *El Guardián;* they have this information classified as "reserved" under the Access to Information law.[171] Furthermore, evidence suggests there are secret decrees that regulate procedures for telecommunications and ISPs to connect to *El Guardian*. As stated above, authorities should disclose the laws—and decrees—under which intelligence agencies are operating so they can be held accountable.[172]

CHILE: Chilean general Transparency Law applies to most state agencies, including the entire judicial branch and the Attorney General's Office (*Ministerio Publico*).[173] Under this law, Chilean citizens may request surveillance statistics and other information, unless the data cannot be disclosed because of national security reasons. Article 38 of Law 19,974 of 2004,[174] which regulates the general framework of Chilean intelligence, classifies all national intelligence information and information collected by intelligence agencies' public servants as reserved and secret. The Public Ministry's annual report does not disclose how many

---

reports/uruguay

169 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: State Surveillance of Communications and the Protection of Fundamental Rights in Uruguay," *Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/uruguay

170 El País, "Judges authorize wiretapping with caution" ["Jueces disponen de escuchas prudentemente"], (2014). http://www.elpais.com.uy/informacion/jueces-disponen-escuchas-telefonicas-prudentemente.html

171 Fabrizio Scrollini, Penumbra: Surveillance, security and public information in Uruguay, GISWATCH. http://www.giswatch.org/en/country-report/communications-surveillance/uruguay

172 Ana Tudurí, Fabrizio Scrollini, & Katitza Rodríguez, "Uruguay: State Surveillance of Communications and the Protection of Fundamental Rights in Uruguay," *Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/uruguay

173 Republic of Chile, Law of Transparency. http://www.leychile.cl/Navegar?idNorma=276363

174 Law 19,974 of 2004. http://www.interior.gob.cl/transparencia/ani/

communications interceptions have been ordered each year.[175]

ARGENTINA: There are no legal obligations to submit transparency reports on communications interceptions for criminal matters in Argentina. Meanwhile, intelligence agencies are compelled to submit confidential reports on their intelligence activities annually to the Bicameral Commission on the Supervision of Intelligence Bodies and their Activities.[176]

In September 2016, the Argentinian House of Representatives adopted the Access to Public Information bill.[177] The new law allows Argentineans to request information from the General Prosecutor and any judge of the Judicial branch.[178] Still, this law contains national security exceptions; information will not be provided in circumstances where a criminal investigation could be jeopardized.[179]

PARAGUAY: The laws that regulate communications surveillance do not require the state to publish transparency reports for either criminal investigations or national intelligence operations. The annual reports of the National Police, the Public Ministry, and SENAD, Paraguay's anti-drug agency, do not contain the number of requests approved and rejected, nor the number of requests made by service provider, authority, type, or purpose.[180] Paraguay is unique in that it recently created a centralized intelligence agency (2014)[181] and also recently approved an Access to Information Law, which only applies to the judicial branch and some parts of the executive branch, but not the new centralized intelligence agency.[182]

---

175 Juan Carlos Lara, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," *Derechos Digitales and Electronic Frontier Foundation,* (2016). https://necessaryandproportionate.org/country-reports/chile

176 Verónica Ferrari & Daniela Schnidrig, *State Communications Surveillance and Protection of Fundamental Rights in Argentina*, *Centro de Estudios en Libertad de Expresión y Acceso a la Información and Electronic Frontier Foundation (2016).* https://necessaryandproportionate.org/country-reports/argentina

177 Télam. La Cámara de Diputados Aprobó la ley de Acceso a la Información Pública. (2016). http://www.telam.com.ar/notas/201609/162990-camara-de-diputados-acceso-a-la-informacion.html.

178 Republic of Argentina. Draft Bill for Access to Public Information. Article 7. "Proyecto de ley de Acceso a la Informacion Publica." http://www.saij.gob.ar/proyecto-ley-acceso-informacion-publica-enviado-al-congreso-poder-ejecutivo-nacional-proyecto-ley-acceso-informacion-publica-enviado-al-congreso-poder-ejecutivo-nacional-nv14182-2016-04-07/123456789-0abc-281-41ti-lpssedadevon

179 Ibid. Aricle 8.

180 Jorge Rolón Luna & Maricarmen Sequera, "State Communication Surveillance and the Protection of Fundamental Rights in Paraguay," *Electronic Frontier Foundation & TEDIC,* (March 2016). https://necessaryandproportionate.org/country-reports/paraguay

181 Insight Crime. http://es.insightcrime.org/noticias-del-dia/congreso-de-paraguay-aprueba-agencia-nacional-de-inteligencia-tras-ataques-del-epp

PERU: Peruvian legislation does not compel intelligence agencies to publish statistics on the number of communications interception requests that have been sent to the judicial branch. This has resulted in a lack of information on the number of approved judicial authorizations in the country. A lack of transparency also exists in the procedures governing communications surveillance. In 2015, the Peruvian government issued Ministerial Order 0631-2015-IN, which stated: "Protocol for accessing geolocation data of cellphones and electronic devices of similar nature." It established the procedure for accessing geolocation data, according to Decree No. 1182. The protocol is not available to the public; it was categorized as classified information pursuant to the Freedom of Information Act.[183]

Peruvian providers have yet to adopt a tradition of transparency reporting in the private sector. In 2015 the Peruvian NGO Hiperderecho and the Electronic Frontier Foundation published "Who Has Your Back?," a report that evaluated the privacy policies and data protection practices of the Peru's major Internet providers. None of the companies in the study provided information on the government requests for data they had received.[184]

Thus, there is no publicly available information from either the government nor or providers on the number of requests the government has sent to ISPs to access their retained data.

EL SALVADOR: Article 10 of the Law on Access to Public Information states that the statistics generated by all State entities are considered public, including those produced by the Attorney General's Office, which oversees the Center for Telecommunications Interventions.[185] Despite that the Attorney General's Office has published statistics on information requests pursuant to this law,[186] the data do not identify the entities or individuals requesting the information. Furthermore, no annual reports have been published on the number of surveillance requests that have been approved or rejected.

HONDURAS: The Freedom of Information Act can be used to obtain statistical information on surveillance requests if the data exist and are not considered confidential. However, the statistical information produced by the Interception Center is considered confidential (*información reservada*). All information produced by the Interception Center

182 Republic of Paraguay, Law 5282. http://informacionpublica.paraguay.gov.py/public/ley_5282.pdf

183 NGO Hiperderecho, "Stalker Law operates under confidential protocol" ["La Ley Stalker reservada forma en la que se aplica"] (2016). http://www.hiperderecho.org/2016/02/policia-ley-stalker-reservada-la-forma-en-la-que-aplica-la-leystalker/

184 Katitza Rodriguez "Quien Defiende tus Datos?", Hiperderecho, Electronic Frontier Foundation (2015) http://www.hiperderecho.org/qdtd/

185 Republic of El Salvador, Decree No.534, Law of Access to Public Information. http://www.redipd.org/legislacion/common/legislacion/elsalvador/Decreto_N534.pdf

186 El Salvador. Attorney's General Office. http://www.fiscalia.gob.sv/datos-estadisticos-de-solicitudes-recibidas-de-enero-mayo-de-2014/#/6/zoomed

also is classified as confidential intelligence information.[187]

GUATEMALA: Guatemalan national law does not require publication of transparency reports on surveillance, and the administration does not publish this information.[188] However, according to Article 30 of the Constitution of Guatemala, all acts of the administration are public. It is unclear, however, whether a successful challenge to the government's secrecy could be mounted based on that provision.

NICARAGUA: Nicaragua has a freedom of information law (Law 621 of 2001). However, it classifies any information related to national security as confidential.[189] No statistics are available on the number of interception requests that have been made.[190]

COLOMBIA: Law 1621 of 2013 does not compel intelligence agencies to report on the number of communications interceptions that take place every year. Although Colombia has a transparency law (Law 1712 of 2014: *"Ley de Transparencia y Derecho a la Informacion Publica*")[191] that compels public agencies to publish data about their activities, national defense and security information are exempt from this requirement.[192] The same exemption occurs for information requests made pursuant to Colombia's constitutional "right to request" (*derecho de petición)*, which allows citizens to request information about any governmental agency. The Intelligence Law in Colombia also expressly states that oversight of intelligence activities is under strict reserve.[193]

Moreover, Colombian criminal proceedings are governed by the principle of publicity. This means that "hearings in which the legality of communications interception and other

187 Edy Tábora Gonzales, Capitulo de Honduras. In: Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, 2015. pdf; 4MB

188 Jorge Jiménez Barillas Hedme Sierra-Castro. Guatemalan Chapter. In: Fundación Acceso, Privacy for digital rights defenders: A study on how the legal frameworks of El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance of human rights defenders. Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015).

189 Republic of Nicaragua, Law 621 of 2007. http://www.oas.org/juridico/spanish/mesicic3_nic_ley621.pdf. Article 15.

190 Fundación Acceso, Privacy for digital rights defenders: A study on how the legal frameworks of El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance of human rights defenders. Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015),

191 Republic of Colombia, Law 1712 of 2014. Article 9, Article 11. http://www.centrodememoriahistorica.gov.co/descargas/transparencia/Ley1712-transparencia-acceso-informacion.pdf

192 Ibid, Article 5.

193 Republic of Colombia, Law 1621 of 2013, Article 21.

surveillance measures are verified are open to public scrutiny."[194]

Despite this, Article 18 of Act 906 of 2004 stipulates that the judge may limit publicity of the procedures if he or she believes it could be harmful to national security. Concerning the private sector, last year the Karisma Foundation and the Electronic Frontier Foundation published a joint report titled "Colombian Users to ISPs: Where Is My Data?," in which they reported that none of the ISPs in Colombia have published transparency reports.[195]

In summary, the States in the region, aside from Mexico, generally have a poor or unclear legal climate related to disclosing the nature, scope, or purpose of state communications surveillance activities.

194 Juan Camilo Rivera & Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

195 Karisma Foundation, Colombian Users to ISPs: "Where is my data?" https://www.eff.org/deeplinks/2015/05/which-internet-providers-tell-colombians-where-their-data

5.
User Notification

If an authority is empowered to surveil communications, the law also must recognize individuals' right to know if they have been surveilled. Individuals should be notified of any decision authorizing communications surveillance that will be carried out on them with enough time and information to challenge the decision or seek other remedies, including access to the materials presented in a support of the authorization request. Notification shall be deferred only if the judge responsible for authorizing the surveillance determines that such notification would seriously jeopardize the purpose for which the surveillance was authorized or if there is an imminent risk of danger to human life. In such situations, however, the law should set deadlines for the deferral of notification.

In jurisdictions such as Colombia and El Salvador, defendants have the right to access evidence derived from surveillance during a criminal trial to challenge its legality or admissibility. However, other jurisdictions also provide, in theory, a broader right of notification to everyone affected by surveillance, whether or not the affected parties ever become defendants in a criminal case, once an investigation is complete. This is the case in Peru and Chile. No States clearly provide for notification prior to the surveillance's completion, even when information is sought retrospectively rather than prospectively.

In the intelligence context, no State in the region has established notification measures. Such procedures should be adopted.

PERU: Peru has a better user notification policy than other countries in the region do. In Peru, user notification occurs only after a criminal investigation closes. According to Article 231 of the Criminal Procedure Code, once surveillance activities and investigations are complete, the individual who was surveilled must be notified. The affected person may ask for judicial reexamination of the surveillance within three days of receiving notice. However, the code specifies that the surveilled individuals need not be notified if notification could jeopardize the life or physical integrity of any third party. This provision is similar to the European Court of Human Rights' decision in *Ekimdzhiev v. Bulgaria,* which notes that once surveillance has ended and the necessary time has elapsed for the legitimate aim of the surveillance to no longer be at risk, those affected must be notified without delay.[196]

Despite this general principle, Peru's laws do restrict notification in at least one surveillance

196 ECHR, Case of the Association for European Integration and Human Rights and *Ekimdzhiev v. Bulgaria*. Application nº 62540/00. Sentence on June 28, 2007.

scenario: The law forbids company employees to reveal whether their company has been ordered to collect phone data. However, this restriction may not apply to the company as a whole. The gray zone is in the wording of the Criminal Procedure Code, which states:

Article 230:

> *4. The concessionaires of public telecommunications services must immediately provide the geolocation of mobile phones and take steps necessary to achieve the interception (intervención) or the recording of communications that have been ordered by a court decision, in real time, continuously, for 24 hours a day, 365 days a year, under penalty of being liable to legal liability in case of failing to do so. The employees of the companies indicated must keep such obligations a secret, except if called upon to testify about them in court.*

CHILE: Chile does not allow prior notification of surveillance. Article 224 of the Criminal Procedure Code requires notification of those affected by a surveillance measure after its completion if the aim of the investigation allows it, and if such notification does not jeopardize the life or physical integrity of a third party. Article 182 protects the secrecy of investigations but allows defendants in criminal cases to obtain access to evidence against them.

MEXICO: There is no legal obligation that compels either the State or companies to notify users if they are the subjects of surveillance. The law does not address notifying affected parties after the conclusion of investigations.

ARGENTINA: There is no legal obligation that compels the State or companies to notify users that they are the subject of surveillance. Like in Mexico, Argentinian law does not address the issue of notification after the conclusion of an investigation. No notification obligation is currently established by law—not for companies, not for the intelligence agencies, and not even for criminal prosecutors conducting investigations or pressing criminal charges. Users may learn about surveillance conducted on them by chance if evidence gathered on them is used as evidence in a criminal procedure. But there is no obligation that mandates public officials to disclose where they obtained such evidence.

However, users do have a right to request access to the information that has been gathered on them by intelligence agencies. This right has been recognized by the Supreme Court in the *Ganora* decision, which states that intelligence officials cannot reject requests made by individuals for access to information about themselves using a blanket exception. On the contrary, the Supreme Court requests intelligence authorities to justify any exception for accessing information.[197] The Supreme Court ratified this doctrinal line in the *R.P., R.D.*

197 Supreme Court of Argentina. Ganora s/ hábeas corpus. Decision of September 16, 1999.

decision of 2011.[198]

BRAZIL: There is no legal obligation that compels either the State or companies to notify targets of surveillance prior to carrying it out. However, the Code of Criminal Procedure provides that a judge, upon an application for a "precautionary measure," (*medida cautelar*) such as an application for a warrant, shall notify the affected party, "except in cases of emergency or the possibility [that notification may] compromise the effectiveness of the measure"[199]

This exception routinely is applied to ongoing criminal investigations. When criminal cases are brought to trial, the law only guarantees that the accused shall be notified that they were surveilled when the prosecution seeks to use evidence obtained through surveillance (Article 370, CPP).

As explained in the Brazil report, "With respect to intermediaries, most of the data requests and wiretap orders are accompanied by gag orders that forbid telephone companies and Internet service providers to provide notification. However, even though no gag orders exist when it comes to notifying users in other circumstances, companies do not proactively engage in this practice."[200]

The law does not address the terms of notification following the conclusion of an investigation.

NICARAGUA: There is no legal obligation in either the Criminal Procedural Code or the Organized Crime Law that compels the State or companies to notify users when they are the subjects of surveillance. Article 66 of the Organized Crime Law imposes a "duty of confidentiality" on anyone involved in communications interception that forbids any disclosure, under penalty of law, except during the course of presenting evidence in a criminal case. This obligation does not appear to expire.

Article 66 Duty of Confidentiality states that:

> *[E]xcept in regard to its incorporation into a criminal process, the authorities, public officers or employees, as well as private parties who take part in the process of communications interception shall maintain absolute secrecy concerning what*

198 Supreme Court of Argentina. R.P, R.D. c/ Secretaría de Inteligencia. Decision of April 19, 2011.

199 Article 282, § 3 CPP

200 Dennys Antonialli & Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab (2015). https://necessaryandproportionate.org/country-reports/brazil

they know. Failure to comply with this duty shall be punished according to the Penal Code.

COLOMBIA: The law guarantees that within the criminal proceeding, at the time of the hearing, the accused person who is being surveillance will be notified so that he or she has the opportunity to question the legality of the surveillance measure in the hearing itself. Article 15 of the Criminal Procedure Code states that parties are entitled to refute any type of evidence collection. The General Prosecutor may collect evidence using different methods of communications interception without the owner of the communications' consent. Such interception is validated by the judge of constitutional guarantees, who analyzes whether the interception is in accordance with all constitutional and procedural guarantees. This kind of evidence may be rejected if it is not in accordance with the aforementioned guarantees. Therefore, in most cases, the person whose communications have been intercepted finds out after the fact, but during the criminal trial proceedings.

As for intelligence proceedings, these authorities, in theory, are not authorized to intercept communications because they are not part of the Judicial Police (SIJIN, in Spanish), which is the authorized institution that supports the General Prosecutor in intercepting communications. The Law on Intelligence and Counter-Intelligence does not have notification obligations since, according to the law, communications interception is relegated to criminal investigations.

The law does not provide for prior notification, nor notification after the conclusion of an investigation, nor notification for a person who is not the criminal defendant.

EL SALVADOR: The Special Law for the Interception of Telecommunications does not specifically require that an affected person be notified about a decision authorizing surveillance. However, Article 25 states that "once the court record of the interception is delivered to a competent judge, that court record shall remain public, except if the confidentiality rules of criminal proceedings are applicable." Article 26 establishes that once the court record of the interception is incorporated into the criminal proceedings, then "the defense will have full and unrestricted access to it."

The law does not provide for prior notification, nor notification after the conclusion of an investigation, nor notification for a person who is not the criminal defendant.

HONDURAS: The legal framework does not specifically require that an affected person be notified *a-priori* about a decision authorizing surveillance. However, the Criminal Procedure Code includes a general notification obligation of the corresponding investigation (*diligencia investigativa*) only after an indictment is filed against the subject. Otherwise, notification is not required. Article 21 of the Special Law of Interception of Communication also establishes the confidentiality of the court record (*reserva del*

expediente) during the time that the surveillance measure is taking place, and the court record must be included in the main court file once the surveillance measure has ceased.[201]

The law does not provide for prior notification, notification after the conclusion of an investigation, or notification for a person who is not the criminal defendant.

201 Honduras Chapter, Edy Tábora Gonzales.Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.).p. 228

6.
Who Watches the Watchers?
Competent Judicial Authority & Due Process

The Necessary and Proportionate Principles require that state communications surveillance be formally authorized on a case-by-case basis by an independent and impartial judiciary. This ensures that the State is not acting beyond its authority and that due consideration is given to the human rights of those affected by the surveillance. It also protects the subject's human rights at every step in the authorization process. By requiring the State to justify each act of surveillance to a judge, this principle ensures that communications surveillance is conducted only if necessary and if the cost of human rights is eliminated or minimized. It also allows the subject of surveillance an opportunity to challenge the state's intended action when possible.

In the majority of countries, judges are entrusted with the power to authorize communications surveillance in criminal investigations; however, courts have issued opinions that have varied the degree of judicial authorization and due process, depending on whether the state is surveilling the content of the communications, location data, or subscriber information. In some states, the law does not require prior, or even retroactive, authorization to access subscriber information, location tracking, or metadata.

The Judicial Authority Principle requires that judicial oversight authority be:

1. separate and independent from the authorities conducting communications surveillance;

2. conversant in issues related to communications surveillance and competent in making judicial decisions about its legality, the technologies used, and human rights; and

3. adequately resourced in exercising the functions assigned to it.

The Due Process Principle addresses many of the same concerns and advances many of the same policies as the Competent Judicial Authority Principle. Due process requires that States respect and guarantee individuals' human rights by ensuring that the lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the public. The principle recognizes that "everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent, and impartial judge established by law, except in cases of emergency, when there is an imminent risk to human life." In such cases, retroactive authorization must be sought

within a reasonably practicable time period. Retroactive authorization may not be justified solely by concerns of a flight risk or concerns about destruction of evidence.

MEXICO: Article 16 of the Constitution requires that any interception of any private communication be authorized by a federal judicial authority exclusively and upon the request of the federal authority appointed by law, or by the public official of the Public Prosecutor's Office of the federal entity. The competent authority shall establish and justify the legal reasons for the request, specifying the type of interception, its subjects, and its duration. The federal judicial authority may not grant these authorizations in electoral, tax, commercial, civil, occupational, or administrative cases, nor in cases of communications between the accused and his/her attorney.

The Mexican Supreme Court (SCJN, in Spanish) has also considered that accessing and analyzing data stored on a mobile phone without a judicial order is an infringement on the right to inviolability of private communications.[202] Likewise, the SCJN recently decided that access to communications metadata stored by telecommunications companies must have prior judicial authorization.[203] The SCJN considers an email interception that it infringes upon the right to inviolability of communications occurs the moment that the password of an account has been taken without judicial order or the user's consent, regardless of whether the content of the email is analyzed.[204]

Regarding location data, while constitutional interpretation has considered that communications metadata is protected in the same way that communications content is protected (meaning accessing them requires judicial authorization), the SCJN has stated that it is not necessary to obtain judicial authorization to monitor location data in real time. One example of this is the SCJN's decision regarding the complaint of unconstitutionality 32/2012,[205] (*acciones de inconstitucionalidad*), in which the majority of the Supreme Court considered that it is constitutional to allow the Public Attorney's Office (PGR) to monitor the geolocation of a mobile phone in real time, without the need for a federal judicial order.

COLOMBIA:[206] The Constitutional Court has stated that the general rule in the Colombian legal system is judicial safeguard, which requires a judge's authorization of decisions that interfere with the fundamental rights of the investigated or accused.[207] Exceptionally, the Office of the Attorney General is given the power to interfere with an

202 Supreme Court, Trial Chamber, Thesis Contradiction 194/2012.
203 Supreme Court, Second Chamber, Amparo in Revision 964/2015.
204 Supreme Court, Trial Chamber, Amparo in Revision 1621/2010.
205 Supreme Court, Plenary session, Complaint of Unconstitutionality 32/2012.
206 Abstract from Colombia Country Report. Juan Camilo Rivera and Katitza Rodriguez, "State Communications Surveillance and the Protection of Fundamental Rights in Colombia," Comisión Colombiana de Juristas, the Electronic Frontier Foundation, & Fundación Karisma, (2016). https://necessaryandproportionate.org/country-reports/colombia

individual's rights with the purpose of collecting information relevant to criminal investigations, though these actions are subject to subsequent judicial review. This exception applies only in the cases of searches, house visits, seizures, and interceptions of communications.[208] This exception must be strictly interpreted so that the safeguard of a prior judicial authorization is not bypassed. Under this rule, for example, the Constitutional Court has held that practices like selectively searching a database for an accused person's confidential information is not one of the activities that may be conducted by the sole request of the Office of the Attorney General of the Nation subject to subsequent judicial review by a judge.[209] Therefore, the Court has demanded that in order to proceed with such searches, prior judicial authorization is required.

However, the Office of the Attorney General is permitted to intercept communications, seize data storage devices and mechanisms, and track individuals, objects, and places involved in a criminal investigation without prior judicial authorization, but with subsequent judicial control. The Criminal Procedure Code establishes the cases and the procedures in which the Office of the Attorney General may make use of this subsequent judicial control. It indicates that the interception of communications must be subjected to judicial control within 36 hours.[210]

Criminal procedure legislation also stipulates that "competent authorities" shall be in charge of the technical proceedings of communications interception and its processing. Despite the vagueness of the law in relation to the authorities in charge of conducting the proceedings, the Constitutional Court endorsed it. The Court argued that the law does specify which authority gives the order and conducts the interception—the Office of the

---

207 Pedro Pablo Camargo's complaint of unconstitutionality against the second paragraph of Article 2, the third paragraph of Article 3 and the first section of Article 5 of Legislative Act Nº.03 of 2002, "which reforms the National Constitution", sentence C-1092, Constitutional Court, November 19, 2003, available at: http://www.corteconstitucional.gov.co/relatoria/2003/C-1092-03.htm

208 Alejandro Decastro González's complaint of partial unconstitutionality against Articles 14, 244, and 246 of Act 906 of 2004 "Which draws up the Criminal Procedure Code," sentence C-336, Constitutional Court, May 9, 2007. http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

209 Ibidem.

210 Articles 235 and 237 of the Criminal Procedure Code. This time period of 36 hours is made up by 12 hours for the judicial police to inform the prosecutor that the order to intercept communications has been given, plus the 24 hours the prosecutor has to conduct the legality control before a criminal judge. See Gustavo Gallón et al. complaint of unconstitutionality against articles 14, 15 (partial) and 16 of Act 1142 of 2007, "Which partially reform Acts 906 of 2004, 599 of 2000 and 600 of 2000 and adopt measures for the prevention and repression of criminal activity having a special impact on social coexistence and security," sentence C-131, Constitutional Court, February 24, 2009 —in which a study of constitutionality was carried out on article 237 of Act 906 of 2004. http://www.corteconstitucional.gov.co/RELATORIA/2009/C-131-09.htm

Attorney General of the Nation—and grants this office the power to determine which authorities conduct the interception and processing.

Moreover, despite that the law does not identify who these "competent authorities" should be, this may be determined through a systematic interpretation of the regulations related to the technical proceedings of communications interceptions. Interpreting Article 46 of Act 938 of 2004, the Court lays down that the aforementioned competence devolves upon the judicial police authorities—currently, those that fulfill these functions are the Technical Corps of the Judicial Police and the National Police.[211]

The Office of the Attorney General also has the power to order the retrieval of information from Internet logs or other similar technologies of an accused person in a criminal investigation, as long as there is judicial authorization within 36 hours following the seizure, and other requirements.[212]

Law 1321, Article 17 differentiates between the interception of communications and monitoring the electromagnetic spectrum. Colombian legislation provides that intelligence agencies do not have the power to intercept communications; intelligence agencies are authorized to monitor the spectrum only and can ask for stored data from ISPs. In the criminal context, a judicial control exists for criminal investigations that require communications interceptions, but such control does not apply to intelligence agencies because according to the law, intelligence agencies are authorized only to monitor the spectrum, not to intercept communications.

Additional due process safeguards are established in Article 29 of Colombia's Constitution, which states that any evidence obtained in violation of due process "is null and void."

ARGENTINA: Communications interception is permitted only with a judicial warrant in the criminal context.[213] It must be done through the authority in charge of intercepting communications, the Judicial Department for Communications Interception (DCCPJ), which functions as a subsidiary of the Supreme Court.

There is no clear regulation on whether judicial authorization can provide access to metadata and location data, but a Supreme Court decision has considered these data to be

211 Dagoberto José Lavalle's complaint of partial unconstitutionality against Article 52 of Act 1453 of 2011, "Which reforms the Criminal Procedure Code, the Children's and Adolescents' Code, the rules on the extinction of property law and stipulates other measures in relation to security," sentence C-594, Constitutional Court, (August 20, 2014). http://www.corteconstitucional.gov.co/RELATORIA/2014/C-594-14.htm

212 Articles 236 and 237 of the Criminal Procedure Code.

213 Judges are in charge of criminal investigations. The New Code of Criminal Procedure, now suspended, will grant this authority to public prosecutors.

on the same level as "private papers," which are protected by Article 18 of the National Constitution. Therefore, the same rules (prior judicial authorization) apply for metadata and for the actual content of personal communications.

Access to subscriber information, however, is not necessarily protected by the Constitutional guarantee that bars access to "private papers." A judge may request an ISP or a telecommunications company to provide the information it has on a subscriber directly, and the provider must comply with the request.

In the intelligence and counterintelligence context, communications interception and access to the content of communications is permitted only with a judicial warrant, and it must be done through the DCCPJ. This stems from the rules governing intelligence and counterintelligence activities, defined by the law as intelligence gathered for the purpose of national security, for preventing activities by actors who pose a risk for the security of the state, and for the purpose of investigating serious criminal activities.[214] These rules have applied to the Intelligence Agency (AFI) since December 2015. However, because the DCCPJ is the one responsible for issuing the judicial authorization, and it reports directly to the Intelligence Secretariat, we can't consider this an independent judicial control mechanism, since the directorate is overseen by an intelligence body within the executive branch.[215]

BRAZIL: Even though legislation seems to require judicial oversight for any and all interception of communications, courts interpreting these laws have varied the degree of judicial oversight and due process, depending on whether the State is surveilling the content of the communications or the subscriber information. This may partially be explained by Brazil's constitutional prohibition of anonymity, which has been wrongly used to justify access to subscriber data as a means of identifying wrongdoers.

Access to communications content requires compliance with constitutional protections and specific legal requirements that must be assured by a court order. Law 9.296 of 1996 requires authorities to obtain a court order prior to any interception. The *Marco Civil da Internet* (Law 12,965 of 2014) also requires judicial authorization to access subscriber information, metadata, location data, and communications content. Despite that, law enforcement authorities have interpreted both laws as permitting access to subscriber information without the court order of "competent authorities." However, who these "competent authorities" should be is not specified.

214 National Intelligence Act No. 25.520 of 2001, Article 2.

215 José Manuel Ugarte, Who is Watching the Watchers? Privacy International, Asociacion por los Derechos Civiles. (ADC) Available at: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

Some courts have ruled that prior judicial authorization is required under Law 9296 to access location data. Other laws specifically permit surveillance without prior judicial authorization. Laws 12,850 and 9.613/99 authorize civil police and the Public Attorney's Office to obtain subscriber information directly from the telephone companies without a warrant.

The requirements for accessing call records are unclear. Despite these being protected by the Constitution and only being permitted to be disclosed with a court order, abusive interpretations of Law 12,850 have allowed law enforcement to request access directly.

PERU: Article 2, paragraph 10 of the Constitution states that any communications, telecommunications, or private correspondence may be opened, seized, intercepted or wiretapped by an authority only with a warrant issued by a judge and with all the guarantees provided for by the law. The Peruvian legal framework also makes it clear that only a judge may authorize a prosecutor to listen to and control the communications of an accused person who is the subject of a preliminary or judicial investigation for one of a particular list of offenses.[216]

However, Legislative Decree 1182[217] did not incorporate a requirement for prior judicial authorization. Instead it grants the police warrantless 24/7 access to real-time user location data and device information in cases of blatant crimes (*flagrante delicto*).[218] A judge will not review compliance with these requirements until 72 hours after the police have accessed the data.

Requiring that a judicial authority reviews the legality of intelligence activities is a strong practice. In Peru, for example, intelligence laws require judicial authorization to implement any communications surveillance measures. In exceptional cases, judicial authorization may be granted after the measures are conducted. Thus, Legislative Decree 1141 on the Strengthening and Modernization of the National Intelligence System (SINA) and of the National Intelligence Bureau (DINI) requires authorization from any of the two ad hoc judges from the judicial branch, which is appointed specifically for this task by the Supreme Court to conduct surveillance. Approval will not be granted unless the National Intelligence Director demonstrates that the surveillance is strictly indispensable for the achievement of the purposes of intelligence activities.

---

216 *See* Law 27,697 and detailed in the Penal and Criminal Procedure Codes, as well as in the Protocol of Joint Action for Intervention or Record Keeping Telephone Communications or Other Forms of Communication, approved by Ministerial Resolution No. 0243-2014-JUS.

217 Republic of Peru, Legislative Decree No. 1182. http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html

218 Peruvian law defines flagrante delicto, to refer to a crime that is being committed, has just been committed, and up to 24 hours after it was committed.

When threats to national security arise and urgency is demonstrated, Legislative Decree 1141 allows the National Intelligence Director to authorize the execution of a special procedure to obtain information under the condition that the request is formalized immediately before an ad hoc chief judge who, within the following twenty-four hours, may validate it or order its cessation. The decree also stipulates that whenever the judge orders a special procedure's cessation, the authorities can appeal.

CHILE: Article 9 of the Criminal Procedure Code, titled "Prior Judicial Authorization," indicates that "all proceedings depriving the accused or a third party of exercising the rights guaranteed by the Constitution, or restricting or disturbing them, shall require a prior judicial authorization."

Article 222 of the Criminal Procedure Code applies to telephone and telecommunications interception. It states that a judge can grant an interception order if there is reasonable suspicion, based on particular facts, suggesting that a person has committed, or is organizing a crime. The law limits the crimes that may be investigated in this way to those that would be punishable by at least five years and a day of imprisonment.

Our Chilean country report exemplifies a specific case that used these powers in violation of this Principle:[219]

> *[I]n April 2012, the former chief of the Directorate of the Intelligence Police (Dipolcar, in Spanish), Major Gonzalo Alveal Antonucci was investigated due to alleged illegal interception of an officer's cellphone and the use of wiretappings to force this officer to quit his job.*[220]
>
> *According to the investigation, between May and July of 2010, the then-chief of internal affairs of Dipolcar required, without judicial authorization and in the context of a police investigation, the telephone interception of the cellphone lines of two officers from the same institution. In accordance with the Public Ministry, this information was used with a purpose different from the ongoing investigation. This is why Major Alveal Antonucci was sued for obstructing an investigation and recording private communications without judicial authorization. The investigation came to an end without a sentence.*[221]

---

219 Juan Carlos Lara and Valentina Hernández, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," Electronic Frontier Foundation & Derechos Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

220 La Segunda, "Golpe a la inteligencia policial: Fiscalía formalizará a ex oficial por escuchas ilegales" [A Blow to Intelligence Police: Public Prosecutor's Office will Sue Former Officer due to Illegal Wiretaps]. Urzúa, M and Candia, V, March 16, 2013.

221 Juan Carlos Lara & Valentina Hernández, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," Electronic Frontier Foundation & Derechos

In the intelligence context, Chilean legislation requires that intelligence authorities obtain judicial authorization to conduct procedures and obtain information through one of two procedures.

The first allows the National Intelligence Agency to request information from different State entities or gather it via publicly available information. For example, pursuant to Article 8 of Law 19,974, the National Intelligence Agency may request information from military authorities, law enforcement, and public security authorities including the Chilean Police (*Carabineros de Chile*) and the Chilean Investigations Police. The National Intelligence Agency also can request information from the various agencies that belong to the Administration of the State and from companies and institutions that depend on contributions from the State.

If, after receiving the information from the other state agencies, the Intelligence Agency still requires information, a second and separate procedure exists for it to obtain telephone, computer, and radio interceptions; computer systems and network interceptions; wiretapping and electronic recordings; and the interception of any other technological system used for the transmission, storage, or processing of electronic communications.

A judicial authorization is required to conduct these special procedures, and only the directors or heads of the intelligence agencies may submit these requests. Authorization to use the special procedures is directly issued by the Minister of the Court of Appeal of the territory in which the procedure is conducted or initiated, or by the corresponding institutional judge.
Additional due process safeguards are established in the Criminal Procedural Code, which states that any evidence that is obtained in violation of the law shall be omitted from legal proceedings.

EL SALVADOR: Article 176 of the Criminal Procedure Code (CPP) provides for the freedom to present facts or circumstances of a case as evidence in a criminal proceeding as long as they have been obtained in a way that respects all constitutional and legal guarantees. Article 1 of the Intervention of Communication Law *(Ley de Intervenciones de las Comunicaciones*) establishes the exceptional nature of communications surveillance, and the need for a warrant when carrying out such surveillance. The article also ensures the confidentiality of any private information that was obtained through interception but is unrelated to the investigation or criminal proceedings. Information obtained illegally, such as without due process, shall be excluded as evidence.

GUATEMALA: Guatemala requires a warrant for the interception of communications, and judges are required to oversee communications interceptions to ensure they operate in

Digitales, (2016). https://necessaryandproportionate.org/country-reports/chile

accordance with the law.[222]

222 Guatemala Chapter, Jorge Jiménez Barillas Hedme Sierra-Castro, Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, (2015). pdf; p. 151

7.
Public Oversight

States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.

Democracies are based on the separation of powers. The purpose of dividing state powers into judicial, legislative, and executive branches is to create checks and balances. Each branch has mechanisms in place to oversee itself and the others to prevent monopolization of power and abuse.[223]

Internal oversight in the executive branch usually consists of a commission inside the same national intelligence system. Oversight typically is a control meant to be outside the intelligence system, but inside the executive branch, oversight usually is assigned to the Ministry of Interior and Defense.

From the legislative perspective, the type of oversight in place depends on whether a country's congress or parliament is a unicameral body or a bicameral body. For example, if a bicameral body exists, it can either have one oversight commission per congressional body or a single commission with members from each chamber.

Finally, judicial oversight usually is implemented by requiring a judicial authorization to carry out surveillance during criminal or national intelligence investigations. However, these systems rarely provide the public oversight the principle requires. In some legal systems, public and civil grand juries provide oversight and auditing functions for various types of governmental operations, and they certainly could be implemented to review surveillance programs. Other times, the judiciary appoints a "special master" to oversee and monitor a program, particularly when the program is in need of significant reform. These special masters ensure program operations are complying with the law and may recommend changes to surveillance programs. A judicial body may in certain cases supervise the whole intelligence system, but no such controls exist in Latin America.

Latin America has almost no tradition of public oversight of intelligence activities. Most of the intelligence agencies in Latin America were formed at a time when the division of

223 The conceptualization of different types of oversight control in the intelligence and counter-intelligence framework where based on: Asociacion por los Derechos Civiles (ADC), Who is Watching the Watchers? Privacy International. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

powers was nonexistent—meaning the agencies were under military rule in which governmental operations were embedded in the executive power.[224] Because these intelligence agencies were part of the militarized dictatorships, most of the governments transitioned into democracies through a negotiation process with the military junta and thus were formed without well-placed controls or public oversight mechanisms. This is a main reason why most of the existing oversight mechanisms in place in the region are ineffective. Intelligence organizations in Latin America were formed at a time when democratic regimes were either weak, authoritarian or non existent meaning oversight mechanisms were placed *on top* of an inherited non-democratic culture.

Furthermore, the *enhanced* nature of Latin American presidentialisms also explains why oversight mechanism in the region are underperforming.[225] In Latin America, presidents are formally more powerful than, for example, their United States peers (they can declare emergencies, can introduce legislation in Congress, and so on).

Furthermore, it has been argued that the political dynamics in the region usually create a situation where Congress *delegates* power to presidents, either *de iure* or *de facto,* at least during the initial moments of a presidency.[226] If these analyses are correct, they could explain why legislative oversight mechanisms do not work. Intelligence agencies in Latin America have been powerful tools in presidential politics, specially used to spy on dissident groups, opposition politicians or independent journalists.[227]

These abuses have been widely documented: from the Peruvian scandals involving Vladimiro Montesinos, former director of the Peruvian Intelligence Agency (SIN) in the 1990s to the intelligence agency (DAS) wire-tapping revelations of the 2000s in Colombia, to the more recent upheaval involving intelligence agencies in Argentina. The use of intelligence agencies to support presidential politics and wishes more forcefully explains why oversight mechanisms do not work. The *delegative* nature of presidential politics explain, furthermore, why legislative oversight mechanisms usually approach their task with a *laissez faire* which is incompatible with the demands of modern democratic societies.

These institutional weaknesses can only be overcome if a strong civil society demands

224 José Manuel Ugarte, El control público de la actividad de inteligencia en América Latina. Ediciones CICCUS, Buenos Aires, (2012).

225 Mainwaring, Scott. "Presidentialism in Latin America." Latin American Research Review 25, no. 1 (1990): 157–179, 160

226 O'Donnell, Guillermo A., ed. *Counterpoints: Selected Essays on Authoritarianism and Democratization*. First Edition edition. Notre Dame, Ind: University of Notre Dame Press, 2003.

227 *See* Ramiro Álvarez Ugarte and Emiliano Villa. El (des)control de los organismos de inteligencia en la Argentina. Asociación por los Derechos Civiles - ADC, (2015). http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

transparency and accountability from the intelligence community. These efforts are usually trumped by the secrecy which surrounds both intelligence activities and organizations. However, the advances produced in the last decade in freedom of information laws throughout the region should provide an opportunity to pierce through these obstacles in order to strengthen citizens' capacity to supervise that part of the state which remains in the dark.

Therefore, aside from improving the institutional design for overseeing and controlling surveillance activities, the region should commit to implementing public oversight mechanisms and building strong civil society communities working on these issues.

EL SALVADOR: The interception of communications is overseen by the Public Ministry (made up of the General Prosecutor and the General Prosecutors Office *(Procuradoría General*, in Spanish).[228] Both governmental agencies are authorized to audit the agency in charge of intercepting communications, though their resolutions are not legally binding.[229] Articles 23 and 26 of the Special Law on the Interception of Telecommunications provide that the Prosecutor for the Defense of Human Rights, together with the Public Prosecutor *(fiscal general*), are legally empowered to draw up the "Operational Protocol of the Intervention Center" and must conduct periodic audits. They also have the right to conduct annual audits of the Interception Center's activities and submit relevant reports to the Committee on Legislation and Constitutional Issues of the Legislative Assembly.

The law empowers the prosecutor to perform specific audits related to violations of the right to privacy and secrecy of communications if he or she deems them appropriate. These audits are annexed to the general report sent to the Legislative Commission. Article 31 of the same law provides that the operation and safety of the Interception Center will be set forth in a regulation prepared by the public prosecutor. This creates a conflict of interest for public prosecutors since it is the prosecutor's own responsibility to develop the regulations that he or she will apply, as the prosecutor is the plaintiff in any criminal proceeding.

ARGENTINA: The Bicameral Commission on the Oversight of Intelligence Bodies and Activities is the country's legislative control mechanism. The Commission was created in 2001, with the approval of National Intelligence Law No. 25,520, and began operating in

228 El Salvador Chapter. Marlon Hernández, Anzora Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.), p. 90-91.

229 El Salvador Chapter. Marlon Hernández Anzora, Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.). p. 90-91.

2004.[230] According to the National Intelligence Law, the Commission's duties include supervising the National Intelligence System's agencies, overseeing its performance to ensure it complies with legal and constitutional regulations, and controlling intelligence activities. The law grants the Commission "great powers to control and investigate on its own initiative." For instance, the Commission can weigh in on any legislation that concerns intelligence activities. It also is required to prepare a confidential annual report on the National Intelligence System's effectiveness, which is submitted to the National Congress.[231]

However, the overall effectiveness of the Commission is undermined by several factors.

First, the executive controls the information to which the Commission has access. The law imposes a general restriction over information concerning intelligence and counterintelligence activities: "The access to such information shall be authorized in each case by the President of the Nation or by an official specially appointed to do so."[232] The Commission thus requires the authorization of the Intelligence Secretariat, which is part of the intelligence system in the executive branch, to access any of this information.[233]

Second, the Commission largely operates in secret. Civil society groups—*Asociacion por los Derechos Civiles* (ADC) and the Latin American Institute for Security and Democracy (ILSED, in Spanish)—point out that despite having requested information about the operational activities of the Bicameral Commission, they have received no response to such requests.[234]

Third, as noted, the Commission's mandated report is classified and not available to the public;[235] however NGOs ADC and ILSED discovered that a copy of the report was given to

---

230 José Manuel Ugarte, Who is Watching the Watchers? Privacy International, Asociacion por los Derechos Civiles - ADC, https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

231 José Manuel Ugarte, Who is Watching the Watchers? Privacy International, Asociacion por los Derechos Civiles (ADC). https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

232 Argentine Republic, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, Article 16.

233 José Manuel Ugarte, Who is Watching the Watchers? Privacy International, *Asociacion por los Derechos Civiles* – ADC. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

234 José Manuel Ugarte, Who is Watching the Watchers? Privacy International, *Asociacion por los Derechos Civiles* (ADC). https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf p. 14

Argentine deputies.[236]

In a report published in 2015 amid the scandalous death of public prosecutor Alberto Nisman, ADC concluded that the Bicameral Commission operates in such secrecy that it makes it impossible to assess whether it is operating correctly, if it all. Testimony gathered during the course of this investigation suggests that the Commission is not operating at all.[237] In 2016 a coalition of civil society organizations working on transparency for the intelligence sector argued that the new government's decisions on the matter do not only solve the old problems facing the intelligence community in Argentina, but have made them worse by naming partisan officials with no expertise and close links to members of the community who have been suspected of conducting illegal intelligence on public figures, involved in illegal smuggling of goods, and drug trafficking.[238]

CHILE: Within the executive branch, intelligence agencies have been unified since 2004 under the National Agency of Intelligence (ANI, in Spanish). ANI possesses oversight control and reports directly to the Ministry of Interior. It also has parliamentary oversight over the Chamber of Deputies, which is limited since the chamber does not have investigatory powers.[239] Article 37 of Law 19,974 prescribes that the intelligence system will report its activities to the congressional commission. Since the Director of ANI prepares the annual report on its intelligence operations and performance, the report is not independent, and its findings are not publicly verifiable since the report is not publicly available, and the operations described within it are carried out by secret commissions.

Article 36 states that the National Comptroller will study the legality of the decrees issued by ANI. The National Comptroller's decisions on legality are made through a documented

235 Articles 13.9 and 33.3 of Law No. 25,520 requires the Commission to issue an annual national report to Congress on all of the intelligence activities it oversees.

236 José Ramiro Ugarte, Who is Watching the Watchers? Privacy International, *Asociacion por los Derechos Civiles* (ADC). https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

237 Ramiro Álvarez Ugarte and Emiliano Villa. Who is Watching the Watchers? Privacy International. Asociacion por los Derechos Civiles. (ADC) Available at: https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

238 ICCSI. AFI: las declaraciones de Arribas y Majdalani que confirman que el Senado no debe brindarles el acuerdo (2016). http://www.iccsi.com.ar/afi-las-declaraciones-de-arribas-y-majdalani-que-confirman-que-el-senado-no-debe-brindarles-el-acuerdo. ICCSI, Acuerdo para no innovar (2016). http://www.iccsi.com.ar/agencia-federal-de-inteligencia-acuerdo-para-no-innovar

239 José Manuel Ugarte, Who is Watching the Watchers? Privacy International. Asociación por los Derechos Civiles – ADC. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

constitutional procedure *(toma de la razón)* and are classified according to the same law. Although Chile grants some oversight responsibility to its National Comptroller and parliament, these processes are not public.

PERU: In 2000, former President Fujimori dismantled the National Intelligence Service (SIN, in Spanish) after a corruption scandal was uncovered within the agency.[240] In 2006, Act 28,664 formed the National Intelligence System (SINA, in Spanish) and the National Directorate of Intelligence (DINI, in Spanish), which specialize in nonmilitary national intelligence and report directly to the President.[241]

The Intelligence Committee of the Congress of Peru serves as legislative control and supervises all SINA activities. It reviews intelligence plans and any files presented to the judges handling the communications interception requests. The Committee also receives an annual report directly from the Intelligence Director. Unlike those of other countries, Peru's Intelligence Committee can investigate on its own will, but must do so under the direction of the DINI.[242] Therefore, the scope of the investigation is undefined.

In spite of these controls, Peru has not succeeded in preventing abuses committed by its intelligence agencies. However, it has maintained some public accountability. Journalistic investigations have led to complaints concerning the DINI and the illegal surveillance of politicians, businessmen, and journalists. Consequently, in February 2015, the President of the Council of Ministers announced her decision to dissolve the DINI and recreate the national intelligence structure. A month later, these revelations prompted a successful motion of censure to the entire cabinet of ministers presided over by Ana Jara, who was the first censure in the country in more than 52 years.[243] The intelligence system was subjected to reorganization immediately.[244]

---

240 José Manuel Ugarte, Who is Watching the Watchers? Privacy International. Asociación por los Derechos Civiles - ADC. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

241 José Manuel Ugarte. El control público de la actividad de inteligencia en América Latina. Ediciones CICCUS, Buenos Aires, 2012.

242 José Manuel Ugarte, Who is Watching the Watchers? Privacy International. https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

243 El Comercio, "Ana Jara was censored by Congress based on DINI's illegal surveillance" ["Ana Jara fue censurada por el Congreso por rastreos de la DINI"]. (2015). http://elcomercio.pe/politica/congreso/ana-jara-congreso-debatira-pedido-censura-caso-dini-noticia-1801055

244 El Comercio, "Government Closes the DINI for 180 Days to Restructure It" ["Gobierno cerrará la DINI por 180 días para su reestructuración"], (2015). http://elcomercio.pe/politica/gobierno/ollanta-humala-dijo-que-analizara-cierre-dini-noticia-1790387

COLOMBIA: The Colombian intelligence law (No. 1621 of 2013) provides for internal and external controls on intelligence activities.[245] Inspectors inside the intelligence agencies must submit an annual report to the Ministry of Defense describing whether the intelligence activities were conducted within their legal framework and constitutional boundaries.[246] A copy of this report should be sent to the Legal Commission on the Supervision of Intelligence and Counterintelligence Activities.[247]

Additionally, Colombia has a Joint Intelligence Board [*Junta de Inteligencia Conjunta*] made up of the directors of each of the military forces in Colombia and the Ministry of Defense.[248] The Board is in charge of supervising all of the intelligence agencies according to the Intelligence Plan[249] and is required to report to the Legal Commission annually. Both reports are classified and not accessible to the public.[250]

External control is carried out by the legislative branch, specifically the Legal Commission on the Supervision of Intelligence and Counterintelligence Activities. This commission has three main functions: to conduct political control and oversight, to check on the efficient use of resources, and to verify the legality of the practices carried out by intelligence agencies.

The powers given to the Legal Commission are aimed at controlling the performance of the oversight mechanisms of intelligence activities. Article 22 of Law 1621 of 2013 indicates that the Legal Commission shall be able to meet with the Joint Intelligence Board, learn about the annual reports written by the inspectors, request further information from them and from the offices of internal control, summon the heads and directors of intelligence agencies, and become acquainted with the national intelligence objectives outlined in the National Intelligence Plan. However, to verify the legality of the activities conducted by

245 Colombian Republic, Law No. 1521 of 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

246 Colombian Republic, Law No. 1521 of 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf Article 18.

247 Colombian Republic, Law No. 1521 of 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Article 18.

248 Colombian Republic, Law No. 1521 of 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Article 12.

249 Colombian Republic, Law No. 1521 of 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Article 12.

250 Colombian Republic, Law No. 1521 of 2013. http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf. Articles 18 and 13 (h).

intelligence and counter-intelligence agencies, the Legal Commission is limited by the fact that it can weigh in only on the information that the agencies deliver to it. This is problematic since many of the activities these agencies conduct go unreported or are considered classified.

Lastly, Colombian intelligence law has two additional safeguards. Article 18 protects whistleblowers. It dictates that members of intelligence and counterintelligence agencies should report any irregularities related to the activities carried out within their agencies to their directors or to the head of the Internal Control Department. In all cases, the whistleblower's identity shall be protected. Article 23 requires an evaluation of the credibility of the Commission itself at least once per year.

According to Law 1321 of 2013, the Legal Commission have eight members, four senators and four members of the Chamber of Representatives.[251] Currently, the commission is not functioning.

BRAZIL: Brazil provides another example of the limitations imposed on political oversight mechanisms that prevent transparency concerning the activities of intelligence and counterintelligence agencies.

The executive branch has internal and external mechanisms of control. Internally, the Director General of ABIN has oversight control, while the Chamber of External Relations and National Defense has external control. According to intelligence policy analysts, it is unclear whether the latter will function on a permanent basis.[252]

On the legislative side, there is a Joint Commission in the National Congress that is in charge of supervising such agencies. Nonetheless, there is almost no information about the functioning of the Commission, except that since its creation in 2000, it has held two or three meetings per year.[253] In addition, there is little information on the Brazilian Intelligence System (SISBIN, in Spanish) available.

There are no oversight entities on the judicial side; however, requests for communications interceptions or access to data do require judicial authorization (Civil Rights Framework for the Internet Article 10.1).

---

251 *See* Congress Website. Los Andes University. http://www.congresovisible.org/comisiones/39/

252 José Manuel Ugarte, Who is Watching the Watchers? Privacy International. *Asociacion por los Derechos Civiles* (ADC) https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

253 José Manuel Ugarte, Who is Watching the Watchers? Privacy International. *Asociacion por los Derechos Civiles* (ADC). https://www.privacyinternational.org/sites/default/files/Who's%20Watching%20the%20Watchers_0.pdf

URUGUAY: Uruguay lacks external oversight mechanisms. This nation is characterized by an intelligence system that is decentralized and fragmented, making central, coordinated oversight difficult.[254] In 2010 Uruguay began undergoing a process to reorganize its intelligence system in order to centralize all the agencies under the National Intelligence System. In 2014 the proposed bill was not approved and currently is being re-proposed in the Uruguayan parliament.[255]

HONDURAS: Honduras lacks an independent oversight body to oversee intelligence activities.[256]

254 Samanta Curti, Reforms in South American Intelligence agencies, "Reformas de los Sistemas de Inteligencia en América del Sur." http://www.kas.de/wf/doc/17940-1442-1-30.pdf

255 El País, Draft Bill for Intelligence Law comes alive again Reflotan Proyecto de Ley de Inteligencia. http://www.elpais.com.uy/informacion/reflotan-proyecto-ley-inteligencia.html

256 Honduras Chapter, Edy Tábora Gonzales.Fundación Acceso, ¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos. Peri, Luciana (coord.).p. 229

8.
Integrity of Communications and Systems

States should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes. Individuals have the right to express themselves anonymously; States therefore should refrain from compelling the identification of users.

The Integrity of Communications and Systems Principles seek to protect against technological mandates that put service providers' infrastructure at risk. They also protect the freedom to secure communications through encryption technology, and the ability to communicate anonymously.[257]

The right to use encryption

Encryption protects the security of a person's communications. It also protects free expression by preventing automated technical censorship systems from blocking access to particular content and even to specific key words. It promotes expression indirectly by giving users confidence that the confidentiality of their communications or browsing history are protected by technical means.

In the absence of encryption, online communications can be intercepted easily.[258] Internet intermediaries that store and process communications often are in a position to possess and read all of the unencrypted communications that pass through their networks.[259]

---

257 This is an abstract of our own submission. See Katitza Rodriguez, EFF Comments Submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2015, https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-promotion-and-protection-right

258 *See* e.g., *Firesheep* (2010). Retrieved February 6, 2015, from http://codebutler.com/firesheep. *See also* John P. Mello Jr. , *Free Tool Offered To Combat Firesheep Hackers*, PCWorld, Retrieved February 6, 2015, from http://www.pcworld.com/article/211531/free_tool_offered_to_combat_firesheep_hackers.htmlSeth Schoen, Richard Esguerra (2010). *The Message of Firesheep: "Baaaad Websites, Implement Sitewide HTTPS Now!*, EFF. Retrieved February 6, 2015, from http://www.eff.org/deeplinks/2010/10/message-firesheep-baaaad-websites-implement. EFF, *Tool Offers New Protection Against 'Firesheep'*, November 23, 2010. Retrieved February 6, 2015, from http://www.eff.org/press/archives/2010/11/23.

259 Electronic Frontier Foundation, Animated Overview: How Strong Encryption Can Help Avoid Online Surveillance, Surveillance Self-Defense, https://ssd.eff.org/en/module/animated-overview-how-strong-encryption-can-help-avoid-online-surveillance

Service providers should be able to design systems that ensure end-to-end encryption so that they ensure that a message can be read by its intended recipient and no one else. Despite encryption's central role in every aspect of information security, efforts to make it more readily and conveniently available to the public often draw disapproval from governments. Some countries have attempted to use legal measures to limit the public's access to encryption tools or to try to exact security-weakening concessions from manufacturers and software developers.[260]

In high-profile cases, as well as in closed-door negotiations, governments have directly pressured individual manufacturers by threatening to ban or block their products and services. From 2010 to 2013, for instance, Canadian mobile manufacturer BlackBerry was involved in public confrontations with the governments of Saudi Arabia, the United Arab Emirates, and India, who objected to BlackBerry's use of strong encryption in Canada and suggested that BlackBerry's products might be banned in their territories.[261] The manufacturer responded by agreeing to deliver a solution that would grant governments access to spy on non-enterprise users.[262]

Some argue there should not be any "impenetrable technology." This demand amounts to a technology mandate and calls for a draconian regulatory framework. The implications this has on innovation, as well as the open-source community as a whole, are dire. Some open-source developers already have taken a stand against building back doors into software.[263] Any additional mandates put on service providers would require providers to spend a significant amount of money making their technologies compliant with the new rules, and these costs would likely be passed onto their customers.

Technological mandates

Laws requiring telecommunications providers to ensure that law enforcement can access their records, either on a case-by-case basis or by building in a permanent access point for the government, can be contrary to the Integrity of Communication and System Principle. This "surveillance by design" can impede pro-privacy innovation by constraining the number of options available to those who are developing Internet and mobile services.

Implementation of technical capacity requirements streamline and automate wiretapping and other communications interception processes, making interception cheaper, faster, and

260 *See* Bert-Jap Koops (2013), *Crypto Law Survey*. http://cryptolaw.org/ (listing known export, import, and domestic use controls on encryption).

261 *See*, e.g., BBC News (2010), *Two Gulf States to Ban Some BlackBerry Functions*. http://www.bbc.com/news/world-middle-east-10830485.

262 *See* Wired News (2013), *BlackBerry gives Indian government ability to intercept messages.* http://www.wired.co.uk/news/archive/2013-07/11/blackberry-india

263 Zooko O'Whielacronx (2010), *Statement on Backdoors*. http://tahoe-lafs.org/pipermail/tahoe-dev/2010-October/005353.html

more convenient. Such streamlining reduces human involvement and oversight in the process, which may reduce providers' ability to challenge or expose abuses such as illegal wiretapping. Wiretapping equipment also has been hacked, remotely activated, and used to covertly carry out illicit interception for espionage purposes. Technical mandates may prevent providers from making changes to their networks for security or engineering purposes, and in some cases forbid or discourage providers from giving users access to cryptographic tools that could protect their communications against government or third-party wiretapping.

It also is worth noting that a carrier's obligation to be capable of performing interceptions is distinct from the ability to decrypt communications or to deploy encryption technologies to which the carrier does not possess the key. However, these questions may not have been considered expressly by legislators in most jurisdictions and virtually have never been tested or examined by courts.

ARGENTINA: On encryption: There is no law in Argentina that prohibits the use of encryption. By applying the constitutional *reserve* principle, which states that anything that is not forbidden is permitted, we can conclude that encryption and the use of encrypting technology is legal in Argentina.

On lawful interception: Argentinean law provides several safeguards against illegal searches and seizures. On the one hand, the National Intelligence Act of 2001 establishes that all interceptions—whether conducted within a criminal investigation or for intelligence gathering purposes—must be authorized by a judge.[264]

Such authorization, as stipulated by the legislative framework, "must be granted in writing and be justified by a detailed description on how the telephone number(s) or e-mail address(es) or any other communications are going to be intercepted or seized."[265]

Interception orders last 60 days but, upon request, can be extended for another 60 days. The interception request is signed by the relevant authorities and is sent to telecommunications companies and ISPs through an official communication which must be complied with if it meets formal requirements. The obligation for intermediary companies to comply with interception orders stems from Article 22 of the National Intelligence Act of 2001, which states that these companies are "responsible of executing the diversion of the [targeted] communication." It should be noted that there is no regulation that prevents companies from deploying confidentiality tools that would make it impossible for them to comply with interception orders.

264 Law 25.520, Article 19.

265 Law 25.520, Article 18.

COLOMBIA: On encryption: Colombia has a broad legal prohibition, dating back to 1993, on any use of encryption technology for communications in the electromagnetic spectrum. It also prohibits the use of voice encryption technology by anyone other than certain government officials. These prohibitions appear to apply to virtually all of the routine uses of encryption in today's communications technologies, but the laws do not seem to be enforced in practice.

On lawful interception: Decree 1704 compels telecommunication services, including Internet service providers such as Movistar and Claro, and network providers *(proveedor de redes*), to facilitate easier wiretapping by introducing technical capacity requirements, supporting government-approved technology standards for categories of data interception, and turning data over to the Prosecutor's Office (*Fiscalía General de la Nación*) upon request.[266] Content and application providers such as MercadoLibre.com and Tapssi.com are excluded from this decree.[267]

Telecommunication network providers and service providers carrying out business within the national territory are required to ensure that the necessary technological infrastructure to provide competent authorities connection and access points to capture communications traffic in their networks is implemented so that the agencies with permanent judicial police functions may perform all activities required for the interception of communications, subject to prior authorization by the National Attorney General or his/her designee.

Telecommunications network and service providers also must respond in a timely manner to the interception of communications requests made by the National Attorney General, in conformity with this decree and the legal framework currently in force, to facilitate interception activities by permanent judicial police agencies.

Moreover, the Ministry of Information and Communications Technologies may, as necessary, define the technical specifications of connection points and type of traffic to be intercepted, impose on telecommunications network and service providers, through general resolutions, technical conditions and models as well as systematic protocols, and respond to the National Attorney General's requests for interception.

EL SALVADOR: On encryption: Article 42-D of the telecommunications law states that telecommunications providers "must decrypt, or ensure that authorities can decrypt, any client or subscriber communications in order to obtain the information referred to by the preceding articles in cases in which the encryption has been provided by the service

266 Colombia, Decree 1704 of 2012, article 2.

267 Article 6 of Law 1341 of 2009 defines "Information Technology and Communications - ICT" and request the Ministry of Information Technology and Communications to create a glossary. Resolution 000202 of 2010, Internet companies are consider content and application providers, and not telecommunication providers.

operator." This may be interpreted as forbidding providers from deploying or providing encryption technologies that they are unable to decrypt, and it remains unclear whether the companies can be punished for failing to turn over information that they do not possess.

NICARAGUA: On lawful interception: Chapter VIII, Article 65 of the "Law on the Prevention, Investigation and Prosecution of Organized Crime and the Administration of Seized, Confiscated and Abandoned Assets" creates a technological mandate to design their services in a surveillance-friendly manner, stating that:

> *"[P]rivate or public companies that provide telephone, computer or other electronic communication services [...] shall provide the conditions, material facilities and techniques necessary for the interceptions to be effective, safe and confidential [...]"*

On encryption: There are no legal or regulatory limitations on encrypting communications or content encryption.

BRAZIL:[268] Brazil's Constitution prohibits anonymity expressly. The use of encryption is not prohibited by law specifically.[269] However, the Brazilian ANATEL requires that telecommunication providers maintain the technological resources and facilities needed to breach telecommunications secrecy within the scope of court orders. ANATEL also requires that providers bear the financial costs of maintaining such technology (Art. 26, *parágrafo único*, Resolution nº 73/98; Art. 90, Resolution nº 477/07; Art. 24, Resolution nº 426/05). The Brazilian Interception Law compels telecommunications providers to cooperate with law enforcement in wiretapping proceedings authorized by law (Art. 7, Lei n. 9.296/96). While this language may be interpreted as constraining, the use and type of encryption and similar technologies implemented by those actors, these (CALEA-type) obligations do not directly extend to content providers, which include third-party applications such as WhatsApp. The rising popularity of popular encrypted messaging apps in Brazil such as WhatsApp has stirred intense debate around encryption in the country.

In May 2016, a judge who demanded personal data from WhatsApp as part of a drug-related investigation in Brazil's northeastern state of Sergipe ordered the five main Internet service providers to block access to WhatsApp's messaging service for 72 hours. ISPs that did not block WhatsApp were threatened with a fine of approximately $142,000 USD per day. In February 2016, the same judge ordered the arrest of the vice president of Facebook Brazil, as

---

268 Electronic Frontier Foundation & Internet Lab, Frequently Asked Questions on State Communication Surveillance. https://necessaryandproportionate.org/country-reports/brazil

269 Dennys Antonialli, Jacqueline de Souza Abreu, "Brazil: State Surveillance of Communications in Brazil and the Protection of Fundamental Rights," Electronic Frontier Foundation & InternetLab (2015). https://necessaryandproportionate.org/country-reports/brazil

Facebook owns WhatsApp. The arrest came after the judge had served WhatsApp with a series of fines for withholding information from the court. Facebook's vice president was released[270] after another Brazilian judge called his incarceration "unlawful coercion."

WhatsApp's lawyer told reporters what he had told the court: WhatsApp cannot provide the content of communications carried out on its messaging service because the company has no record of those communications.[271] That may be for technological reasons—many WhatsApp communications are end-to-end encrypted. It also may be the result of the company's own logging policies: WhatsApp says it makes no permanent record of the data that the court requires. In either case, the court was punishing a single employee for the company's inability to comply with its own impossible demands.[272] In December 2015, Brazilian ISPs also were required to block Brazilians' access to WhatsApp in an unrelated case from São Paulo, an order that was overturned quickly on appeal.

GUATEMALA: On encryption: There are no legal or regulatory limitations on development and use of encryption.

HONDURAS: On encryption: There is no constitutional rule governing the promotion or limitation of encryption or anonymity. None of these issues have been addressed by the Constitutional Chamber of the Supreme Court. However, the Honduran Communications Interception Law *(Ley de Intervención de las Comunicaciones)* is potentially ambiguous with regard to the interception obligations of service providers. It requires communications service providers to make "all material, technical, and human resources necessary to ensure that interception is effective, secure, and confidential" available to government entities; it remains unclear to what extent this would limit such providers from adopting or promoting security or encryption tools, which limit their own access to user communications.

PERU: On encryption: There are no legal or regulatory limitations on the development and use of encryption.

On lawful interception: Article 230 of the Criminal Procedural Code makes clear that ISPs should keep their systems "in close proximity to" police to facilitate the execution of any surveillance orders. Following this rule, any kind of anti-surveillance measure deployed by the ISP could be read as a violation of that obligation:

270 Brazil judge orders release of Facebook executive, Yahoo, (2016). https://www.yahoo.com/news/brazil-judge-orders-release-facebook-executive-130638549.html?ref=gs

271 Sérgio Rodas, Executivo do Facebook é preso por causa de apuração envolvendo WhatsApp, (2016). http://www.conjur.com.br/2016-mar-01/executivo-facebook-preso-causa-apuracao-envolvendo-whatsapp

272 Apesar de problemas judiciais, WhatsApp diz que não vai mudar (2016). http://www1.folha.uol.com.br/tec/2016/03/1745230-apesar-de-problemas-judiciais-whatsapp-diz-que-nao-vai-mudar.shtml

[4]. The concessionaires of public telecommunications services must provide the geolocation of mobile phones immediately and take the necessary steps to achieve the interception (intervención) or the recording of communications that has been ordered by a court decision, in real time, continuously, for 24 hours a day, 365 days a year, under penalty of legal liability in cases they fail to do so. The employees of the designated companies must keep such obligations a secret, except if they are called upon to testify about them in court. These concessionaires shall grant the National Police of Peru access to their technology and ensure its compatibility and interconnectedness with the national police's Communications Interception and Control System (Sistema de Intervención y Control de las Comunicaciones). Also, when, for reasons of technological innovation, the concessionaires update their equipment and software, they are obliged to ensure their technology continues to be compatible with the National Police of Peru's Communications Interception and Control System.

On the other hand, ISPs have a general duty protect the communications of their users to the best of their abilities. For instance, by providing or allowing the use of end-to-end communication, ISPs imply that they could not forbid their users from using end-to-end encryption.

CHILE: On encryption: There are no legal or regulatory limitations on the development and use of encryption.

On lawful interception: Carriers in Chile are required to cooperate with wiretap orders, to maintain the technical capacity to perform wiretaps, and to inform the telecommunications authority of the kind of technology they will have available to do so. They have no prohibition on deploying confidentiality tools.

MEXICO: On encryption: There are no legal or regulatory limitations on the development and use of encryption. Companies have no prohibition on deploying encryption tools.

9.
Safeguards Against Illegitimate Access and Right to Effective Remedy

States in the region define in their criminal law various offenses for accessing communications without authorization or arbitrarily revealing communications or personal data. Generally, the laws establish penalties for illegal interception or improper disclosure of private information, and remedies for these offenses.

PERU, BRAZIL, & ARGENTINA: Peruvian Law 27,697 notes that those involved in the investigative process, including the judge, court staffers, prosecutor, support staff, National Police, and technical witnesses, must keep the information obtained as a result of a communications interception confidential. The same duty of confidentiality exists in Brazil[273] and Argentina.[274]

In the intelligence context, Argentina's intelligence legislation imposes criminal sanctions on members of intelligence services who unduly intercept, seize, or divert the course of communications that are not addressed to them.[275] In 2015, Law No. 25,520 on National Intelligence added criminal provisions to punish those who, permanently or in passing, engage in the tasks regulated by this law: If they "unduly intercept, seize or divert the course of postal, telegraphic or fax communications, or of any other system designed to send objects or transmit images, audios, or data packets, or any other kind of information, file, records and/or private documents, or documents of restricted or unauthorized reading, or documents that are not available to the public, which are not addressed to them."[276]

This law also imposes criminal penalties on those who, having a judicial order and being compelled to do it, "fail to destroy or delete the copies of recordings, postal, cable, or fax interceptions, or any other element showing the result of interceptions, seizures or diversions."[277] Also, according to this law, those public officials or government employees who perform intelligence activities prohibited by this law must also be punished.[278]

273 Republic of Brazil, Law 9,296 of 1996, Article 8.

274 Republic of Argentina, National Criminal Procedural Code, Article 143.

275 Argentine Republic, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, Article 42.

276 Argentine Republic, Law No. 25,520 on National Intelligence, Official Journal of December 6, 2001, Article 42.

277 Ibid, Article 43.

278 Ibid, Article 43b.

Furthermore, the Argentinian legislation on intelligence services does not include incentives for intelligence agents to publicly disclose information about the practices that infringe on fundamental rights.[279]

While formal guarantees exist, there are no known cases of intelligence officers who have been punished by the intelligence authorities themselves or by the bodies in charge of overseeing their operations for illegally breaching a citizen's private communications. There have been cases in which the Judiciary has found out about illegal breaches, but those have been in the context of civil complaints and have resulted the granting of damages.[280]

COLOMBIA: Criminal law specifies a series of crimes that punish illegal communications surveillance, including the interception of communications without a warrant. However, Article 250 of the Constitution allows the Attorney General's Office to intercept communications with subsequent judicial review, thus creating a pathway for it to address any violations. Additionally, a reform of the Penal Code passed in 2009 to protect individuals' information added a new title to this code, which established offenses including abusive access to a computer system, illegitimate interference with computer systems or networks of telecommunications, interception of computer data, computer damage, and the use of malware and spoof websites to capture personal data.[281]

CHILE: Chilean criminal law includes penalties for those who violate the right to privacy. Telecommunications Services Decree No. 18 of January 2014 punishes the interception or malicious capture of any type of signal without authorization. The imprisonment and fine penalties increase if there is a public or private broadcast of the content of these signals. The Criminal Code, Article 161-A, criminalizes those who capture, records or intercept private conversations without permission. The penalty includes a lesser fine or imprisonment but increases if the criminals spread the conversations he or she obtained.

When surveillance occurs pursuant to law, the law requires telecommunications companies to remain quiet when they become aware of communications surveillance, unless they are requested to testify in a criminal proceeding. It is uncertain, however, what penalties are imposed if this duty is violated. This latter provision may be a problem for the user notification principle; this is discussed further in the section related to that principle.

279 See, Bertoni, Eduardo, "The Intelligence Law, a Lost Opportunity" [*Ley de inteligencia, oportunidad perdida*], Bastión Digital, (2015). http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgJU.dpuf.

280 National Court of Appeals in Administrative Matters. Case of Ventura, Adrián c. Estado Nacional EMGFFAA s/ daños y perjuicios. Decision of February 28, 2008 (p. viii).

281 Republic of Colombia, Law 1273 of 2009.

10.
Final Recommendations

Many of the region's surveillance laws are difficult to understand because several relevant provisions are scattered across many different laws that are intended to cover a variety of issues—not just surveillance. To ameliorate this problem, countries should have one comprehensive surveillance law instead of multiple provisions dispersed throughout many laws, resolutions, and decrees.

Surveillance laws should not make arbitrary distinctions between different kinds of protected information, such as content, metadata, geolocation, subscriber, retained data, and real-time communications. Instead, access to any type of protected information should be permitted only when, at minimum, an impartial judge has issued an order based on the necessity, proportionality, adequacy, and legitimate aim of the requested measure. Moreover, legal safeguards such as due process, transparency, public oversight, notification, and the rights to effective remedy should all be adopted within this region's countries.

Recommendations related to individual principles

1. On the principle of legality

When regulating access to and collection of personal, protected information, States have a duty to enact clear legislation that cannot be arbitrarily interpreted. For this reasons, we recommend the following:

1. Brazil should modify Article 21 of Criminal Organizations Law 12,850, which criminalizes the refusal or failure to submit "account information, logs, documents, and information requested by the court, Public Attorney's Office, or the chief of civil police during the course of the investigation or proceedings" and establishes penalties ranging from six months to two years of incarceration. Article 21 has obscured situations in which a warrant is required. Brazil also should modify Article 17 of Law 12,850 to establish strict limits on mandatory data retention for telecommunications companies.

2. Colombia should modify Decree 1704 of 2012 to clarify that telecommunications and phone companies are not required to retain information that they do not need for business purposes.

3. El Salvador should repeal Article 31 of the Special Law for the Interception of Telecommunications and prepare a legal norm that publicly determines the procedure for the interception of telecommunications. Similarly, Peru should enact

a legal norm to establish the procedure for access to geolocation data of cellphones and electronic devices so that the extent and basis of the government's authority is publicly known.

4. Guatemala should modify Article 48 of the Law Against Organized Crime to specify what kind of communications can be intercepted.

5. Honduras should modify Articles 3 and 10 of the Communication Interceptions Act to indicate explicitly the types of surveillance techniques and technologies that are or are not permitted.

6. Similarly, Chile, Paraguay, Guatemala, and Uruguay should remove loopholes in their legislation (such as Article 200 of Paraguay's Criminal Procedural Code) that can be interpreted as authorizing any and every surveillance method that may be developed in the future. They should provide clarity about the techniques and technologies that are legal, and under which circumstances they may or may not be used. Other States should immediately stop using malicious software for spying purposes because their laws do not authorize its use.

7. States should hold public hearings to examine whether IMSI-catchers or any other new surveillance technologies are in use in their territories and to identify the kinds of entities that are using them. Where such devices are found to be in use, legislation should be updated to address them in a way that complies with the 13 Necessary and Proportionate Principles. Updates should include judicial authorization and public oversight requirements, as well as transparency obligations to avoid abuses of power. For example, such a law must ensure that any data collection using cell-site simulators is authorized by an order issued by a neutral judge based on necessity, proportionality, adequacy, and legitimate aim. In general, States should ensure that invasive new surveillance technologies are controlled by law in a stronger manner than techniques like wiretapping have been, and that a culture of secrecy and legal vacuum do not surround new technology.

2. On the principle of legitimate aim

All States in the region should limit the circumstances under which authorization for communications surveillance is granted; in addition to wiretapping, this includes all forms of surveillance, such as device location, or metadata monitoring. For example, States could specify that communications surveillance can be used only for the investigation of a certain list of serious crimes. Additionally, States could limit surveillance to evidentiary use for defined serious crimes and ensure that surveillance measures only proceed when there is a reasonable suspicion that the surveillance will yield admissible evidence.

States like Honduras that do not limit the scope of surveillance activities should modify their legislation to fulfill these requirements.

3. On the principle of necessity

States in the region should authorize communications surveillance only when it is the sole way to achieve a legitimate aim or when it is the least likely means of infringing on human rights. Following Brazil's example, States should specify that a judge cannot authorize the interception of communications when the desired evidence also could be obtained by another means. It also is good practice to specify the cases in which forms of communications surveillance cannot be carried out by the authorities under any circumstances.

4. On the principle of adequacy

States of the region should limit the use of communications surveillance to cases where there is reasonable belief that a person is responsible for a crime and that surveillance would be useful to the investigation of that crime.

5. On the principle of proportionality

States in the region should adopt rules that fairly balance the legitimate aim pursued by communications surveillance and the fundamental rights affected by these activities. Specifically, States should:

1. Require that any surplus data that has been collected for the purpose of surveillance be destroyed or returned promptly.

2. Require judges to issue only warrants that are highly specific in their authorization of communications surveillance, ensuring that the judges know and have examined the particulars of the proposed surveillance activities (from targets and methods, to goals and timeframes).

3. Restrict the use of communications surveillance to cases in which there is a strong degree of certainty a crime has been committed.

4. Adopt measures such as targeting and minimization to limit the impact that technical surveillance methods have on the people and devices that are not the intended targets.

5. Place time limits on communications interceptions. States like Brazil, whose legislation establishes that wiretapping orders can be renewed indefinitely, should modify these provisions.

6. Reject data retention laws that compel ISPs and telecommunications providers to retain telephone calls and subscriber data or metadata of an entire population for potential use by law enforcement. Mexico, Peru, Chile, Brazil, Paraguay, Colombia, and Honduras should repeal the laws that require such retention. The European Union has ruled that data retention laws violate privacy rights, but Latin America's

progress in this area is lagging.

6. On the principle of competent judicial authority

States in the region should require that restrictions on the right to the inviolability of communications be reviewed by judicial authorities. As a general rule, judicial review should precede the surveillance of personal communications. Judicial review occur after the inviolability of communications has been breached only in specified emergency cases in which life or physical integrity is at risk.. In all cases involving judicial review *a posteriori*, review must occur promptly after the restriction. States should clarify that each specific act of surveillance requires a separate judicial authorization and that the renewal or expansion of any authorized surveillance measure requires new judicial approval.

Judges should have sufficient knowledge and receive appropriate briefings to better understand the details of each proposed surveillance measure, and their impact on the communications systems. For example, judges may be unaware that tower dumps (activity records from cellular infrastructure) inevitably include data about a large number of innocent third parties who are not the intended targets of surveillance. As such, States should explore the idea of obtaining independent technical experts to help educate judges.

7. On the principle of due process

States in the region should incorporate due process by, at a minimum, decreeing that private documents obtained without a judicial warrant and without the appropriate legal safeguards will have no legal effect. States should also act to avoid informal arrangements, including voluntary cooperation in surveillance, between the private sector and government to facilitate communications surveillance; instead, surveillance should be carried out pursuant to formal requests made in accordance with law.

8. On the principle of user notification

States in the region should incorporate an obligation to notify those directly affected by surveillance into their laws. To the extent that there must be exceptions to when such notification must be provided, these exceptions must be defined in detail and employed as infrequently as possible. Entities requesting surveillance must justify why notification must be delayed in particular cases.

Where secrecy concerning surveillance is necessary for a compelling government interest, the law must provide for how and when this secrecy will end and how targets or other persons affected by surveillance may be informed eventually and, where appropriate, obtain a remedy against illegal surveillance.

9. On the principle of transparency

States in the region should enact laws that encourage companies to maximize the amount of

information they disclose to the public about their surveillance capabilities and practices. Such transparency will help citizens hold their governments accountable. Mexico's General Law on Transparency and Access to Public Information encourages providers to publish information related to governmental requests for information. They can follow the example of Mexico, whose law encourages companies to provide information related to government requests for data.

Companies should publish transparency reports voluntarily showing statistics about the nature and scope of their interaction with governments and participation in surveillance activities.

10. On the principle of public oversight

States in the region should implement public oversight mechanisms to control potential abuses of power when it comes to communications surveillance. Private oversight within government is not a substitute for public oversight.

Annex I

Constitutional Protections Against Communications Surveillance

All countries featured in this study have constitutions that protect the right to private life, and particularly the inviolability of communications.

MEXICO's constitution, as with many other modern constitutions, expressly recognizes the right to data protection in Article 6:

> *[I]nformation relating to private life and personal data shall be protected in the terms and with the exceptions provided for by law.[...]*
>
> *All people have the right to enjoy the protection of their personal data, and to access, correct, and delete such data. All people have the right to oppose the disclosure of their data, according to the law. The law shall establish exceptions to the criteria that dictate the handling of data; such exceptions may include national security reasons, law and order, public security, public health, or the protection of a third party's rights.*[282]

Article 16 details numerous other privacy protections for communications, including:

> *[N]o person shall be disturbed in his private affairs, his/her family, papers, properties or be invaded at home without a written order from a competent authority duly explaining the legal cause of the proceeding.*
>
> *Every person has the right to enjoy protection on his personal data, and to access, correct and cancel such data. Every person has the right to oppose the disclosure of his data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of a third party's rights. [...]*
>
> *Only a judicial authority can issue a search warrant at the request of the Prosecution Service. The search warrant must describe the place to be searched, the person or persons to be apprehended and the objects to be seized. [...]*

282 Const. of Mexico, art. VI, § 2 and 3.

Private communications are inviolable. The law shall punish any action against the liberty and privacy of private communications except when they are voluntarily given by one of the individuals involved in them. A judge shall assess the implications of such communications, provided they contain information related to the perpetration of a crime. Any private communications obtained in a way that violates this law shall not be admitted in court as evidence.

Only the federal judicial authority can authorize wiretapping and the interception of private communications at the request of the appropriate federal authority or the State Public Prosecution Service. The authority that makes the request shall present, in writing, the legal causes for the request, describing therein the kind of interception required, the individuals subjected to the interception, and the term thereof. The federal judicial authority cannot authorize wiretapping nor the interception of communications in the following cases: when the matters involved are a) of electoral, fiscal, commercial, civil, labor or administrative nature, b) communications between a defendant and his attorney. [...]

The judiciaries shall have control judges [jueces de control] who shall immediately, and by any means, resolve the precautionary measures requests and investigation techniques, ensuring compliance with the rights of the accused and the victims. A detailed record of all the communications between judges and the Public Prosecution Service and other competent authorities shall be kept.

Authorized wiretapping and interception of communications shall be subjected to the requirements and limitations set forth by law. Any communications that result from telephone wiretapping or interception of communications that do not comply with the aforementioned requirements will not be admitted as evidence. [...][283]

Interpreting Article 16, the Supreme Court of Justice, in Amparo 1621/2010 of 2011, stated that the right to the inviolability of communications protects both the content of communications and the data associated with said communications:

[W]ith the purpose of guaranteeing the secrecy of all communicative processes, it is essential that any data associated with the communication be protected as well. Even though it is true that these data are not classified as the "content" of communication, it usually gives information about the circumstances under which the communication has taken place, thus affecting—directly or indirectly—the privacy of those who participate in the communication. [...] Hence, by way of example, the call logs of a telephone network user, the identity of the participants, the duration of the phone call or the identification of an IP address, carried out

283 Const. of Mexico, art. XVI.

without the necessary guarantees for the restriction of the fundamental right to secrecy of communications, may lead to their infringement."[284]

In another case (*Thesis contradiction 194/2012*), the Supreme Court answered the following legal privacy question:

[A]rticle 16 of the Mexican United States Constitution holds that private communications are inviolable. Thus, is Article 16 violated when the ministerial authority—or agents under his command review—extract or use, as evidence, electronic files stored in text, audio, image or video of a cell phone belonging to the detainee connected with the commission of a crime?

In its answer, the Supreme Court in *Thesis Contradiction 194/2012* stressed that access and analysis of data stored on a mobile phone without judicial authorization is a violation of the right to the inviolability of private communications:

According to Article 16 of the Constitution of the Mexican United States, in order to intercept a private communication, a specific authorization from the Federal Judicial authority is required, upon request of the federal authority entitled by law or the Public Prosecution Service (titular del Ministerio Público) of the corresponding federal entity so all existing forms of communication, including any that may result from technological developments, including the mobile phone [...], must be protected by the fundamental right to inviolability. [Moreover] access and analysis of data stored on a mobile phone without judicial authorization is a violation of the right to the inviolability of private communications.[285]

Additionally, in Amparo *1621/2010* (*Amparo en revisión)*, the Supreme Court pointed out that private communications are inviolable, regardless of their content. Additionally, the information that identifies the communication, such as the numbers dialed by a user, the identity of callers, the duration of the call or, for email, the Internet protocol address, shall also be protected. Furthermore, the Supreme Court stressed that the protection of private communications perseveres in time. Thus, after the communication has occurred, the means in which the content of communications is conserved or stored also becomes inviolable. The Supreme Court made clear that for a communication to be inviolable, the message must be transmitted through any medium or technical device developed by technology. This may be by telegraph, telephone, email or any other means arising from technological advances. The Supreme Court clarified that an email is deemed intercepted when the password or security key has been obtained without judicial authorization or authorization from the account owner, or when such authorization has been revoked.[286]
The Mexican Supreme Court has recently considered that the obligation to retain

284 Mexico, Supreme Court of Justice, Direct Amparo in revision 1621/2010, (15 June 2011).

285 Supreme Court of Mexico, First Chamber, Contradiction of Thesis 194/2012.

286 México, Supreme Court, Trial Chamber, Amparo in Review 1621/2010 and Thesis Contradiction 194/2012 clarifying the scope of privacy protection.

communications data of all Mexicans "do[es] not constitute an interference with the right to the inviolability of communications."[287]

> *[L]ikewise, the [Mexican Supreme Court] has not considered that the constitutional protection given to the content of communications, as well as metadata, extends to mobile phone location data in real time. One example of this is the [Mexican Supreme Court's] decision regarding the complaint of unconstitutionality 32/2012,[288] (acciones de inconstitucionalidad), in which the majority of the Supreme Court considered that it is constitutional to allow the Public Attorney's Office (PGR, in Spanish) to monitor the geolocation of a mobile phone in real time, without a federal judicial order. Thus, although at the normative level, the Constitution grants comprehensive protections for the right to the inviolability of communications, the interpretation of those provisions has not been extended to protect people from mass data retention or the collection of mobile phone location data.*[289]

Article 100 of the Political Constitution of the Republic of HONDURAS protects "the inviolability and privacy of correspondence, specifically mail, telegrams, and telephone conversations, except by judicial order."[290] Interpreting this provision, the Criminal Chamber of the Supreme Court of Honduras ruled that the constitutional protection of the right to communications privacy extends to digital and telephone communications, even if they are trivial, mundane, or insignificant. In the same ruling, the Chamber made clear that the protection of the inviolability of communications includes the protection of any communication record kept by any public or private entity. The Chamber stated that the right to the inviolability of communications, embodied in Article 100, comes from the human right to privacy. They added that the constitutional protection extends to both real-time and ex-post facto communications surveillance:[291]

> *[L]e Secret Des Lettres is inviolable [...] and the inviolability of private communications is derived from the right to private life, enshrined in Article 100 of our Constitution of the Republic, which prohibits third parties—outside the communication and primarily the State—from seizing, collecting, intercepting, opening, recording, reproducing or disclosing private communication, no matter if such actions are carried out at the time the communication is taking place (in real time), or ex-post facto, or when the communication is registered, on letters, phone devices or computers, or electronically on e-mails, mailboxes, social networks, chats,*

287 Supreme Court. Second Chamber. Amparo in Revision 964/2015.

288 Supreme Court. Plenary session. Complaint of Unconstitutionality 32/2012.

289 Luis Fernando García, "State Communications Surveillance and the Protection of Fundamental Rights in México," *Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales* (2016). https://necessaryandproportionate.org/country-reports/mexico

290 Political Const. of the Republic of Honduras, art. C.

291 Honduras, Criminal Chamber, Supreme Court of Justice, Judgment CP-48-2011, 20. http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf

etc. [...] The inviolability of communications includes the protection of records kept by public or private companies.[292]

The Constitution of EL SALVADOR also ensures the protection of communications. Article 24 has two parts. The first recognizes the inviolability of communications and the second explains exceptions to this protection:

Correspondence of every kind is inviolable; if intercepted, it shall not be given credence nor accepted as evidence in any legal action, except in cases of insolvency proceedings and bankruptcy. The interference and intervention in telephone conversations is prohibited.

Exceptionally, the court may authorize, in writing and with reason, the temporary intervention of any kind of telecommunications, but must preserve the secrecy of any private issues that are not related to the proceeding. Information coming from an illegal interference will have no value [...][293]

The Constitution of the Federative Republic of BRAZIL protects the inviolability of personal intimacy, private life, and the home. This includes protecting the privacy of correspondence, telegraphic data, and telephonic communications. The exception to this is when there is a court-ordered examination for the purposes of a criminal investigation.[294] Brazil also protects the right to habeas data, noting that access to it shall be granted in the following cases:

1. to discover personal information about the petitioner contained in public records or the public data banks of government agencies or entities; and

2. to correct data whenever the petitioner prefers to do so through confidential judicial or administrative proceedings.[295]

Although this constitutional language is favorable, it has not been robustly interpreted.

[I]nterpretation issues threaten the actual protection that such rights afford against undue surveillance of communications by State authorities. [...] [Despite that] the right to privacy (provided for in a general fashion under subsection X of the same article) allows for the protection of communications in a broader sense[296] *including*

292 Honduras, Criminal Chamber. Supreme Court of Justice, Judgment CP-48-2011, 20. http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf

293 Const. of El Salvador, art. XXIV.

294 Const. of the Federative Republic of Brazil, art. V, § 10, 11, and 12.

295 Const. of the Federative Republic of Brazil, art. V, § 72.

296 *See* Federal Supreme Court Case, *Mandado de Segurança* 24.817/DF. A case tried by Justice Celso de Mello on Feb. 3, 2005, which associates confidentiality breaches of tax, banking, and telephone records with restrictions on the rights provided for by Article X. http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605418

not only the content of communications, but also information about the circumstances in which they took place and between whom they happened (which may be revealed with account information[297] and metadata[298]).

The Constitution of ARGENTINA recognizes the inviolability of the home and communications.[299] While the Constitution refers expressly to written letters, the Supreme Court of Argentina has extended constitutional protection to communications over the Internet.[300] In *Halabi, Ernesto c/ P.E.N.*, for example, the Supreme Court ruled that Argentina infringed upon the right to privacy with the provision of the National Telecommunications Law of 2003 and its secondary regulation. These laws compelled all telecommunications companies and Internet service providers to record, index, and store traffic data for a 10-year period. Telecommunications companies were also obligated to provide this data to the Argentinean Judicial Branch and the Attorney General's Office when required. The data retention provision was annulled due to its vague wording. The Court said the law was a "drastic interference with the private sphere of the individual." It stressed that browsing data are closely connected with communication content and therefore could not be retained. The decision clarified that the rules did not provide a specific system to protect online communications against the accumulation and automatic processing of personal data.[301]

Article 26 of the Constitution of NICARAGUA also recognizes the right to privacy:

Everyone has the right to:

1. *Privacy in his/her life and that of his/her family;*
2. *The inviolability of his/her domicile, correspondence, and communication of any kind; and*

---

297 For the purposes of this report, account information refers to information included in the user's records with the telephone company, autonomous system operator, or application provider.

298 For the purposes of this report, metadata refers to all data and records generated from a given communication other than the communication's content, such as the date, time, and duration of communication, sender, addressee, geographic location of the device, if known (such as identifiers or measurements by a radio base station), device identification codes (such as IMEI), and the like.

299 Const. of Argentina, art. XVIII: "[...] The home is inviolable, as well as correspondence and private papers; and a law shall determine in which cases and for what reasons there may be a search and occupation [...]."

300 Argentina, Supreme Court, *Halabi v. Poder Ejecutivo Nacional*, (26 June 2007, 24 Feb. 2009). http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986

301 Argentina, Supreme Court, *Halabi v. Poder Ejecutivo Nacional*, (26 June 2007, 24 Feb. 2009). http://www.iprofesional.com/notas/78867-Fallo-Halabi-Ernesto-c-PEN---ley-25873---dto-156304-s-amparo-ley-16986

3. *Know about any information that the public authorities may have on record about him/her, as well as the right to know why, and for what purpose, they hold such information.*

Article 27 provides equal protection to nationals and foreigners:

> *All individuals are equal before the law and have the right to equal protection.*
>
> *[...] Foreigners have the same rights and duties as Nicaraguans, with the exception of political rights and other rights established by law.*

Other nations have incorporated similar protections into their constitutions:

- PERU's 1993 Constitution recognizes a catalog of rights. These include the secrecy and inviolability of communications, home and documents,[302] personal and family matters, and one's own voice and image. Peru's Constitution also ensures that public or private information service providers, computerized or not, cannot disclose information affecting personal and family privacy.[303]

- The Constitution of URUGUAY recognizes the inviolability of correspondence and private papers.[304]

- Article 36 of PARAGUAY's Constitution sanctions the right to the inviolability of private documentary heritage and communication.[305]

- The Constitution of GUATEMALA recognizes the protection of the inviolability of correspondence, documents, books, and the home.[306]

---

302 Const. of Peru, art. II, § 10: Secrecy and Inviolability of Private Communications and Documents. Communications, telecommunications, or any private correspondence may only be opened, seized, intercepted, or tapped by the authority of a warrant issued by a judge and with all the guarantees provided in the law. Any matter unrelated to the circumstances under examination shall be kept secret. Private documents obtained in violation of this provision have no legal effect. Books, receipts, and accounting and administrative documents are subject to inspection or audit by relevant authority in accordance with the law. Any action thus taken may not include removal or seizure, except by a court order.

303 Const. of Peru, art. II, § 6, 7, and 9.

304 Const. of Uruguay, art. XXVIII: "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."

305 Const. of Paraguay, art. IIIVI. http://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay.php

306 Const. of Guatemala, art. XXIII and XXIV: "The correspondence of any person, his [or her] documents, and books are inviolable. They may only be inspected or seized by virtue of a firm resolution dictated by a competent judge and with the legal formalities. The secrecy of correspondence and telephone, radio, and cablegram communications and of other

- Article 15 of the Constitution of Colombia recognizes the right to personal and family privacy and the inviolability of correspondence and other forms of private communication. It notably requires that interception or recording be pursuant to a court order and carried out in accordance with established law. Furthermore, Article 28 of the Colombian Constitution states that everyone is free. "[N]o one may be importuned in his/her person or family, sent to jail or arrested, nor may his/her home be searched except pursuant to a written order from a competent legal authority, subject to legal process and for reasons previously established by law."[307]

CHILE's Constitution is the only one in the region that excludes personal data protection from its list of independent rights or from being a part of the right to private life.[308]

The right to privacy is protected expressly in Latin American constitutions, either as a right to private life, right to privacy/intimacy, protection of personal and habeas data, or the secrecy and inviolability of communications, the home, and papers. However, court decisions on the topic remain scarce, and the right to privacy will continue to be developed as more decisions are issued.

products of the modern technology is guaranteed."

307 Const. of Colombia, art. XXVIII.

308 Nelson Remolina, "Constitutional Approach for the Protection of Personal Data in Latin America," *Revista Internacional de Protección de Datos Personales* (International Magazine on the Protection of Personal Data) 1 (no. 1). (2012). http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf as cited in Juan Carlos Lara and Valentina Hernández, "State Communications Surveillance and the Protection of Fundamental Rights in Chile," *Electronic Frontier Foundation & Derechos Digitales,* (2016). https://necessaryandproportionate.org/country-reports/chile

Annex II
The Normative Power of International Human Rights Treaties

In Latin America, international human rights standards are key to analyzing the legality of States' communications surveillance practices. International human rights treaties establish core human rights and set out the circumstances in which these rights may be restricted or limited when a State conducts communications surveillance. The legal basis of international human rights treaties usually is found in each country's constitution. In some instances, the countries' constitutional courts have acknowledged and further developed the legal status of international human rights treaties.[309]

Regardless of how they are integrated into the domestic legal framework, any state that has ratified international human rights treaties is obliged to comply with international obligations, according to Article 26 of the Vienna Convention on the Law of Treaties.

Likewise, the Inter-American Court on Human Rights (the I/A Court H.R.) can exercise a "control of conventionality," a mechanism in which the inter-American and national judges evaluate the compatibility of national legal instruments and practices with the American Convention on Human Rights. Article 62 of the American Convention specifies that any state that ratifies the convention can declare that it recognizes the jurisdiction of the Inter-American Court on Human Rights in interpreting and applying the convention.

The I/A Court H.R., in *Aguado-Alfaro et al. v. Peru*, explained that domestic judges are subject to a State-ratified international treaty and should exercise the control of conventionality *ex officio* between domestic laws and the American Convention:

> *128. [W]hen a State has ratified an international treaty such as the American Convention, the judges are also subject to it; this obliges them to ensure that the effet util of the Convention is not reduced or annulled by the application of laws*

309 For an in-depth analysis, read Gongora Mera and Manuel Eduardo, *La difusión del bloque de constitucionalidad en la jurisprudencia lationamericana y su potencial en la construcción del ius constituionale commune latinoamericano,* (Instituto de Investigaciones Jurídicas, Instituto Max Planck de Derecho Público Comparado y Derecho Internacional, 2014), http://www.corteidh.or.cr/tablas/r31277.pdf. *See also* Nash Rojas, Claudio, *Derecho internacional de Los derechos humanos en Chile: Recepción y aplicación en el ámbito interno,* (Law Faculty, University of Chile, September 2012), http://www.cdh.uchile.cl/media/publicaciones/pdf/91.pdf

> *contrary to its provisions, object and purpose. In other words, the organs of the Judiciary should exercise not only a control of constitutionality, but also of "conventionality"*[310] *ex officio between domestic norms and the American Convention; evidently in the context of their respective spheres of competence and the corresponding procedural regulations.*[311]

The I/A Court H.R in *Almonacid-Arellano et al v. Chile*, also affirmed that domestic judges and courts are bound by the American Convention:

> *124. [T]he Court is aware that domestic judges and courts are bound to respect the rule of law, and therefore, they are bound to apply the provisions in force within the legal system. But when a State has ratified an international treaty such as the American Convention, its judges, as part of the State, are also bound by such Convention. This forces them to see that all the effects of the provisions embodied in the Convention are not adversely affected by the enforcement of laws which are contrary to its purpose and that have not had any legal effects since their inception. In other words, the Judiciary must exercise a sort of "conventionality control" between the domestic legal provisions which are applied to specific cases and the American Convention on Human Rights. To perform this task, the Judiciary has to take into account not only the treaty, but also the interpretation thereof made by the Inter-American Court, which is the ultimate interpreter of the American Convention.*[312]

All branches of the States that have ratified the American Convention are bound by it, not just domestic judges. In *Yatama v. Nicaragua,* the I/A Court H. R. ordered the State of Nicaragua to ensure its domestic legislation complied with the provisions of the American Convention of Human Rights.

> *170. [T]he general obligation that the State should adapt its domestic laws to the provisions of the Convention to guarantee the rights it embodies, which is established in Article 2, includes the issuance of rules and the development of practices leading to effective enforcement of the rights and freedoms embodied in the Convention, and also the adoption of measures to derogate norms and practices of any kind that entail a violation of the guarantees established in the Convention. This general obligation of the State Party implies that the measures of domestic law*

---

310 Inter-American Court of Human Rights, Case of Almonacid Arellano et al., paragraph 124, http://www.corteidh.or.cr/docs/casos/articulos/seriec_154_ing.pdf.

311 Inter-American Court of Human Rights, , Case of the Dismissed Congressional Employees, Aguado-Alfaro et al. v. Peru, (Judgment of November 24, 2006), http://www.corteidh.or.cr/docs/casos/articulos/seriec_158_ing.pdf.

312 Inter-American Court of Human Rights, Case of Almonacid-Arellano et al v. Chile, (Judgment of September 26, 2006), http://www.corteidh.or.cr/docs/casos/articulos/seriec_154_ing.pdf.

must be effective (the principle of effet utile), and to this end the State must adapt its actions to the protection norms of the Convention.[313]

In Argentina,[314] Colombia,[315] Chile,[316] Mexico,[317] and Paraguay,[318] human rights treaties ratified by the State pose the same binding characteristics as the country's constitution and are legally enforceable in domestic courts. For example, the Mexican Supreme Court recognized that both constitutional and international sources of human rights law must be respected by authorities and the Mexican legal system. Neither source of human rights law is more important than the other. Rather, they form a "parameter of constitutional consistency."[319] When they conflict, it is understood that in accordance with the *pro personae* principle, legal norm most favorable to the individual is preferred.[320]

In Colombia, the Constitutional Court stated that international human rights treaties and international humanitarian law together with the constitution form the "constitutional block" providing the source of law for human rights.[321] The Constitutional Court of

313 Inter-American Court of Human Rights, Yatama v. Nicaragua Judgment, (Preliminary Objections, Merits, Reparations and Costs, June 23, 2005), par. 170, http://www.corteidh.or.cr/docs/casos/articulos/seriec_127_ing.pdf.

314 Argentinian, Supreme Court of Justice, Ekmekdjian, Miguel Ángel v. Sofovich, Gerardo et al., July 7, 1992. For an in-depth analysis, read Verónica Ferrari and Daniela Schnidrig, *State Communications Surveillance and the Protection of Fundamental Rights in Argentina,* (Electronic Frontier Foundation & Center for Studies on Freedom of Expression and Access to Information, March 2016)

315 Colombia Const. art. 93. *See also* Jaime Rodríguez v. Iván Mejía Alvarez, sentence T-1319 (Constitutional Court, December 7, 2001), http://www.corteconstitucional.gov.co/relatoria/2001/t-1319-01.htm

316 Chile Const. art. V and VI.

317 Mexican Const. art. I. The Mexican Constitution establishes a *pro personae* principle, that provisions should be interpreted in the most favorable way for human rights. The Supreme Court also recognizes constitutional and international sources of human rights law as components of the same catalog to be respected by the authority and the Mexican legal system (Supreme Court. Plenary session. Thesis Contradiction 293/2011).

318 Paraguayan Const. art.CXXXVII and CXLV.

319 García Luis Fernando, *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México*, Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales (2016).

320 García Luis Fernando, *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México*, Electronic Frontier Foundation & Red en Defensa de los Derechos Digitales (2016)

321 "The constitutionality block has three legal effects: 1) treaties of human rights take precedence over domestic legislation; 2) Human rights treaties can be considered at the same level of the national constitution, so a conflict between a human rights treaty and a domestic law can result in a declaration of unconstitutionality; and 3) the rights protected by international human rights treaties can be invoked through national actions that protect constitutional rights." Gongora Mera and Manuel Eduardo. *La difusión del bloque de constitucionalidad en la jurisprudencia lationamericana y su potencial en la construcción del ius constituionale commune latinoamericano,* (Instituto de Investigaciones Jurídicas,

Colombia also allows declarations made by international bodies like the Inter-American Commission on Human Rights, the Inter-American Court of Human Rights, and the United Nations Human Rights Council to influence the interpretation of domestic legislation.[322] The Court also gives normative power to international documents other than treaties, such as international principles. Occasionally, the Court uses expert-drafted documents, as these are considered important for interpreting international human rights laws.[323]

In Peru, human rights treaties must be approved by Congress before they are ratified by the President of the Republic.[324] The rules relating to the rights and freedoms recognized by the Peruvian Constitution are interpreted in accordance with the Universal Declaration of Human Rights and other international treaties ratified by Peru. The Peruvian Constitution also notes that in case of doubt or conflict between criminal laws, the judge must apply the law that is most favorable to the defendant.[325]

Guatemala's constitutional court also adheres to the "constitutional block" doctrine.[326] The Constitutions of Guatemala and Peru make clear that human rights enshrined in international treaties have constitutional statuses even if they are not specified in the constitution.

The human rights treaties, covenants, and instruments ratified by Nicaragua and approved by a legislative act are considered domestic law and are applicable inside and outside Nicaragua after entering into force internationally.[327]

Several countries have supremacy clauses whereby a treaty will prevail in a conflict with a domestic statute. These countries, for example, include Colombia, Guatemala, and

---

Instituto Max Planck de Derecho Público Comparado y Derecho Internacional, 2014), http://www.corteidh.or.cr/tablas/r31277.pdf

322 To read a more comprehensive analysis of the constitutional block doctrine, read Molina Carlos Ernesto, *Complaint of partial unconstitutionality against article 19 of the Substantive Labor Code*, sentence C-401, (Constitutional Court, April 14, 2005), http://www.corteconstitucional.gov.co/RELATORIA/2005/C-401-05.htm and Rodrigo Uprimny Yepes, *Constitutional, Human Rights and New Criminal Procedure Block*, (Judicial School Lara Bonilla, Superior Council of Judicature, Bogotá, 2006).

323 *See* Camilo Rivera, Juan and Katitza Rodríguez, *Colombia: Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales,* Electronic Frontier Foundation (2016).

324 Peruvian Const. art. LVI.

325 Peruvian Const. art. CXXXIX, item 9.

326 Fundación Acceso, Privacy for digital rights defenders: A study on how the legal frameworks of El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance of human rights defenders. Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015), 133.

327 Nicaraguan Const. art. CXXXVIII, item 2.

Honduras.[328] El Salvador treats conflicts between treaties and domestic laws similarly, but gives priority to constitutional provisions when they conflict with treaties.[329]

328 Guatemalan Const. art.XLVI. Honduras Const. art. XVIII.

329 El Salvadorian Const. art. CXLIV-CXLIX. Fundación Acceso, Privacy for digital rights defenders: a study on how the legal frameworks of El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance of human rights defenders. Peri, Luciana (coord.), (San José, C.R.: Fundación Acceso, 2015), LXXIV -LXXV.