MEMORANDUM TO INTERESTED PERSONS

RE: Right to Privacy and the Legality of Colombian Surveillance Activities

DATE: August 4, 2015

TABLE OF CONTENTS

I. INTRODUCTION ....................................................................................................................................................... 2

II. BACKGROUND: .......................................................................................................................................................... 3

A. PAST INTELLIGENCE AGENCY ABUSES .................................................................................................................. 3
B. IMPUNITY FOR PAST CRIMES .................................................................................................................................. 5
C. REPORTS OF ONGOING SURVEILLANCE OF LAWFUL HUMAN RIGHTS ACTIVITIES IN COLOMBIA .... 6

III. RELEVANT INTERNATIONAL RIGHT TO PRIVACY STANDARDS ................................................................. 3

A. CURRENT INTER-AMERICAN STANDARDS ................................................................................................................ 7
B. INTERNATIONAL HUMAN RIGHTS LAW FRAMEWORK ........................................................................................... 10
C. STANDARDS CONCERNING THE PROTECTION OF ATTORNEY – CLIENT PRIVILEGED
   COMMUNICATIONS .................................................................................................................................................. 14
D. COMPARATIVE CASE STUDY: THE EROSION OF CONSTITUTIONAL PROTECTIONS IN THE UNITED
   STATES ........................................................................................................................................................................... 15

IV. ANALYSIS ........................................................................................................................................................................ 19

A. PAST SURVEILLANCE ACTIVITIES OF COLOMBIA’S DEPARTMENT OF ADMINISTRATIVE SECURITY
   (DAS) VIOLATES THE AMERICAN CONVENTION ON HUMAN RIGHTS ........................................................................ 19
B. TO ENSURE AN EFFECTIVE REMEDY, THE STATE OF COLOMBIA MUST FULLY INVESTIGATE AND
   PROSECUTE PAST ABUSES, PROVIDE ACCESS TO RECORDS AND EXPUNGE UNLAWFULLY ACQUIRED
   INFORMATION ................................................................................................................................................................. 22
C. COLOMBIAN LAW DOES NOT APPEAR TO SATISFY COLOMBIAN CONSTITUTIONAL REQUIREMENTS
   ......................................................................................................................................................................................... 24
D. TO PREVENT ONGOING VIOLATIONS AND THE REPETITION OF ABUSES, COLOMBIA MUST REVISE
   ITS LAWS TO GENERALLY REQUIRE PRIOR JUDICIAL AUTHORIZATION OF SURVEILLANCE
   ACTIVITIES BASED ON A SHOWING THAT SUCH SURVEILLANCE IS STRICTLY NECESSARY TO
   ACHIEVE A LEGITIMATE PURPOSE ............................................................................................................................. 28

1 This memorandum has not been reviewed by the ABA House of Delegates and should therefore not be construed as representing ABA policy.
I. Introduction

In response to reports of widespread surveillance of human rights defenders and members of Congress by Colombian intelligence agencies for the express purpose of disrupting and discrediting their activities, the American Bar Association Center for Human Rights was asked to provide a summary of international right to privacy standards concerning the lawfulness of such surveillance activities. The following memorandum outlines relevant standards in the international and Inter-American systems and provides recommendations on how to ensure that surveillance activities are subjected to meaningful restrictions that protect the right to privacy, the integrity of confidential attorney-client communications and the right to a remedy for past abuses.

Credible reports of pervasive surveillance of the legitimate activities of Colombian legislators and human rights defenders, including in particular lawyers, has jeopardized their ability to investigate human rights violations and hold their government accountable without fear that private information obtained by the government will be used against them. The failure to fully investigate past violations, expunge unlawfully acquired communications, limit ongoing surveillance activities to those strictly necessary to serve a legitimate government interest or reform Colombia’s laws to comply with international and constitutional standards have left the victims without a meaningful remedy. The State of Colombia should be compelled to provide such remedies and to reform its domestic legislation to ensure compliance with relevant international standards, including in particular protections for the confidentiality of attorney-client communications. Absent such a remedy, technological developments that enable governments to collect vast amounts of personal information about millions of individuals threaten the ability of Colombian citizens to effectively participate in democratic governance without fear of reprisal.
To ensure compliance with international law, the Inter-American Court on Human Rights should adopt strict standards for surveillance laws, including prior judicial approval before surveillance begins and ad hoc judicial review. Such judicial review must be subject to clear legal standards requiring an evidentiary showing that the surveillance of that particular person, place or thing is strictly necessary to investigate serious criminal activity.

II. BACKGROUND:

A. PAST INTELLIGENCE AGENCY ABUSES

In February 2009, the Colombian newspaper, *Semana*, reported that the Colombian intelligence agency, the Department of Administrative Security (DAS), had illegally tapped journalists, judges and human rights defenders. Official documents produced by DAS and later disclosed by the Colombian Attorney General stated that the objectives of the surveillance included “generating controversy regarding [non-governmental organizations],” “neutralizing influence in the Inter-American Commission on Human Rights” and “generating divisions within opposition movements.” A stated objective of DAS was to carry out a “judicial war” (*Guerra Jurídica*) aimed at “neutralizing the influence of the Inter-American Court for Human Rights in Costa Rica.” The United Nations High Commissioner for Human Rights reported that DAS was behind threats against human rights defenders, including direct insinuations of violence sent to defenders’ private residences.

The Special Strategic Intelligence Group (G3) carried out much of the surveillance. Documents indicate that a few rogue agents did not carry out these activities; rather top DAS leadership attended G3 meetings and received G3 memos.

The purported purpose of the surveillance was to establish a link between illegal armed groups and NGOs. However, official documents released by Colombia’s Attorney General did not

---


4. *Id.*


demonstrate any unlawful activity by the targeted NGOs. Rather, the G3’s focus appears to have been, according to human rights groups, “the daily, legitimate activities of human rights groups, journalists and others, with a particularly obsessive focus on actions taken to present human rights concerns to the international community.” This surveillance included documenting attendance at human right related events, detailed tracking of international travel of human rights lawyers and advocates presenting cases at the Inter-American Commission, European Parliament and United Nations. International NGOs characterized the G3’s activities as “routine, massive spying on human rights groups including sensitive discussion of preparation of court cases that involved government agent defendants, information from victims of human rights violations, and confidential information between lawyers, their clients and judicial authorities.”

Surveillance targeted not only the professional activities of human rights defenders, but also their private lives, including spying on their homes and family members. According to press reports, DAS provided bodyguards to protect human rights defenders under the U.S. funded protection program, at least some of whom reported to DAS on the activities of the very individuals under their protection.

The targets of DAS surveillance included opposition political candidates and United Nations staff, including UN special rapporteur missions. DAS documents included e-mails from U.S. and European human rights groups, such as Human Rights Watch, Peace Brigades International, International Federation on Human Rights, among others. DAS also tapped the phone of U.S. contractor Management Sciences in Development, which carried out USAID’s human rights program in Colombia.

In February 2009, the Inter-American Commission issued a press release expressing concern that DAS had intercepted communications of “well- known individuals, including members of the executive, legislative, and judicial branches, members of political parties, human rights defenders, and journalists.” The Commission also acknowledged in July 2009, that the G3 reportedly conducted intelligence operations linked to cases at the international level and on the international contacts of domestic human rights defense groups.

In September of 2011, the press reported that members of DAS sold intelligence information to illegal groups and other interested parties before their access to such information ended in

---

7 Id. at 2.
8 Id.
9 See Id. at 3.
10 Id.
11 See Id. at 4.
13 Id. at 5.
14 Id.
Although President Santos dissolved DAS in 2011 due to the scandal, the Commission expressed concerns about the inadequacies of judicial actions against former DAS members and the failure to establish mechanisms for individuals to access and review information obtained about them unlawfully by the government. The Commission stated that such mechanisms should include means “by which individuals can gain access to intelligence information kept on them and thereby can request that it be corrected, updated, or, if applicable, removed from the intelligence files.”

B. IMPUNITY FOR PAST CRIMES

Following these revelations, with the support of former President Uribe, President Santos dissolved DAS and promised investigations into those responsible. In September 2011, the Supreme Court of Justice convicted former DAS Director Jorge Noguera Cotes of homicide and sentenced him to 25 years in prison.

In 2012, the U.N. High Commissioner for Human Rights confirmed that other former DAS Directors and 40 other members of DAS were under judicial investigations for abuses and illegal activities. She also expressed concern about a new intelligence law adopted in June of 2012 that established two commissions, one to assist in purging intelligence files and a congressional commission to monitor intelligence activities. According to the High Commissioner, the congressional commission has a weak mandate and the law lacks effective internal control mechanisms. In response, the High Commissioner called for the adoption of measures to comprehensively reform the intelligence services and transform the institutional culture that...

---


20 Id.


24 Id. at ¶ 25.
leads to the commission of human rights violations.\textsuperscript{25}

Despite these recommendations, the Inter-American Commission recently expressed concern for the high level of impunity in the State’s response to the DAS scandal. In its August 2014 report on Colombia, the Commission reported that since the revelations, authorities have only presented two cases.\textsuperscript{26} The Commission also highlights that the Attorney General has dropped many cases and deals struck with DAS members to serve as witnesses in other cases.\textsuperscript{27}

According to the Commission, the National Police hired former DAS members as civil personnel, and 3,218 ex-DAS members transferred to work in the offices of the Protection of Victims, Witnesses, and Technical Investigations body (CTI), a sub-office of the judicial police.\textsuperscript{28} During this transfer, there was reportedly no process for preventing the hire of past DAS employees implicated in the illegal activities of the agency.\textsuperscript{29}

C. REPORTS OF ONGOING SURVEILLANCE OF LAWFUL HUMAN RIGHTS ACTIVITIES IN COLOMBIA

Despite the closing of DAS, the Colombian government reportedly continues to conduct invasive surveillance of human rights organizations and journalists. In February 2014, the press reported that military intelligence officials and the Central Intelligence Agency were intercepting conversations between delegates during peace negotiations in Havana, Cuba.\textsuperscript{30} Under the program code named “Andrómeda”, officials set up a fake restaurant and internet café where officials would eavesdrop on official conversations and hack into BlackBerrys and e-mail accounts.\textsuperscript{31} President Santos reacted by ordering an investigation and described allegations of phone hacking as “unacceptable”.\textsuperscript{32} Heads of both intelligence institutions immediately resigned their posts.\textsuperscript{33}

However, ten days following the revelations of this surveillance program, General Ernesto Maldonado, investigator for the Colombian Armed Forces, presented a report that claimed the surveillance actions of the military officials were legal.\textsuperscript{34} His assessment relied on 10 interviews,
22 polygraph tests, and reviews of official orders from 2012, 2013, and 2014.\textsuperscript{35} Despite concluding that the surveillance was legal, General Maldonado nonetheless recommended reforms. First, General Moldonado suggested that, to bring increased transparency to the ongoing investigation, six officials who were directly involved should be relieved of their posts; second, certification documents from the intelligence and counter-intelligence agencies should be reviewed on a monthly basis to guarantee that each activity undertaken by the agency met relevant legal requirements; third, it may be necessary to “solicit support from international authorities or friendly governments in order to raise the standards of control in the intelligence operations, in particular regarding cyber-terrorism.” \textsuperscript{36}

However, press accounts in October 10, 2014 of further surveillance of several high level officials from the peace negotiation commission, several members of the International Committee of the Red Cross, foreign embassy officials, journalists and human rights researchers call into question whether these recommendations have led to meaningful reforms.\textsuperscript{37} According to the reports, high level officials within the Armed Forces were informed of an extensive list of e-mail addresses being utilized by the military intelligence agency to collect information about so-called “metadata” which includes information on who, how, when and where communications were created, viewed or modified.\textsuperscript{38}

While the full scope of ongoing surveillance remains unclear, the latest allegations raise concerns that the mere dissolution of DAS has not been adequate to ensure that Colombian authorities only engage in surveillance when strictly necessary to achieve a legitimate government interest, such as the investigation of criminal misconduct. Such revelations leave human rights defenders, lawyers and journalists with no choice but to curtail their activities to prevent the disclosure of sensitive, confidential information.

\section*{III. RELEVANT INTERNATIONAL RIGHT TO PRIVACY STANDARDS}

\subsection*{A. CURRENT INTER-AMERICAN STANDARDS}

Article 11 of the American Convention of Human Rights protects the right to privacy.\textsuperscript{39} Article 11(2) states, “no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.”\textsuperscript{40} The Court has interpreted this provision to prohibit arbitrary actions and to require any action infringing on privacy to meet three requirements: 1.) it must be established by law; 2.) it must

\begin{itemize}
\item \textsuperscript{35} \textit{Id.}
\item \textsuperscript{36} \textit{Id.}
\item \textsuperscript{37} Los de la lista, Semana, Oct. 28, 2014. \url{http://www.semana.com/nacion/articulo/inteligencia-militar-lista-de-periodistas-funcionarios-del-gobierno/407292-3}.
\item \textsuperscript{38} La polémica lista de Inteligencia Militar, Semana, Oct. 28, 2014. \url{http://www.semana.com/nacion/articulo/la-lista-de-periodistas-funcionarios-que-tenia-la-central-de-inteligencia-militar/407290-3}.
\item \textsuperscript{39} American Convention on Human Rights, Nov. 21, 1969, 1144 U.N.T.S. 143, Art. 11(2).
\item \textsuperscript{40} \textit{Id.} 
\end{itemize}
have a legitimate purpose; and 3.) it must be appropriate, necessary, and proportionate.\(^{41}\)

In defining “established by law” the Court has held that the law must be established by the legislature in accordance with the Constitution.\(^{42}\) With regards to the interception of telephone conversations, the Court has stated that the law must be “precise and indicate the corresponding clear and detailed rules…, [including] the circumstances in which this measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed.”\(^{43}\)

In considering the final requirement of appropriateness, necessity, and proportionality, the Inter-American Court has not provided an analysis of this prong in the two cases it has considered regarding intercepted private communications. In *Escher et al. v. Brazil*, the Court found that because the interception was contrary to domestic law there was no need to consider whether the State provided a legitimate purpose or whether the surveillance was suitable, necessary, and proportionate to the end sought.\(^{44}\) Similarly, in the case of *Tristán Donoso v. Panamá*, the Court did not elaborate on whether the State had met the obligation to prove that the interception of communications was appropriate, necessary and proportional.\(^{45}\)

While the Inter-American Court has not had occasion to elaborate on these requirements in the context of the right to privacy, it has done so extensively in interpreting the same requirements for restrictions on freedom of expression. For a provision to be necessary, the Inter-American Court recognizes that restrictions must “be justified by reference to governmental objectives which, because of their importance, clearly outweigh the social need for the full enjoyment of the right” to free expression.\(^{46}\) It has also held that such restrictions “should in no way limit, more than strictly necessary, the full scope of freedom of expression and become a direct or indirect means of prior censorship.”\(^{47}\) Consistent with the European Court, the Inter-American Court has found that “[i]f there are various options to achieve this objective, the one which least restricts the protected right should be selected.”\(^{48}\) The Court explained that “it is not enough . . . to demonstrate that a law performs a useful or desirable purpose; to be compatible with the Convention, the restrictions . . . [cannot] limit the right established in this Article more than is strictly necessary.”\(^{49}\)

The Inter-American Commission has taken the position that States must:


refrain from engaging in any type of arbitrary or abusive meddling in the home or offices of the organizations of human rights defenders, or in their correspondences and telephone and electronic communications. Instruct the authorities affiliated with the state security agencies to respect these rights and impose disciplinary and criminal sanctions on those who engage in such practices.50

It has further recommended that States prohibit the introduction of information obtained unlawfully into court proceedings in order to discourage illegal surveillance.51

In its 2011 report on the situation of human rights defenders, the Inter-American Commission emphasized that any state interference into the lives of human rights defenders, including family, home, correspondence, or private communications, must meet these requirements to comply with the Convention. The Commission goes further to observe that a “great number of interferences in the private life of human rights defenders in the region have been carried out without meeting the aforementioned requirements and have even been conducted without judicial authorization that includes the grounds and reasons provided by the relevant authorities.”52 The Commission has stated that “interference with private communications” is legitimate only “where there are factual indications for suspecting a person of planning, committing or having committed certain criminal acts [or] strong suspicion that offenses are about to be committed.”53

The Inter-American Commission concluded that human rights defenders in the region continue to suffer from arbitrary and abusive intelligence activities through interception of private communications. The Commission notes, “these activities continue to be among the many forms of harassment used to hamper defenders in their work”.54 The Commission also confirms that it has observed the practice of illegally intercepting human rights defenders’ correspondence and telephone and electronic communications.55 The Commission expressed profound concern that in some instances military or police intelligence facilitated the executions of human rights defenders.56

Although the Inter-American Commission and Court have articulated basic restrictions on government surveillance activities, the Court has not yet directly addressed the question of whether international law requires prior judicial authorization in the absence of such a requirement in local law.57 Nor has it articulated what evidentiary standards are required to demonstrate the necessity of a warrant or how court orders must be tailored to ensure proportionality. The Inter-American Court could address many of these gaps in the jurisprudence

54 Id. ¶ 67.
55 Id. ¶ 70.
56 Id.
57 The principle of legality enshrined in Article 7 of the American Convention requires States to abide by their own laws.
by reference to international standards.

B. INTERNATIONAL HUMAN RIGHTS LAW FRAMEWORK

Major international conventions have long protected the right to privacy. The Universal Declaration of Human Rights establishes that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The International Covenant on Civil and Political Rights (ICCPR) states “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”

Additionally, the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms states, “(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.”

The U.N. Human Rights Committee – the body charged with authoritative interpretation of the ICCPR – explained in general comment No. 16 that Article 17 of the ICCPR protects the “integrity and confidentiality” of correspondence. The Committee stated that no interference can occur “except in cases envisaged by the law” and that laws authorizing surveillance must comply with the “provisions, aims, and objectives of the [ICCPR].” The Committee has interpreted the term “arbitrary”, as applied in international law to situations of surveillance, to require an analysis of whether an intrusion is reasonable in a given circumstance. The Committee has further clarified that the concept of reasonableness means “any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.”

To avoid violation of the ICCPR, States must demonstrate the “necessity [of the interference] and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of [ICCPR] rights.”

---

63 Id.
65 Human Rights Committee, 18th Sess., CCPR/C/21/Rev.1/Add. 13, ¶ 6 (May 26, 2004).
The United Nations General Assembly, on December 18th, 2013, in a 57 Member co-sponsored resolution, called upon “all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasizing the need for States to ensure the full and effective implementation of their obligations under international human rights law.”66 In recognition that international law must keep pace with modern technology that make unprecedented levels of pervasive surveillance possible, the United Nations General Assembly requested that the United Nations High Commissioner for Human Rights submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communication and the collection of personal data, including on a mass scale, to the Human Rights Council and the General Assembly.67 On June 30, 2014, the United Nations High Commissioner for Human Rights issued an expansive report outlining the applicable international law standards for current advances in surveillance. The High Commissioner concluded that while international law provides for a “clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance […] many State practices have […] revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.”68

In broad terms, the High Commissioner emphasized that surveillance “must not arbitrarily or unlawfully interfere with an individual’s privacy, family, home or correspondence; governments must take specific measures to ensure protection of the law against such interference […] consistent with the overarching principles of “legality, necessity, and proportionality”.70 The principle of “legality” requires that government surveillance may only occur pursuant to previously and properly enacted laws “and the law must be sufficiently accessible, clear and precise so that any individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.”71

The principle of “necessity” means that any limitation must be “necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.”72 Meaning that limitation placed on the right to privacy must have “some chance of achieving [the stated] goal” and the onus is on the State to show that the limitation connects to a “legitimate aim.”73 National security and prevention of terrorism, the most common and expansive aims claimed by States, could be a “legitimate aim” so long as the degree of interference is “assessed

67 Id. at 1.
68 Id. (citations omitted).
69 Id. at ¶ 15.
70 Id. at ¶ 23.
71 Id.
72 Id.
73 Id.
against the necessity of the measure to achieve [the] aim and the actual benefit it yields towards such a purpose.”

All limiting measures must be “proportionate”, meaning “the least intrusive instrument amongst those which might achieve the desired result.” Again, the onus is on the State to show that the interference is both necessary and proportionate to the specific legitimate aim.

Mass or “bulk” surveillance that serve legitimate aims and codified in an accessible legal regime may nonetheless be found “arbitrary” and thus in violations of international law. As clearly stated by the High Commissioner, “it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.”

According to the High Commissioner, in order to ensure full realization of the right protected under international law, the State is required to ensure that interference with the right to privacy is authorized by laws meeting the following criteria: 1.) the law must be “publicly accessible”; 2.) the law must “contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims”; 3.) the law must be “sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected”; and 4.) the law must “provide for effective safeguards against abuse.” Such safeguards must include “adequately resourced institutional arrangements.” The High Commissioner concluded that while safeguards can take a variety of forms, involvement from “all branches of government in the oversight of surveillance programmes, as well as an independent civilian oversight agency, is essential to ensure the effective protection of the law.” The mere requirement of judicial review alone may be insufficient, according to the High Commissioner, as such review in many countries of the digital surveillance activities of intelligence and/or law enforcement agencies has “amounted effectively to an exercise in rubber-stamping.”

The European Court on Human Rights has implemented many of these principles in its jurisprudence. Article 8 § 2 of the European Convention guarantees the right to privacy and only permits intrusions on the right “in accordance with the law.” In the case Uzun v. Germany the

---

74 Id. at ¶ 24.
75 Id. at ¶ 25.
76 Id. at ¶ 26.
77 Id. at ¶ 27.
78 Id. at ¶ 28.
79 Id. at ¶ 29.
80 Id. at ¶ 30.
81 Id. at ¶ 31.
82 Id. at ¶ 32.
83 Id. at ¶ 33.
Court addressed the issue of surveillance in the context of an investigation carried out Germany’s Federal Office of Criminal Investigations. The Federal Office undertook surveillance including visual surveillance, tapping of telephones, radio interception, and video surveillance, as well as the use of a Global Positioning System receiver installed in the accused’s accomplice’s car. The accused was under investigation for his alleged participating in a bomb attack. The Court ultimately found that the German law sufficiently protected against illegitimate surveillance and that the measures challenged by the accused met the requirements of the European Convention. Specifically, the surveillance was conducted “in accordance with the law” as required by the Convention, as the relevant domestic law was sufficiently clear “to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law.”

The European Court requires legal “foreseeability” in the context of covert measures of surveillance stating, “[t]he law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures.” The Court went on to explain, “in view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated.” Finally, it qualified this point by recognizing that however clearly drafted a legal provision may be, there will always be an element of judicial interpretation and the need for clarification or adaptation to changing circumstances, therefore this requirement is not to be read to disallow such judicial interpretation.

The European Court has also stated that “the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power and compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights [right to privacy].” The assessment of adequate and effective guarantees against abuse “depends on all the circumstances of the case.

---

85 Id. at ¶ 10-12.
86 Id. at ¶ 9.
87 Id. at ¶ 60-62.
88 Id. at ¶ 60.
such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law." However, oversight should be normally judicial, as “judicial control affords the best guarantees of independence, impartiality and a proper procedure.”

National authorities, as grounds for requiring the limitation of rights, commonly invoke national security at a legitimate aim. While national security may be a legitimate aim in certain cases, in the context of freedom of association the European Court has stated that restrictions in the name of national security are only permitted where there is an actual, not hypothetical threat. Similarly, usage of national security as a legitimate aim to limit the right to privacy should be analyzed through an informed consideration of the particular national security threat being claimed by the State seeking limitation on the right.

C. STANDARDS CONCERNING THE PROTECTION OF ATTORNEY – CLIENT PRIVILEGED COMMUNICATIONS

Particular concern is warranted when considering the implication of current surveillance practices for the legal profession and the vital attorney-client privilege that facilitates the realizations of numerous rights, including the rights of the accused, right to fair trial, and right to liberty and security of persons. Secret surveillance regimes of world powers provide little assurance that privileged communication between lawyer and clients are not included in vast eavesdropping programs. The issue of attorney-client privilege is exceedingly important in the situation of surveillance in Colombia. Victim legal representation organizations appear to have been targeted by the prior Colombian surveillance regime and such organizations continue to allege the existence of intrusive State surveillance that hampers their ability to competently represent their clients, as detailed above.

93 Id.
97 See Rubinstein, Ira S., Gregory T. Nojeim, and Ronald D. Lee. "Systematic government access to personal data: a comparative analysis." International Data Privacy Law 4.2 (2014): 96-119. (analysis of the surveillance law of Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States); See also Liberty and Others v. The United Kingdom (complaint that private information, including privileged information was monitored and stored by the State. The Court found that the State did not provide publically accessible indications of their procedures and therefore the surveillance was not “in accordance with the law.”)
The right to counsel enshrined in international law is illusory without assurances that communications between an attorney and client will remain confidential. The ICCPR guarantees the right of criminal defendants “to have adequate time and facilities for the preparation of his defense and to communicate with counsel of his own choosing.” The Human Rights Committee, in General Comment No. 13, found that “to communicate” requires that counsel maintain full respect for the confidentiality of their communications and that “[l]awyers should be able to counsel and to represent their clients in accordance with their established professional standards and judgment without any restrictions, influences, pressures or undue interference from any quarter.”

The United Nations Basic Principles on the Role of Lawyers also embodies the importance of the attorney-client privilege in Principle 22, stating, “[g]overnments shall recognize and respect that all communications and consultations between lawyers and their clients within their professional relationship are confidential.” A number of United Nations standards and guiding principles on the rights of detained individuals also point to the importance of respecting attorney-client privilege.

The European Court of Human Rights states that, “it is clearly in the general interest that any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion. It is for this reason that the lawyer-client relationship is, in principle, privileged.” The Court went on to say “that if a lawyer were unable to confer with his client without such surveillance [eavesdropping] and receive confidential instructions from him his assistance would lose much of its usefulness, whereas the Convention is intended to guarantee rights that are practical and effective.”

As specifically applied to situation of tapping phone conversations, the European Court in Kopp v. Switzerland found that the law and practice of phone tapping did not ensure that the exchange of information falling under the lawyer-client privilege was protected.

D. COMPARATIVE CASE STUDY: THE EROSION OF CONSTITUTIONAL PROTECTIONS IN THE UNITED STATES

---

101 See Body of Principles for the Protection of All Persons Under Any Form of Detention or Imprisonment, G.A. Res. 43/173, Principle 18 (Dec. 9, 1988); Rule 93 for the U.N. Standard Minimum Rules for the Treatment of Prisoners, Economic and Social Council resolution 663 (XXIV), (July 31, 1957); and Human Rights Committee General Comment No. 20 on protection of detainees.
103 Id. (citing Campbell and Fell v. the United Kingdom, Eur. Ct. H.R. (ser. A) No. 80, at 49, ¶ 111-113 (June 28, 1984)).
The United States’ practice of intercepting the communications of millions of Americans without a court order based on probable cause that such individuals are engaged in criminal activity demonstrates the inherent danger to democratic governance posed by newly developing surveillance technologies. Absent strong jurisprudence in the Inter-American system and around the world ensuring that surveillance is only undertaken when strictly necessary to serve a legitimate government interest, there is a pronounced danger that other governments will adopt these practices.

In response to the British practice during the colonial era of engaging in sweeping searches to uncover allegedly seditious conduct, the drafters of the United States Constitution included strong privacy protections that in many ways anticipated the requirements subsequently enshrined in international law. The Fourth Amendment states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

The United States Supreme Court has long recognized, not only the importance of the right to privacy, but also the relationship between the right to privacy and other fundamental rights, including the right to freedom of association. For example, it prohibited the compelled disclosure of the membership lists of a leading civil rights organization on the grounds that “[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.”

In 1967, the Supreme Court held in *Katz v. United States* that the Fourth Amendment required the government to obtain a warrant prior to intercepting telephone calls. In subsequent cases, it has noted that the consolidation of information about individuals, even public records, can threatens privacy interests and that the accumulation of extensive personal details in a single electronic device requires heightened judicial scrutiny prior to a government search.

In 1974, in response to revelations that U.S. law enforcement and intelligence agencies had engaged in widespread surveillance of members of Congress, political parties and civil rights leaders – including surveillance of the Rev. Martin Luther King that subsequently contributed to efforts to blackmail him – the Congress enacted the Privacy Act which prohibits, *inter alia*, the maintenance by the government of records “describing how any individual exercises rights guaranteed by the First Amendment [including freedom of association, assembly and expression] unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity[.]”

---

106 U.S. Const. amend. VI.
107 See *Nat’l Ass’n for Advancement of Colored People v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 462 (1958) (establishing that Alabama’s proffered legitimate justification for demanding the membership list of the NAACP was insufficient to establish a proper justification, and the Court may consider the State’s ulterior motivations.)
110 See Privacy Act 5 U.S.C. § 552a(e)(7).

16
Congress also amended U.S. surveillance law by adopting the Foreign Intelligence Surveillance Act (FISA). The Act required a court order based on probable cause that the target was an agent of a foreign power before the government could intercept electronic communications for intelligence purposes. Investigations of criminal suspects continued to require a warrant based on probable cause of criminal activity, pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

While not without controversy, this bifurcated system for foreign intelligence and criminal surveillance appeared to satisfy the core requirements of the Fourth Amendment until amendments to FISA occurred in the wake of the terrorist attacks of 9/11. In August 2007, Congress passed the Protect America Act of 2007 (PAA), granting the government the power to collect “foreign” communications that “pass through communication nodes on U.S. soil.” The Act made it easier to conduct pervasive surveillance by permitting courts orders that authorized general target selection parameters rather than requiring that the target of the surveillance be identified with particularity, as required by the Fourth Amendment. Recent disclosures of apparently official documents suggest that the United States has utilized these authorities to collect records related to the communications of millions of Americans. In the wake of these revelations, Pres. Obama instituted administrative reforms to impose greater checks and balances on U.S. surveillance activities. The Congress is currently considering further reforms.

The experience in the United States demonstrates how any departure from the requirement that surveillance be strictly necessary and proportionate to a legitimate interest can undermine not only the right to privacy but democratic governance itself. The surveillance of civil rights leaders, members of Congress and political parties was undertaken with the purpose of disrupting the activities of those organizations. The slow drift away from the requirements of the Fourth Amendment, including the authority to intercept communications without a showing of probable cause of criminal activity or a judicial order stating with particularity the records to be seized, has been interpreted to permit the collection of private records on millions of Americans. These deviations from accepted constitutional doctrine have cast doubt over the legality of U.S. intelligence operations, thereby undermining public support and leaving public officials without a clear understanding of what is and is not permitted.

---

The United States is not alone in this trend. Many countries continue to operate non-transparent surveillance programs without respect for the strict requirements of legality, necessity, and proportionality under international law.\footnote{See Rubinstein, Ira S., Gregory T. Nojeim, and Ronald D. Lee. "Systematic government access to personal data: a comparative analysis." \textit{International Data Privacy Law} 4.2 (2014): 96-119. (analysis of the surveillance law of Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States)} It is therefore imperative that international and regional human rights bodies require States to adopt domestic legislation in strict conformity with the requirements of legality, necessity and proportionality.

Regarding respect for the attorney-client privilege, the United States provides a distinctly contradictory example; one of strong standards for attorney-client privilege that have been ignored by its surveillance regime, forcing legal professionals to alter their work in ways detrimental to the rights of their clients.

In its seminal case on the topic, the Supreme Court of the United States ruled that, “the privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.”\footnote{Upjohn Co. v. United States, 449 U.S. 383, 389, 66 L. Ed. 2d 584 (1981).} Several years later the Court held that the 6\textsuperscript{th} Amendment right to counsel “is the right to the effective assistance of counsel,”\footnote{Strickland v. Washington, 466 U.S. 668, 686, 80 L. Ed. 2d 674 (1984).} and effective assistance of counsel can be limited by “various kinds of state interference with counsel's assistance”.\footnote{Id. at 692.} In 2012 the Court dismissed a case brought by Amnesty International, including a number of attorney employees, on the grounds that the organization could not prove it was being surveilled by the government.\footnote{See Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013).} However, during oral arguments Justice Kennedy stated, “I think the lawyer would engage in malpractice if he talked on the telephone with some of these clients, given this statute [FISA],”\footnote{Adam Liptak, \textit{Challenge to Wiretaps is Heard by Justices}, N.Y. TIMES, Oct. 29, 2012. Available at: http://www.nytimes.com/2012/10/30/us/supreme-court-hears-challenge-to-wiretaps-law.html?_r=0} a statute he said gave the State “extraordinarily wide-reaching power.”\footnote{See MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (1983).} It seems Justice Kennedy both foresaw the flaws in FISA that would be exemplified by the Snowden revelations and the impact those practices would have on the legal profession. Justice Kennedy’s statement stems from the ethical requirement in the Model Rules of Professional Conduct, which requires lawyers to protect information received in the course of representation unless the client gives informed consent for its release.\footnote{See Id. at 61-65.} Therefore, lawyers have begun to alter their practices given their knowledge that communications, such as calls with clients outside the United States, are likely tracked or monitored by the government.\footnote{See Human Rights Watch, “With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy” (July 2014) 49-65.}

As extensively documented in the recent report from Human Rights Watch, “With Liberty to Monitor All”, legal professionals in the United States have been forced to alter their practices due to knowledge of potential surveillance.\footnote{See Id. at 61-65.} Attorneys interviewed by Human Rights Watch varied in their reactions to government surveillance, some decided not to take cases likely to
receive surveillance and some were forced to only communicate with foreign clients in person in order to maintain their duty of confidentiality. The overarching conclusion – government surveillance is resulting in “the erosion of the right to counsel, a pillar of procedural justice under human rights law and the US Constitution.”

In order to adequately address past violations of the American Convention on Human Rights and provide an effective remedy to victims, Colombia must fully investigate and prosecute those responsible. Additionally, Colombian surveillance law remains flawed – failing to satisfy Colombian Constitutional protections. Ongoing violations exist because Colombian law lacks adequate requirements of prior judicial authorization, fails to limit surveillance to legitimate purposes, and leaves attorneys vulnerable to surveillance in the course of their lawful professional duties.

IV. ANALYSIS

A. PAST SURVEILLANCE ACTIVITIES OF COLOMBIA’S DEPARTMENT OF ADMINISTRATIVE SECURITY (DAS) VIOLATES THE AMERICAN CONVENTION ON HUMAN RIGHTS

Clearly documented facts in DAS files seized and examined after the revelations of 2009, present strong evidence that Colombia violated the American Convention on Human Rights. The American Convention provides that “no one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.” The Inter-American Court has defined this provision to require three elements to be met to justify infringement on the right to privacy enshrined in the American Convention: 1.) it must be established by law; 2.) it must have a legitimate purpose; and 3.) it must be appropriate, necessary, and proportionate. Past actions by DAS fail all three.

First, actions by DAS and the specialized G3 group were not established by law. The Inter-American Court requires that surveillance activities be codified by the legislature in accordance

---

127 See Id. at 5.
128 Id.
with the Constitution.\footnote{The Word “Laws” in Article 30 of the American Convention on Human Rights, Advisory Opinion OC - 6/86 (ser. A) No. 6 ¶ 22 (May 9, 1986).} The Colombian Constitution establishes that forms of private communications are inviolable, that “can only be intercepted or registered pursuant to judicial order…”\footnote{CONSTITUCIÓN POLÍTICA DE COLOMBIA [C.P.] art. 15 (unofficial translation).} As DAS interceptions were not conducted pursuant to judicial order and did intrude on private communications, the actions were not in accordance with the Constitution as required by the American Convention.\footnote{See Haugaard, Lisa, et al. “Far worse than Watergate: widening scandal regarding Colombia’s intelligence agency.” Latin America Working Group Education Fund (2010), 1.} Additionally, alleged DAS actions violated Colombian law as it stood at the time. The Code of Criminal Procedure of 2004, did not require prior judicial authorizations in particular circumstance, but did require judicial review within 36 hours of the interception of a communication to determine the “formal and material legality of the action”.\footnote{CÓDIGO DE PROCEDIMIENTO PENAL (C.C.P.) (Criminal Procedure Code) art. 14 (Law 906 of 2004). Available at: http://www.alcaldiaibogota.gov.co/sisjur/normas/Norma1.jsp?i=14787; See also, LEY 734 de 2002, Congress of Colombia, Feb. 2, 2002. Available at: http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Providencias/05-C-818.htm#material_y_formal (explaining that formal and material legality refers to the principle that criminal conduct must be codified in the law and that the facts of the situation must be contemplated within the codification of the crime.)} DAS documents indicate far reaching surveillance well beyond that contemplated by the Code of Criminal Procedure.\footnote{L. 1453 junio 24, 2011, (DIARIO OFICIAL) [D.O.] (Colom.). available at: http://www.alcaldiaibogota.gov.co/sisjur/normas/Norma1.jsp?i=43202} In 2007, the Constitutional Court required prior judicial authorization to be received before attempting to access personal information.\footnote{Corte Constitucional [C.C.] [Constitutional Court] May 9, 2007, Sentencia C-336/07, Gaceta de la Corte Constitucional [G.C.C.] (para. 33). Available at: http://www.alcaldiaibogota.gov.co/sisjur/normas/Norma1.jsp?i=25922#0} Unfortunately, this requirement was legislated out of the Code of Criminal Procedure through reforms in 2011.\footnote{L. 1453 junio 24, 2011, (DIARIO OFICIAL) [D.O.] (Colom.). available at: http://www.alcaldiaibogota.gov.co/sisjur/normas/Norma1.jsp?i=43202} DAS conducted unauthorized surveillance activities between 2007 and 2009, in contradiction to the Constitutional Court decision and not otherwise prescribed by law.\footnote{Haugaard, Lisa, et al. "Far worse than Watergate: widening scandal regarding Colombia’s intelligence agency.” Latin America Working Group Education Fund (2010) 6.}

Second, surveillance undertaken by DAS was not conducted for a legitimate purpose. The explicit objectives of DAS surveillance were all carried out in furtherance of the “judicial law” aimed at “neutralizing the influence of the Inter-American Commission for Human Rights”\footnote{Corte Constitucional [C.C.] [Constitutional Court] May 9, 2007, Sentencia C-336/07, Gaceta de la Corte Constitucional [G.C.C.] (para. 33). Available at: http://www.alcaldiaibogota.gov.co/sisjur/normas/Norma1.jsp?i=25922#0} and included the objectives of “generating controversy regarding [non-governmental organizations]”, “neutralizing influence in the Inter-American Commission on Human Rights” and “generating divisions within opposition movements.”\footnote{Id. at 1.} These objectives clearly violate the requirement established by the Inter-American Court that a “legitimate purpose” be one “where there are factual indications for suspecting a person of planning, committing or having committed certain criminal acts [or] strong suspicion that offenses are about to be committed.”\footnote{Case of Escher et al. v. Brazil, Inter-Am. Ct. H.R., Application ¶ 87 (December 20, 2007). See also Case of Klass v. Germany, Eur. Ct. H.R., 2 EHRR 214 (September 6, 1978).}
Reports of DAS documents indicate that agents undertook surveillance against a wide range of activities and targets, documenting the daily activities of NGOs, journalists, and activists.143 Third, DAS actions were neither appropriate, necessary, nor proportionate. DAS activities allegedly included routine and massive spying on human rights groups, including confidential discussions of court cases between lawyers, clients, and judicial authorities.144 DAS provided bodyguards to protect human rights defenders, some of whom reported back to DAS on the activities of their clients.145 While the Inter-American Court has not explicitly addressed the requirement of appropriateness, necessity, and proportionality in the context of surveillance it has provided applicable guidance in the area of freedom of expression. The Court indicates that government objectives must outweigh the social need for the full enjoyment of the right.146 It also holds that restrictions may not limit more than strictly necessary147 and that if various options exist, the least restrictive of the right must be selected.148 DAS surveillance does not appear to have made any attempt to select the least restrictive means of achieving the stated goal of neutralizing influence of international human rights bodies and generating divisions in opposition movements.149 Given this illegitimate purpose, it is impossible for the Court to find that DAS actions were in pursuit of an objective that should outweigh the social need for the full enjoyment of the right to privacy.

In regard to the ability to bring a case claiming violations stemming from a surveillance regime, the European Court of Human Rights has ruled that, “while the existence of a surveillance regime might interfere with privacy, a claim that this created a rights violation was justiciable only where there was a ‘reasonable likelihood’ that a person had actually been subjected to unlawful surveillance” in cases challenging the law as applied.150 The European Court of Human Rights has allowed facial challenges to surveillance law without showing specific reasonable likelihood that it was applied to the individual.151

If the Inter-American Court were to adopt a similar requirement for the adjudication of surveillance violations to the European standard of “reasonable likelihood of being subjected to unlawful surveillance”, it would first have to analyze whether the domestic surveillance law

144 Id. at 3.
145 Id. at 4.
150 The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, Human Rights Council, Agenda items 2 and 3, 27th Sess., A/HRC/27/37, ¶ 40 (30 June 2014). (Citing Esbester v. the United Kingdom, application No. 18601/91, Commission decision of 2 April 1993; Redgrave v. the United Kingdom, application No. 202711/92, Commission decision of 1 September 1993; and Matthews v. the United Kingdom, application No. 28576/95, Commission decision of 16 October 1996.)
meets the international standards, as outlined above, and whether it contradicts other domestic legal protection. If a particular law fails to fulfill these requirements, the Court would have to conclude that surveillance conducted under this law is unlawful. Therefore, a showing of “reasonable likelihood” of surveillance conducted under an inadequate surveillance law would trigger the State’s obligation to adjudicate the claim in a manner consistent with all fair trial protections in domestic and international law. However, even if “reasonable likelihood” is not found, the Inter-American Court should follow European precedent and allow facial challenges to surveillance laws where the law on its face does not meet the standards outlined in international law. International standards have indicated that “independent oversight body [...] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society” can provide prompt, thorough and impartial investigations into alleged violations.\(^\text{152}\) Under the European standard for duty to investigate and adjudicate, the Court would be tasked with considering whether the domestic surveillance law is itself unlawful under international norms, and only if the law is being challenged as applied would the Court move to a “reasonable likelihood” analysis. If the domestic law is found to violate the protections of the American Convention, then all surveillance conducted under the law must be considered unlawful, giving rise to the obligation to investigate and adjudicate claims able to demonstrate a reasonable likelihood of being subject to surveillance.

In the case of Colombia, strong evidence exists that past actions by DAS violates the American Convention on Human Rights, giving rise to the obligation to fully investigate and prosecute past abuses.

**B. TO ENSURE AN EFFECTIVE REMEDY, THE STATE OF COLOMBIA MUST FULLY INVESTIGATE AND PROSECUTE PAST ABUSES, PROVIDE ACCESS TO RECORDS AND EXPUNGE UNLAWFULLY ACQUIRED INFORMATION**

The Inter-American Court has held that States have an obligation to investigate and prosecute human rights violations but has not yet had occasion to consider whether this doctrine applies to situations of systematic violations of the right to privacy.\(^\text{153}\) The duty to punish doctrine was established by *Velásquez-Rodríguez v. Honduras*, when the Court held that under Article 1(1) of the American Convention the State must respect the “rights and freedoms recognized by the Convention,”\(^\text{154}\) and ensure “free and full exercise of [those] rights…to every person subject to its jurisdiction.”\(^\text{155}\) The Court in *Velásquez-Rodríguez* went on to clarify that the obligation to ensure free and full enjoyment of human rights meant the State has an obligation to “prevent, investigate, and punish any violations of the rights recognized by the Convention.”\(^\text{156}\) Some scholars have argued that since *Velásquez-Rodríguez* dealt with systematic state practices of

---


\(^\text{155}\) *Id.* at ¶ 166.

\(^\text{156}\) *Id.*
torture the duty to punish doctrine should only apply to cases of comparable severity. However, the language chosen by the Court in Velásquez-Rodriguez did not limit the State’s duty to prevent, investigate, and punish to cases of particular rights violations. In fact, the Court maintained similarly broad language to define the duty to punish doctrine in a number of subsequent cases. Therefore, in light of its own jurisprudence and the standards set out in international law, the Court should find that in cases of systematic surveillance, the State carries an obligation to investigate, punish, and prevent violations to the right to privacy as protected under the American Convention on Human Rights.

Full analysis of the domestic surveillance law will also inform the Courts separate consideration as to whether the law and State actions constitute a systematic violation, giving rise to a gross violation of human rights. International law provides that where human rights violations rise to the level of gross violations, criminal prosecution is required as opposed to other non-judicial remedies. This analysis will turn on how the Court chooses to define a “gross violation.” While the United Nations Basic Guidelines on the topic do not define what constitutes a gross violation, other sources provide some guidance in establishing a definition. The difference between “simple” and “gross” human rights violations require consideration of both the nature and the scope of the violation. First appearing in 1967, the term has come to be defined as “pattern of gross and reliably attested violations of human rights.”

---

161 Id. at ¶ 4, 5.
164 U.N. Commission on Human Rights, Resolution 8 (XXIII) concerning the question of violations of human rights and fundamental freedoms in any part of the world (March 1967).
Applying these international norms to situations of surveillance requires regional courts to consider whether systematic surveillance, either unlawful under domestic law or lawful under an impermissible domestic law, amount to gross violations of human rights. Courts must consider the scope of the surveillance and the nature of that surveillance. In order to determine the appropriate measures to ensure prevention of ongoing violations, and sufficiently address past violations, the Court must examine the impact, usage, and intent of the surveillance. In situations such as Colombia, the Court should take into account the troubling intent of past violations and the ongoing impact of current surveillance.

International law requires that the law must “provide for effective safeguards against abuse.”\textsuperscript{166} Specific targeting of attorneys for the exercise of their profession or surveillance regimes that broadly collect communications of attorneys would clearly violate the prohibition on disproportionate surveillance. Safeguards must be in place to address the possibility of this abusive action. Therefore, effective safeguards should include stringent prior judicial approval mechanisms that take into account the importance of attorney-client privileged information. Such safeguards should be a required aspect of a surveillance regime that comports with international legal standards. The High Commissioner\textsuperscript{167} and the European Court of Human Rights have indicated that courts charged with full and adequate adjudication of unlawful surveillance claims should have the power to order deletion of data when necessary.\textsuperscript{168} Courts empowered to order complete deletion of unlawfully collected information would provide an additional safeguard to attorneys and would deter authorities from collecting information on illegitimate targets.

The results of this analysis will provide the Court a clear roadmap for what will constitute an effective remedy that adequately protects against the possibility of ongoing abuse, addresses past violations, and punishes those responsible for violations, therefore fulfilling the right to an effective remedy.

**C. Colombian Law Does Not Appear to Satisfy Colombian Constitutional Requirements**

Colombia’s legal framework for regulating surveillance activities does not contain safeguards that meet international standards. Absent revisions to the legal framework to include the required protections, Colombian human rights defenders will continue to have reasonable cause for concern about ongoing violations of their right to privacy.

Article 15 of the Political Constitution of Colombia states that:

> “Every individual has the right to personal and family privacy and to his/her good reputation, and the State will respect them and ensure they are respected. Similarly, individuals have the right to know, access and correct any information that has been


\textsuperscript{167} Id. at ¶ 41.

\textsuperscript{168} See for example Segersted-Wiber and others v. Sweden, Eur. Ct. of Human Rights, application No. 62332/00, ¶ 118-119 (June 6, 2006). See also CCPR/C/21/Rev.1/Add. 13, ¶ 15-17.
collected about them in databases and records of public and private entities. The collection, processing and distribution of data will respect the liberty and other guarantees included in the Constitution. Correspondence and other forms of private communications are inviolable. They may only be intercepted or registered pursuant to judicial order, in those cases and with the formalities established by law. …”

However, in 2002, the Constitution was amended to allow the Attorney General to intercept and record communications without a prior court warrant. Article 250 lists one of the functions of the Attorney General as being: “to advance records, searches, seizures and interceptions of communications. In these events the judge who exercises the function of control of guarantees will be in charge of a posterior judicial review, in the following thirty-six hours.”

Article 14 and Article 244 of the Code of Criminal Procedure (Law 906 of 2004), establish the procedures for intercepting communications. Article 14 originally did not require prior judicial authorization when it was “necessary to search selective computer data, mechanisms or other means, that are not publically accessible, or when it was necessary to intercept communications.” The Article did require that a judge review such interception within 36 hours, with the goal of determining “formal and material legality of the action.” Article 224 of the Code of Criminal Procedure establishes that when an investigation aims to access information that may be confidential, the approval of the prosecutor in charge of the investigation is required before access and a judicial review of the action is required within 36 hours.

Constitutional Court Decision C-336/07, of 2007, examined these provisions to determine if prior judicial authorization should be required when attempting to access personal information. The Court concluded that because these forms of collection of information implicate the fundamental right to privacy, the Attorney General must always seek prior judicial authorization. However, while the Court held that prior judicial authorization is constitutionally required, it did not determine what information the State must provide to secure a court order authorizing surveillance.

Following the Constitutional Court decision, Congress amended the Code of Criminal Procedure in 2011. Article 52 of the amended code authorizes the Attorney General to issue warrants to

---

169 CONSTITUCIÓN POLÍTICA DE COLOMBIA [C.P.] art. 15 (unofficial translation).
172 Id. See also,LEY 734 de 2002, Congress of Colombia, Feb. 2, 2002. Available at: http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Providencias/05-C-818.htm#material_y_formal (explaining that formal and material legality refers to the principle that criminal conduct must be codified in the law and that the facts of the situation must be contemplated within the codification of the crime.)
173 CÓDIGO DE PROCEDEMIENTO PENAL (C.C.P.) (Criminal Procedure Code) art. 224 (Law 906 of 2004).
intercept communications “for the purpose of gathering material and physical evidence, search and location of the accused or convicted person, to intercept private communications transmitted by any network by magnetophonic recording or similar recording.” Such warrants are valid for 6 months. The Attorney General may extend the warrant if the circumstances justifying the interception remain. However, the extension is subject to prior review by the Control of Guarantees judge. Therefore, the Attorney General has the ability to conduct surveillance for up to 6 months before seeking any form of judicial review.

In August 2012, the Minister of Justice issued Decree 1704 regarding communication interceptions and data retention. The Decree orders all telecommunications service providers to implement the technological means and infrastructure required to guarantee access to the networks by the judicial police to undertake lawful interception activities conducted pursuant to a warrant issued by the Attorney General. This decree has been criticized by international human rights groups, which argue that it such infrastructure makes communications systems more vulnerable to unauthorized access and provides the government immediate access to the communications of anyone in the country.

Also in 2012, Law 1581 was enacted, purportedly to comprehensively protect personal data and provide individuals the ability to access and rectify information in databases maintained by third parties in accordance with their constitutional rights. However, in apparent contravention of Article 15 of the Constitution, the law exempts a number of databases from coverage, namely any database regarding national security and defense information, money laundering, or financing of terrorism, government intelligence and counter-intelligence, and those containing journalistic and editorial information, among others.

On June 7, 2011, in reaction to the DAS scandal, the Colombian Congress passed the Law on Intelligence and Counter-Intelligence, which provided for additional protection against criminal practices undertaken by DAS predecessor organization National Intelligence Directorate (DNI). However, the United Nations High Commissioner for Human Rights found that given the severity of past abuses, the 2011 law was not sufficient and that “[s]ustained and systematic action by the executive, the judiciary, the new parliamentary oversight committee and the Procurator General, in conjunction with the intelligence services themselves and their internal controls, is necessary.” The High Commissioner also expressed concern that many records

176 Id. at art. 52.
177 Id.
collected by DAS remained housed in the National Archive and that some 5,000 former DAS employees were transferred into new Government departments. The Inter-American Commission reiterated these same concerns in its 2014 report on justice, truth, and reparation in Colombia.

On April 17, 2013, the Colombian Congress passed the most recent revision to the Law on Intelligence and Counter-Intelligence, which aimed to “strengthen the legal framework that allows intelligence and counter-intelligence organs to fulfill their missions in accordance with constitutional and statutory requirements.” Authorities must destroy and not include in the intelligence and counter-intelligence database all information collected during these surveillance activities that does not serve the established goals of the mission. Regarding the interception of personal communications and data, the law requires that all such interception be in accordance with the Constitution and the Code of Criminal Procedure as previously discussed.

A controversial provision of the law authorizes the monitoring of the “electromagnetic spectrum” without prior judicial approval on the grounds that such surveillance does not amount to the “interception” of communications. This provision clearly conflicts with the Constitutional Court’s interpretation of the Constitution as the monitoring of the “electromagnetic spectrum” entails the ability to analyze all electronic activity from any device.

In summary, Colombia’s existing statutory and regulatory authorities appear to conflict in several respects with relevant Constitutional Court jurisprudence requiring prior judicial approval of the interception of electronic communications. First, the Code of Criminal Procedures authorizes surveillance pursuant to a “warrant” issued by the Attorney General for up to six months without any judicial oversight. Second, intelligence and counter-intelligence agencies can conduct electronic monitoring of the “electromagnetic spectrum” without ever seeking judicial authorization. Third, telecommunication companies are required to structure their networks in a way that allows for government access to private communications. Third, in contravention of express constitutional requirements, regulations granting access to private information held by third parties summarily exempts all national security and intelligence information. For the reasons outlined, in addition to contravening the Colombian Constitution

---

183 Id. at ¶ 58.
184 Id. at ¶ 59.
187 Id. at Art. 17.
188 Id.
189 See “Preguntas y respuestas frecuentes de Espectro Radioelectrico en Colombia,” Enciclopedia del Estado, Republic de Colombia. Available at: https://www.gobiernoenlinea.gov.co/web/guest/encyclopedia/wiki/Enciclopedia%20del%20Estado/Preguntas+y+respuestas+frecuentes+de+Espectro+Radioeléctrico+en+Colombia; See El Presidente de la Republica, Decreto 4392 Nov. 23, 2010, 47902 DIARIO OFICIAL [D.O.] (Colom.) Available at: http://www.alcaldiaibogota.gov.co/sisjur/normas/Normal.jsp?i=40814 (stating “Que el articulo 75 de la Constitucion Politica de Colombia establece que el espectro electromagnetico es un bien publico inenajenable e imperceptible sujeto a la gestion y control del Estado.”)
and relevant jurisprudence of the Constitutional Court, Colombia surveillance authorities do not meet international legal standards.

D. TO PREVENT ONGOING VIOLATIONS AND THE REPETITION OF ABUSES, COLOMBIA MUST REVISE ITS LAWS TO GENERALLY REQUIRE PRIOR JUDICIAL AUTHORIZATION OF SURVEILLANCE ACTIVITIES BASED ON A SHOWING THAT SUCH SURVEILLANCE IS STRICTLY NECESSARY TO ACHIEVE A LEGITIMATE PURPOSE

Colombia’s flawed surveillance laws fail to meet international standards and thereby expose Colombian citizens to the potential for the repetition of abuses. While Colombian authorities claim that alterations to the surveillance regime following the DAS revelations address past violations and prevent future violations, these reforms fail to require a judicial warrant that is narrowly tailored to a legitimate government interest, namely the investigation of suspected criminal activity, as required by international law.

Article 1 and 25 of the American Convention oblige State to ensure full protection of the right enshrined in the Convention and to provide judicial remedies for any violations. The Inter-American Court has held that these articles further oblige States to take adequate measures to prevent the repetition of abuses. In a case concerning allegations of unlawful surveillance, the Court stated that it “may order States […] to adapt their domestic law to conform to the American Convention, therefore as to amend or remove any provisions that unjustifiably curtail such rights, as required by the international obligation of States to respect rights and adopt domestic law provisions established in Articles 1(1) and 2 of the Convention.” In the same case the Court underscored the importance of the State adopting legislative and administrative measures necessary to implement constitutional protections to ensure “wiretapping comply with the purpose and other obligation set forth in the American Convention”, and the importance of legislation limiting the use of information held by the government regarding the private life of a person. The Court ultimately found a violation to the right to privacy based on the State’s release of information collected on the petitioner. Given the rapidly growing technological abilities of governments, the Court has also indicated that States must increase their commitment to adapt their traditional means of protection the right to privacy to the current times.

Current Colombian surveillance law only requires prior judicial approval when warrants are to be extended beyond 6 months. Prior to six months no judicial oversight is required, giving the

192 Id. at ¶ 206.
193 Id. at ¶ 223(3).
195 L. 1453, junio 24, 2011, (DIARIO OFICIAL) [D.O.] Art. 52 (Colom.).
Attorney General vast power to conduct surveillance without supervision. Additionally, all electromagnetic spectrum communications are exempt from any warrant requirement under current Colombian law. Recent abuses of this highly permissive legal framework support the need for stringent procedural safeguards, including prior judicial authorization in all cases. Such authorization must hold authorities to a high burden to prove that legality, necessity, and proportionality are met in accordance with international law, remembering that the “least intrusive” instrument must be utilized to achieve the desired legitimate aims.

International law requires that surveillance laws be tailored to a specific legitimate aim, be sufficiently precise, and limited in categories of persons, duration, and use and storage of the collected data. Even if surveillance laws are sufficiently limited in the aforementioned ways, if prior judicial authorization is not required to ensure each provision of the limited surveillance law is upheld in each instance of interferences, the rights at question remain ineffectively safeguarded as required by international law.

E. TO PROTECT THE RIGHT TO COUNSEL, COLOMBIA MUST REFRAIN FROM CONDUCTING SURVEILLANCE ON ATTORNEYS ABSENT A SHOWING THAT THEY ARE LIKELY TO HAVE ENGAGED IN CRIMINAL MISCONDUCT

Respect for the confidentiality of attorney-client communications is essential to the proper functioning of any judicial system. Surveillance of such communications should only be permitted if there is compelling evidence that the attorney is engaged in unlawful activity. Surveillance of attorneys merely because they may represent or have contact with those alleged to have engaged in criminal activity without any showing that the attorneys were involved in illegal activity is per se disproportionate and therefore a violation of the right to privacy.

The international law framework for controlling surveillance in accordance with the right to privacy provides adequate protections, when fully applied, to protect against surveillance of confidential attorney-client communications. First, international standards require that laws interfering with the right to privacy be “publicly accessible.” A publically accessible law would allow attorneys to understand the surveillance regime, such that they could predict with some reasonable degree of certainty when their communications are likely to be monitored.

If surveillance is properly limited to those believed to be engaged in criminal activity, then attorneys can be reasonably assured that their communications are not intercepted so long as they do not engage in criminal activity.

---

196 Id.
199 Id. at ¶ 30.
200 Id. ¶ 28-30.
201 Id. at ¶ 28.
Second, international law requires that the law must “contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims”.

The mere fact that the attorney represents individuals thought to be engaged in criminal activities, including armed insurgents, is not a legitimate reason to intercept confidential communications as all individuals, including those suspected of criminal activity have a right to confidential communications with their counsel. The DAS' apparent policy of treating Colombian human rights attorneys as an extension of illegal armed groups clearly conflicts with international law in that it permitted surveillance of individuals not believed to be engaged in criminal activities.

Nor did the surveillance of human rights defenders meet the requirement that surveillance be proportional to a legitimate interest. As the U.N. High Commissioner on Human Rights explained “it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.” Thus, even if a client is legitimately the target of surveillance, the State may not simply sweep up all of his communications regardless of such actions impact on all those surrounding the target. The State may not conduct surveillance on an individual when communicating with his attorney, absent separate justification to believe the client is utilizing the attorney in furtherance of criminal activities. International law calls for the limitation on the durations of surveillance, and procedures for the use and storage of the data collected, therefore international law would be respected through restrictive procedures for the collection, use and storage of privilege attorney-client communications. Limiting surveillance in this manner would provide additional protection against undue surveillance of confidential attorney client communications.

The negative impact on the legal profession of secretive and broad surveillance programs, that do not meet all requirements under international law, is clear. Cases of national and international importance that may lead to violations of their personal right to privacy will deter lawyers for taking such cases. Lawyers must adjust how they communicate with their clients, leading to limitations in the effectiveness of their representation.

VII. CONCLUSION

202 Id.
203 Id. at ¶ 25.
204 Id. at ¶ 28.
International law continues to expand on the rapidly growing issue of surveillance. On October 23, 2014, the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, released his annual report focused on the protection of the right to privacy in expansive surveillance regimes. During the sixty-ninth session of the General Assembly, Mr. Emmerson reiterated that “measures that interfere with the right to privacy must be authorized by accessible and precise domestic law that pursues a legitimate aim, is proportionate and necessary.” To enforce such domestic law and ensure the right to privacy, Mr. Emmerson asserts that “We need strong and independent oversight bodies that are adequate for a review before these programmes are applied,” and that “individuals must have the right to seek an effective remedy for any alleged violation of their online privacy rights.”

As international law continues to adjust to current realities of surveillance capacities, the key principles of legitimacy, necessity, and proportionality remain at the heart of effective protection of the right to privacy. As elaborated by the United Nations Human Rights Council, these principles require strong upfront protections to State intrusion of private communications. Organs of the United Nations have taken the first step in further defining the parameters of permissible surveillance laws. Regional human rights systems should adopt these strict parameters of permissible surveillance programs such that the international community is united in its promotion of the right of privacy in the face of problematic State surveillance activities.

The situation in Colombia presents the Inter-American system with the opportunity to further elaborate its binding jurisprudence in this area, and take important steps towards the restriction of abusive surveillance programs currently being elaborated in the region. It is vital that the international community presents united standards for what constitutes a permissible surveillance law, including strong upfront protections, extensive oversight, and access to effective remedies for those subject to questionable surveillance.

Not only is the right to privacy of millions at stake – the chilling effect experienced by vital aspects of a democratic society continues to dramatically impact the realization of numerous fundamental human rights across the Americas.

---


208 Id.