
**Before the
Inter-American Court of Human Rights**



Members of José Alvear Restrepo Lawyers'
Collective

v.

Colombia



**Brief of *Amici Curiae* Article 19, Electronic
Frontier Foundation, Fundación Karisma, and
Privacy International**



ROXANNA ALTHOLZ
INTERNATIONAL HUMAN RIGHTS LAW CLINIC
UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF LAW
353 Law Building
Berkeley, CA 94720
+1 (510) 643-8781
raltholz@law.berkeley.edu

ASTHA SHARMA POKHAREL
INTERNATIONAL HUMAN RIGHTS LAW CLINIC
UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF LAW
353 Law Building
Berkeley, CA 94720
+1 (510) 642-4139
asharmapokharel@clinical.law.berkeley.edu

Counsel for *Amicus Curiae*

Table of Contents

I. TABLE OF CITED AUTHORITIES	I
II. INTEREST OF AMICI CURIAE	1
III. SUMMARY OF ARGUMENT.....	2
IV. ARGUMENT.....	3
A. TO THE DETRIMENT OF DEMOCRATIC SOCIETIES, UNLAWFUL AND ARBITRARY STATE SURVEILLANCE VIOLATES A CONSTELLATION OF HUMAN RIGHTS PROTECTED BY THE AMERICAN CONVENTION.	3
1. <i>Colombia has built a pervasive communications surveillance system with expansive technical capabilities.</i>	4
2. <i>Colombia’s communications surveillance system has far-reaching implications for a constellation of human rights protected by the American Convention.</i>	8
a. Communications surveillance interferes with the right to privacy.	9
b. Communications surveillance interferes with the rights to life and personal integrity.	11
c. Communications surveillance interferes with the right to freedom of expression and thought.	12
d. Communications surveillance interferes with the freedom of association and movement.	14
e. Communications surveillance imperils the rights of children.....	16
B. COLOMBIA’S FAILURE TO ADEQUATELY REGULATE COMMUNICATIONS SURVEILLANCE BY INTELLIGENCE AGENCIES VIOLATES RIGHTS PROTECTED BY THE AMERICAN CONVENTION.	18
1. <i>This Court must examine Colombia’s surveillance against the most protective international human rights standards.</i> 19	19
a. Communications surveillance by intelligence authorities must be regulated to meet the standards of legality, legitimacy, suitability, necessity, and proportionality established by the American Convention.....	19
b. This Court should affirm that mass surveillance is incompatible with international human rights standards.	23
c. Communications surveillance must be subject to prior judicial authorization and independent oversight to safeguard against abuse.....	24
d. Targets of unlawful communications surveillance must have access to effective remedies, which requires notice of surveillance and the ability to correct or erase the information collected.	27
e. The public must have the right of access information on state surveillance practices, which is a crucial safeguard against abuse.	29
2. <i>Colombia’s existing legal framework regulating intelligence activities enables abusive surveillance practices in violation of the American Convention.</i>	30
a. The Intelligence Law gives Colombian authorities wide latitude to surveil HRDs for vague purposes, in an undefined manner, and for an indefinite period, with inadequate safeguards against abuse.	30
i. The vagueness and overbroad language of the Intelligence Law invites unlawful state surveillance.	31
ii. The Intelligence Law has failed to prevent unlawful communication interception by intelligence agencies...32	32
iii. The Intelligence Law gives intelligence authorities ill-defined power to access metadata retained by communication service providers in violation of the principle of proportionality.	34
iv. The Intelligence Law fails to properly limit who may be subject to communications surveillance.	35
v. The Intelligence Law is unclear on the permitted duration of surveillance and enables data retention for excessively long periods of time.	36
vi. The Intelligence Law exempts intelligence agencies from any meaningful process of authorization, oversight, or notification, exacerbating the threats posed by the excessive discretion delegated to those agencies.	37
b. Colombian law regulating data processing, correction, erasure, and data transfers exacerbate the risks posed to members of CCAJAR and their families.....	41
i. Colombian laws give HRDs no opportunity to correct or erase the data that the state has collected on them. 41	41
ii. Colombian laws provided inadequate safeguards against improper foreign data transfers.	43
V. CONCLUSION	45

I. TABLE OF CITED AUTHORITIES

CASES

Barreto Leiva v. Venezuela, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 206 (Nov. 17, 2009).....	28
Big Brother Watch v. United Kingdom, App. No. 58170/13, Eur. Ct. H.R. (May 25, 2021), https://hudoc.echr.coe.int/fre?i=001-210077	passim
Cantoral-Huamaní and García-Santa Cruz v. Peru, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 167 (Jul. 10, 2007)).	15
Case C-140/20, G.D. v. Commissioner of An Garda Síochána and others, ECLI:EU:C:2022:258, ¶ 105 (Apr. 5, 2021)	24
Case C-293/12, Digital. Rights Ireland., Ltd. v. Minister for Communications, ECLI:EU:C:2014:238 (Apr. 8, 2014).....	passim
Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).....	29, 42
Case C-623/17, Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affs. and Others., ECLI:EU:C:2020:790 (Oct. 6, 2020)	24, 25
Case C-746/18, H. K. v. Prokuratuur, ECLI:EU:C:2021:152, ¶¶ 26, 59 (Mar. 2, 2021)	39
Case of “Las Dos Erres” Massacre v. Guatemala, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 211 (Nov. 24, 2009)	22
Case of Abrill Alosilla et al. v. Perú, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 223 (Mar. 4, 2011).	28
Case of the Persons Deprived of Liberty in the “Dr. Sebastião Martins Silveira” Prison in Araraquara, São Paulo, Provisional Measures, Order, ¶ 24, (Inter-Am. Ct. H.R. Sept. 30, 2006), https://www.corteidh.or.cr/docs/medidas/araraquara_se_02_ing.pdf	11
Case of the Xákmok Kásek Indigenous Community v. Paraguay, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 214 (Aug. 24, 2010).....	28
Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net v. Premier Ministre, ECLI:EU:C:2020:791, ¶¶ 137-39 (Oct. 6, 2020)	24, 38
Castillo Páez v. Perú, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 34 (Nov. 3, 1997)	27
Chaparro Álvarez and Lapo Íñiguez v. Ecuador, Interpretation of the Judgment on Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 189 (Nov. 26, 2008).....	23
Chitay Nech et. al v. Guatemala, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 212 (May 25, 2010)	17, 22
Claude Reyes et al. v. Chile, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 151 (Sept. 19, 2006)	14, 23, 30
Constitutional Court v. Peru, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 71 (Jan. 31, 2001)	28
Constitutional Tribunal (Camba Campos et al.) v. Ecuador, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 268 (Aug. 28, 2013)	28
Corte Constitucional [C.C.] [Constitutional Court], julio 12, 2012, Sentencia C-540, Gaceta de la Corte Constitucional [G.C.C.] (Colom.)	34, 35, 36
Corte Suprema de Justicia [C.S.J.] [Supreme Court], septiembre 1, 2020, Sentencia T-374/20 (Colom.), https://www.corteconstitucional.gov.co/relatoria/2020/T-374-20.htm	14

Ekimdzhev v. Bulgaria, App. No. 70078/12, Eur. Ct. H.R. (Jan. 11, 2022), https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-214673%22%7D	passim
Escher et al. v. Brazil, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 200 (Jul. 6, 2009).....	passim
Escué Zapata v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 165 (Jul. 4, 2007).....	24, 26
Faber v. Germany, App. No. 40721/08, Eur. Ct. H.R. (Jul. 24, 2012), https://hudoc.echr.coe.int/eng?i=001-112446	23
Fernández Prieto and Tumbeiro v. Argentina, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 411 (Sept. 1, 2020)	24
Furlan and Family v. Argentina, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 246, ¶¶ 125-27 (Aug. 31, 2012)	17
Goiburú et al. v. Paraguay, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 153 (Sept. 22, 2006)	22, 28
Gomes-Lund v. Brazil, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 11.552 (Nov. 24, 2010)	14
Gómez Paquiyauri Brothers v. Peru, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 110 (Jul. 8, 2004).	16, 17
Herrera Ulloa v. Costa Rica, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 107 (Jul. 2, 2004).....	12, 19
Huilca Tecse v. Peru, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 121 (Mar. 3, 2005).....	14, 15
Inter-Am. Ct. H.R., Public Hearing in Case Members of José Alvear Restrepo Lawyers' Collective v. Colombia Part 2, YOUTUBE (May 13, 2022), https://youtu.be/8Fiv0Hcl86o . 2, 19, 30, 33	
Iordachi v. Moldova, App. No. 25198/02, Eur. Ct. H.R. (Sept. 24 2009), https://hudoc.echr.coe.int/fre?i=002-1661	21
Isaza Uribe et al. v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 363 (Nov. 20, 2018).....	22, 32
Ivcher Bronstein v. Peru, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 74 (Feb. 6, 2001).....	26, 28
Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, Sec'y of State for the Home Dep't v. Watson, ECLI:EU:C:2016:970 (Dec. 21, 2016).....	passim
Juridical Condition and Human Rights of the Child, Advisory Opinion OC-17/02, Inter-Am. Ct. H.R. (ser. A) No. 17 (Aug. 28, 2002).	16, 18
Juvenile Reeducation Institute v. Paraguay, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 112 (Sept. 2, 2004).....	17
Kaliña and Lokono Peoples v. Suriname, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 309 (Nov. 25, 2015).	28
Kimel v. Argentina, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 177 (May 2, 2008).	11, 20, 23
Lagos del Campo v. Perú, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 340 (Aug. 31, 2013).	28
López -Álvarez v. Honduras, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 141 (Feb. 1, 2006).....	28

Manuel Cepeda Vargas v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 213 (May 26, 2010).....	4
Mapiripán Massacre v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 134 (Sept. 15, 2005)	19
Maritza Urrutia v. Guatemala, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 103 (Nov. 27, 2003).....	24
Matter of the Monagas Detention Center (“La Pica”), Provisional Measures, Order, (Inter-Am. Ct. H.R. ., ¶ 14, (Inter-Am. Ct. H.R. Feb. 9, 2006), https://www.corteidh.or.cr/docs/medidas/lapica_se_02_ing.pdf	11
Merits Report No. 57/19, Corporación Colectivo de Abogados “José Alvear Restrepo” v. Colombia, Case 12.380 OEA/Ser.L/V/II.172 Doc. 66	passim
Molina Thiessen v. Guatemala, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 106 (May 4, 2004).....	22
Myrna Mack-Chang v. Guatemala, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 101 (Nov. 25, 2003).....	24, 26
Nadege Dorzema et al. v. Dominican Republic, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 251 (Oct. 24 2012)	28
Nogueira de Carvalho et al. v. Brazil, Preliminary Objections and Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 161 (Nov. 28, 2006)	11
Opinion 1/15, Draft Agreement between Canada and the European Union, ECLI:EU:C:2017:592 (Jul. 26, 2017).....	44
Pacheco Tineo Family v. Bolivia, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 272 (Nov. 25, 2013).....	28
Roman Zakharov v. Russia, Application No. 47143/06, Eur. Ct. H.R. (Dec. 4, 2015), https://hudoc.echr.coe.int/fre#%22itemid%22:[%22002-10793%22]	passim
Rotaru v. Romania, App. No. 28341/91, Eur. Ct. H.R. (May 4, 2000), https://hudoc.echr.coe.int/eng?i=001-58586	13, 37
Ruano Torres et al. v. El Salvador, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 303 (Oct. 5, 2015).....	28
Sedletska v. Ukraine, App. No. 42634/18, Eur. Ct. H.R., ¶¶ 62, (Apr. 1, 2021)	21
Sommer v. Germany, App. No. 73607/13, Eur. Ct. H.R. (Apr. 27, 2017), https://hudoc.echr.coe.int/eng?i=001-173091	21
Sürek v. Turkey (No. 3), App. Nos. 23927/94 and 24277/94, Eur. Ct. H.R. (1999), https://hudoc.echr.coe.int/fre?i=001-58278	12
Szabo v. Hungary, App. No. 37138/14, Eur. Ct. H.R. (Jan. 12, 2016), https://hudoc.echr.coe.int/fre?i=001-160020	passim
Tibi v. Ecuador, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 114 (Sept. 7, 2004).....	28
Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 193 (Jan. 27, 2009).	20, 21, 22, 33
Umohoza v. Rwanda, 2 AfCLR 165 (African Court on Human and Peoples’ Rights 2017).....	23
Valle Jaramillo et al. v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 192 (Nov. 27, 2008).....	9, 11, 15, 16
Velásquez Rodríguez v. Honduras, Preliminary Objections, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 1 (June 26, 1987)	28

Vélez Lóor v. Panama, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 218 (Nov. 23, 2010)	28
Villagrán Morales et. al v. Guatemala, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 63 (Nov. 19, 1999).....	17
Villamizar Durán et al. v. Colombia, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 364 (Nov. 20, 2018).....	22, 32
Yarce et al. v. Colombia, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 325 (Nov, 22, 2016)	15

CONSTITUTIONAL PROVISIONS, STATUTES, AND REGULATIONS

American Declaration of the Rights and Duties of Man, O.A.S., Res. XXX (1948), O.A.S. Off. Rec. OEA/Ser.LV/I.4 Rev. (1965)	27
Convention on the Rights of Persons with Disabilities, <i>opened for signature</i> Dec. 13, 2005, 2515 U.N.T.S. 3.....	9
Convention on the Rights of the Child, <i>opened for signature</i> Nov. 20, 1989, 1577 U.N.T.S. 3. ..9, 18	
Decree 1704, agosto 15, 2012 DIARIO OFICIAL (Colom.)	37
Decree 2149, diciembre 20, 2017, DIARIO OFICIAL (Colom.)	43
European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS 5 (1953)	10, 22
G.A. Res. 1671 (XXIX-O/99), Human Rights Defenders in the Americas, Support for the Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas (June 7, 1999).....	9
G.A. Res. 217A (III), Universal Declaration of Human Rights (Dec. 10, 1948).....	9, 27
G.A. Res. 2517 (XXXIX-O/09), Human Rights Defenders: Support for the Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas (June 4, 2009).....	9
G.A. Res. 53/144, Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms (Mar. 8, 1999)	9
G.A. Res. 68/167 (Dec. 18, 2013)	25, 27
G.A. Res. 69/166, The Right to Privacy in the Digital Age (Dec. 18, 2014).....	30, 36
G.A. Res. 75/291, The United Nations Global Counter-Terrorism Strategy: seventh review (July 30, 2021).....	27
Hum. Rts. Council Res. 48/4, pmbl., U.N. Doc. A/HRC/RES/48/4 (Oct. 7, 2021).	21
International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, <i>opened for signature</i> Dec. 18, 1990, 2220 U.N.T.S. 3.	9, 22, 27
International Covenant on Civil and Political Rights, <i>opened for signature</i> Dec. 16, 1966, 999 U.N.T.S.171.....	9
Investigatory Powers Act 2016 (U.K.)	41
L. 1581, octubre 18, 2012, DIARIO OFICIAL (Colom.).....	42, 45
L. 1621, abril 17, 2013, DIARIO OFICIAL (Colom.)	passim
L. 1712, marzo 6, 2014, DIARIO OFICIAL p. 1	42
L. 906, septiembre 1, 2004, DIARIO OFICIAL (Colom.)	31
Organization of American States, American Convention on Human Rights, Nov. 22, 1969, O.A.S.T.S. No. 36; 1144 U.N.T.S. 123.	passim

Resolution 912, enero 15, 2009, DIARIO OFICIAL (Colom.).....	37
--	----

REPORTS BY INTERNATIONAL HUMAN RIGHTS BODIES

Catalina Botero Marino (Special Rapporteur for Freedom of Expression), Inter-American Commission on Human Rights, <i>Freedom of Expression and the Internet</i> , OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13 (Dec. 31, 2013)	passim
Clément Nyaletsossi Voule (Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association), <i>Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association</i> , U.N. Doc. A/HRC/41/41 (May 17, 2019)	15, 16
Comm. Against Torture, <i>Consideration of Reports Submitted by States Parties under Article 19 of the Convention Concluding Observations of the Committee against Torture: Colombia</i> , U.N. Doc. CAT/C/COL/CO/4 (May 4, 2010)	4
Comm. on the Rts. of the Child, <i>Concluding Observations of the Committee on the Rights of the Child: France</i> , U.N. Doc. CRC/FRA/CO/4 (June 22, 2009)	17
Comm. on the Rts. of the Child, <i>Concluding Observations of the Committee on the Rights of the Child: United Kingdom of Great Britain and Northern Ireland</i> , U.N. Doc. CRC/C/GBR/CO/4 (Oct. 20, 2008).....	17
Comm. on the Rts. of the Child, <i>Concluding Observations on the Combined Fourth and Fifth Periodic Reports of Colombia</i> , U.N. Doc. CRC/C/COL/CO/4-5 (Mar. 6, 2015).	18
Comm. on the Rts. of the Child, <i>Concluding observations on the second periodic report of Kuwait</i> , U.N. Doc. CRC/C/ KWT/CO/2 (Oct. 29, 2013).....	17
Comm. on the Rts. of the Child, <i>General Comment No. 25 on Children’s Rights in Relation to the Digital Environment</i> , U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).....	18
David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), <i>Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression</i> , U.N. Doc. A/HRC/29/32 (May 22, 2015)	9, 13
David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), <i>Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Surveillance and Human Rights</i> , U.N. Doc. A/HRC/41/35 (May 28, 2019).....	12, 14
David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), <i>Report on the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression</i> , ¶ 56, U.N. Doc. A/HRC/32/38 (May 11, 2016).....	13
David Kaye, et al. (Special Rapporteur on Freedom of Opinion and Expression et al.), <i>Joint Declaration on Freedom of Expression and Responses to Conflict Situations</i> (May 4, 2015), http://www.osce.org/fom/154846	23, 37
David Kaye, et al. (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression et al.), <i>Communication sent to Colombia by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Special Rapporteur on the Situation of Human Rights Defenders, Special Rapporteur on the Promotion of Truth, Justice, Reparation and Guarantees of Non-repetition, and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the Organization of American States</i> , COL 5/20 (June 15, 2020).....	3

Edison Lanza (Special Rapporteur for Freedom of Expression), <i>Standards for a Free, Open and Inclusive Internet</i> , OEA/Ser.L/V/II CIDH/RELE/INF.17/17 (Mar. 15, 2017)	10, 35
Edison Lanza (Special Rapporteur on Freedom of Expression), <i>The Right to Information and National Security</i> , OEA/Ser.L/V/II CIDH/RELE/INF.24/20 (July 2020)	26, 30, 37
Frank La Rue (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), <i>Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression</i> , U.N. Doc. A/HRC/23/40 (Apr. 17, 2013)	passim
Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), <i>Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Mission to the former Yugoslav Republic of Macedonia</i> , U.N. Doc. A/HRC/26/30/Add.2 (Apr. 1, 2014)	14
Frank William La Rue, Cataline Botero (Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights), <i>Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression</i> (June 21, 2013), https://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&IID=1	passim
Hum. Rts. Comm., <i>Concluding Observations on the Initial Report of Pakistan</i> , U.N. Doc. CCPR/C/PAK/CO/1 (Aug. 23, 2017).....	44
Hum. Rts. Comm., <i>Concluding Observations on the Fifth Periodic Report of Belarus</i> , U.N. Doc. CCPR/C/BLR/CO/5, ¶ 44 (Nov. 22 2018)	20, 25, 27
Hum. Rts. Comm., <i>Concluding Observations on the Fourth Periodic Report of the United States of America</i> , U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014)	8, 22, 36, 38
Hum. Rts. Comm., <i>Concluding Observations on the Seventh Periodic Report of Colombia</i> , U.N. Doc. CCPR/C/COL/CO/7 (Nov. 17, 2016)	33
Hum. Rts. Comm., <i>Concluding Observations on the Seventh Periodic Report of Germany</i> , ¶ 43, U.N. Doc. CCPR/C/DEU/CO/7 (Nov. 11, 2021)	25
Hum. Rts. Comm., <i>Concluding Observations on the Seventh Periodic Report of Sweden</i> , U.N. Doc. CCPR/C/SWE/CO/7 (Apr. 28, 2016).	44
Hum. Rts. Comm., <i>Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland</i> , U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17 2015).....	24, 44
Hum. Rts. Comm., <i>Concluding Observations on the sixth periodic review of Hungary</i> , U.N. Doc. CCPR/C/HUN/CO/6 (May 9, 2018).....	23, 25, 27
Hum. Rts. Comm., <i>Consideration of reports submitted by States parties under article 40 of the Covenant Concluding: Colombia</i> , U.N. Doc. CCPR/C/COL/CO/6 (Aug. 4, 2010)	4, 11
Hum. Rts. Comm., <i>Consideration of reports submitted by States parties under article 40 of the Covenant</i> , U.N. Doc. CCPR/C/COL/CO/6 (Aug. 4, 2020).....	43
Hum. Rts. Comm., <i>General Comment No. 16: Article 17 (Right to Privacy)</i> , in <i>Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies The Right to Respect of Privacy, Family Home and Correspondence and Protection of Honour and Reputation</i> , U.N. Doc. HRI/GEN/Rev.9 (Apr. 8, 1988).	10
Hum. Rts. Comm., <i>General Comment No. 34: Article 19: Freedoms of Opinion and Expression</i> , U.N. Doc. CCPR/C/GC/34 (Sept. 11, 2011).	13
Hum. Rts. Comm., <i>General Comment No. 37 on the Right of Peaceful Assembly (Article 21)</i> , U.N. Doc. CCPR/C/GC/37 (Sept. 17, 2020)	15

Hum. Rts. Comm., <i>List of issues in relation to the seventh periodic report of Colombia: Replies of Colombia to list of issues in relation to the seventh period report of Colombia</i> , U.N. Doc. CCPR/C/COL/Q/7/Add.1 (Aug. 18, 2016).	34
Hum. Rts. Comm., <i>Van Hulst v. Netherlands</i> , U.N. Doc. CCPR/C/82/D/903/1999 (Nov. 1, 2004)	22
Industrio y Comercio Superintendencia, <i>Circular Externa No. 005 [External Memorandum]</i> , August 10, 2017, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Circular_Externa_5_Ago_10_2017.pdf	45
Inter-Am. Comm'n H. R., <i>Chapter V: Follow-up to Recommendations Made by the IACHR in Its Report TruthCountry or Thematic Reports</i> , in <i>Annual Report 2018</i> (2018), http://www.oas.org/en/iachr/docs/annual/2018/docs/IA2018cap.5CO-en.pdf	43
Inter-Am. Comm'n. H. R., <i>Declaration of Principles on Freedom of Expression</i> , Res., 108th Sess. (Oct. 2000), http://www.cidh.oas.org/Relatoria/showarticle.asp?artID=26&IID=1.29 , 42	
Inter-Am. Comm'n. H.R., <i>Human Rights Defenders and Social Leaders in Colombia</i> , OEA/Ser.L/V/II 29 (2019).	4, 22
Inter-Am. Comm'n. H.R., <i>Report on Situation of Human Rights Defenders in the Americas</i> , OEA/Ser.L/V/II.124 Doc.5 rev.1 (Mar. 7, 2006).	16
Inter-Am. Comm'n. H.R., <i>Truth, Justice and Reparation: Fourth Report on Human Rights Situation in Colombia</i> , OEA/Ser.L/V/II. Doc. 49/13 (Dec. 31, 2013)	3
<i>Johannesburg Principles on National Security, Freedom of Expression and Access to Information</i> , princ. 1.3, U.N. Doc. E/CN.4/1996/39 (Mar. 22, 1996).....	23
Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), <i>Report of the United Nations Special Rapporteur on the Right to Privacy</i> , U.N. Doc. A/HRC/34/60 (Sept. 6, 2017)	8, 14
Joseph Cannataci (Special Rapporteur on the Right to Privacy), <i>Report of the Special Rapporteur Artificial intelligence and privacy, and children's privacy</i> , U.N. Doc. A/HRC/46/37 (Jan. 21, 2021).....	17
Joseph Cannataci (Special Rapporteur on the Right to Privacy), <i>Report of the Special Rapporteur on the Right to Privacy</i> , U.N. Doc. A/HRC/40/63 (Oct. 16, 2019).....	passim
Joseph Cannataci (Special Rapporteur on the Right to Privacy), <i>Report of the United Nations Special Rapporteur on the Right to Privacy</i> , U.N. Doc. A/HRC/37/62 (Oct. 25, 2018)	11, 12
Maina Kiai (Special Rapporteur on the Rights to Freedom of Peaceful assembly and of Association), <i>Report of the Special Rapporteur on the Rights to Rreedom of Peaceful Assembly and of Association on His Follow-up Mission to the United Kingdom of Great Britain and Northern Ireland</i> , U.N. Doc. A/HRC/35/28/Add.1 (June 8, 2017)	15
Martin Scheinin (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism), <i>Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism: Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, Including on Their Oversight</i> , U.N. Doc. A/HRC/14/46 (May 17, 2010)	passim
Michel Forst (Special Rapporteur on the Situation of Human Rights Defenders), <i>Visit to Colombia: Report of the Special Rapporteur on the Situation of Human Rights Defenders</i> , U.N. Doc. A/HRC/43/51/Add.1 (Dec. 26, 2019)	4
Pedro Vaca Villareal (Special Rapporteur for Freedom of Expression), <i>Annual Report of the Office of the Special Rapporteur for Freedom of Expression</i> , OEA/Ser.L/V/II Doc. 28 (Mar. 30, 2021) http://www.oas.org/en/iachr/docs/annual/2020/Chapters/rele-en.PDF	7, 8

Press Release, Inter-Am. Comm’n H.R., <i>IACHR and its Special Rapporteurship for Freedom of Expression Urge the State of Colombia to Conduct a Diligent, Timely, and Independent Investigation into Allegations of Illegal Surveillance Against Journalists, Justice Operators, Human Rights Defenders</i> , Press Release No. 118/20 (May 21, 2020), https://www.oas.org/en/iachr/media_center/PReleases/2020/118.asp	23
U.N. High Comm’r for Hum. Rts., <i>Annual Report of the United Nations High Commissioner for Human Rights on the situation of human rights in Colombia</i> , U.N. Doc. A/HRC/34/3/Add.3 (Mar. 14, 2017)	33, 43
U.N. High Comm’r for Hum. Rts., <i>Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in Colombia</i> , ¶ 25, U.N. Doc. A/HRC/19/21/Add.3 (Jan. 31 2012)	41, 43
U.N. High Comm’r for Hum. Rts., <i>Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in Colombia</i> , U.N. Doc. A/HRC/13/72 (Mar. 4, 2010)	4
U.N. High Comm’r for Hum. Rts., <i>Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in Colombia</i> , U.N. Doc. A/HRC/4/48 (March 5, 2007)	43
U.N. High Comm’r for Hum. Rts., <i>The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights</i> , U.N. Doc. A/HRC/27/37 (June 30, 2014)	passim
U.N. High Comm’r for Hum. Rts., <i>The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights</i> , U.N. Doc. A/HRC/39/29 (Aug. 3, 2018)	passim

BOOKS, ARTICLES, AND NGO REPORTS

“¡Tapen, tapen, tapen!”: así fue el allanamiento de la Corte Suprema a una instalación del Ejército, SEMANA (Jan. 13, 2020), https://www.semana.com/nacion/multimedia/nuevas-chuzadas-del-ejercito-en-colombia/647868/	7
Adriaan Alsema, <i>Colombia Police ‘Wiretapping, Shadowing and Intimidating Journalists’</i> , COLOMBIA REPORTS (Dec. 3, 2015), https://colombiareports.com/colombias-police-wiretapping-and-intimidating-journalists/	6
Ali Boyacı et al, <i>Monitoring, Surveillance, and Management of the Electromagnetic Spectrum: Current Issues in Electromagnetic Spectrum Monitoring</i> , 18 ELECTRICA 100 (2018), https://electricajournal.org/Content/files/sayilar/28/100-108.pdf	34
<i>Chuzadas sin Cuartel</i> , SEMANA (Jan. 1, 2020), https://www.semana.com/nacion/articulo/chuzadas-por-que-se-retiro-el-general-nicacio-martinez-del-ejercito/647810/	8
Congressional Research Service, <i>Overview of Department of Defense Use of the Electromagnetic Spectrum</i> (2021), https://crsreports.congress.gov/product/pdf/R/R46564/8	34
DEJUSTICIA, FUNDACIÓN KARISMA AND PRIVACY INTERNATIONAL, <i>THE RIGHT TO PRIVACY IN COLOMBIA STAKEHOLDER REPORT UNIVERSAL PERIODIC REVIEW 30TH SESSION – COLOMBIA</i> (2017), https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=5412&file=EnglishTranslation	41, 43
DEJUSTICIA, <i>RESPONSE TO CALL FOR INPUTS ON HUMAN RIGHTS CHALLENGES RELATING TO THE RIGHT TO PRIVACY IN THE DIGITAL AGE IN COLOMBIA</i> (2018),	

https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Dejusticia.pdf	45
<i>Dónde Estan Mis Datos?</i> , FUNDACIÓN KARISMA (2021), https://web.karisma.org.co/donde-estan-mis-datos-2021/	6
<i>El Informe Forense de las Carpetas Secretas</i> , SEMANA (May 12, 2020), https://www.semana.com/nacion/articulo/el-informe-forense-de-las-carpetas-secretas/670853/	7
FRONT LINE DEFENDERS, FRONTLINE DEFENDERS GLOBAL ANALYSIS (2018), https://www.frontlinedefenders.org/en/resource-publication/global-analysis-2018	4
FUNDACIÓN KARISMA, FUNDACIÓN KARISMA’S RESPONSE TO CALL FOR INPUT TO A REPORT ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE BY THE UN HIGH COMMISSIONER FOR HUMAN RIGHTS (2018), https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Karisma.pdf	6
FUNDACIÓN KARISMA, UN RASTREADOR EN TU BOLSILLO: ANÁLISIS DEL SISTEMA DE REGISTRO DE CELULARES EN COLOMBIA 27 (2017), https://nomascelusvigilados.karisma.org.co/para-leer/informe-de-investigaci%C3%B3n.html	35
<i>Guide to International Law and Surveillance 3.0</i> , PRIVACY INTERNATIONAL (2021), https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance	11
Gustavo Gallon, <i>Inteligencia en Beneficio del Gobierno y de Toda la Sociedad</i> , EL ESPECTADOR (May 6, 2020), https://www.elespectador.com/opinion/columnistas/gustavo-gallon/inteligencia-en-beneficio-del-gobierno-y-de-toda-la-sociedad-column-918263/	44
<i>In Colombia, PUMA Is Not What It Seems</i> , DIGITAL RIGHTS LAC (2015), https://digitalrightslac.derechosdigitales.org/en/en-colombia-el-puma-no-es-como-lo-pintan/ . 6	
Juan Sebastian Lombo, <i>El Fantasma de la Comision de Inteligencia</i> , EL ESPECTADOR (May 25, 2020), https://www.elespectador.com/noticias/politica/el-fantasma-de-la-comision-de-inteligencia	41
KATITZA RODRÍGUEZ PEREDA, ELECTRONIC FRONTIER FOUNDATION, COMPARATIVE ANALYSIS OF SURVEILLANCE LAWS AND PRACTICES IN LATIN AMERICA (2016), https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016.pdf	41
KATITZA RODRIGUEZ, VERIDIANA ALIMONTI, NECESSARY AND PROPORTIONATE, THE STATE OF COMMUNICATION PRIVACY IN COLOMBIA (2020), https://necessaryandproportionate.org/uploads/2020-colombia-en-faq.pdf#question5	31
<i>Las Carpetas Secretas</i> , SEMANA (May 5, 2020), https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/	8, 42
<i>Lo que quería el Ejército con ‘Hombre invisible’ que hizo chuzadas reveladas por Semana</i> , PULZO (Jan. 14, 2020), https://www.pulzo.com/nacion/como-funciona-software-hombre-invisible-que-uso-ejercito-para-chuzar-PP828082	7
PAUL SIEGHART, PRIVACY AND COMPUTERS (1976)	11
<i>Policía podrá Interceptar Facebook, Twitter y Skype en Colombia</i> , EL TIEMPO (June 22, 2013), https://www.eltiempo.com/archivo/documento/CMS-12890198	6
PRIVACY INTERNATIONAL, DEMAND/SUPPLY: EXPOSING THE SURVEILLANCE INDUSTRY IN COLOMBIA (2015), https://privacyinternational.org/sites/default/files/2017-12/DemandSupply_English.pdf	7

PRIVACY INTERNATIONAL, IMSI CATCHERS : PI’S LEGAL ANALYSIS (2020),
<https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis>7

PRIVACY INTERNATIONAL, SHADOW STATE: LAW AND ORDER IN COLOMBIA (2015),
https://privacyinternational.org/sites/default/files/2017-12/ShadowState_English.pdf.5, 6, 7

PRIVACY INTERNATIONAL, THE RIGHT TO PRIVACY IN COLOMBIA (2016),
https://privacyinternational.org/sites/default/files/2017-12/HRC_colombia.pdf35

PRIVACY INTERNATIONAL, THE STATE OF PRIVACY IN COLOMBIA (2019),
<https://privacyinternational.org/state-privacy/58/state-privacy-colombia>.....43

Rodrigo Silva Vargas, ‘*Ventilador de la parapolítica*’ involucra a Luis Camilo Osorio,
 CARACOL RADIO (Nov. 2, 2007),
https://caracol.com.co/radio/2007/11/02/nacional/1193982780_501669.html5

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) ...8

The Global Principles on National Security. and the Right to Information (The Tshwane Principles), OPEN SOCIETY JUSTICE INITIATIVE (2013),
<https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles>.....27, 30

Vivian Newman Pont, *Legal Interceptions: More Questions Than Answers* DEJUSTICIA (Nov. 26, 2012), <https://www.dejusticia.org/en/legal-interceptions-more-questions-than-answers/>.5

Yomna N, *Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks*, EFF (June 28, 2019), <https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks>.7

II. INTEREST OF AMICI CURIAE

ARTICLE 19 is a global human rights organization, with its international office in London (registered UK charity No. 32741) and several regional offices, including ARTICLE 19 Mexico and Central America and ARTICLE 19 Brazil and South America. The organization takes its name and mandate from Article 19 of the Universal Declaration of Human Rights, which guarantees the right to freedom of opinion and expression and campaigns against censorship in all its forms around the world. Over the years, ARTICLE 19 has produced a number of standard-setting documents and policy briefs based on international and comparative law and best practice on freedom of expression issues, including those related to freedom of expression and surveillance. ARTICLE 19 frequently submits written comments and amicus curiae in cases that raise issues touching on the international guarantee of freedom of expression before regional courts—such as the Inter-American Court of Human Rights, the European Court of Human Rights, and the African Court on Human and Peoples’ Rights—as well as courts in national jurisdictions.

The Electronic Frontier Foundation (EFF) is an international non-profit civil society organization defending freedom of expression, privacy, and innovation in the digital world. EFF champions users’ human rights in the digital realm through impact litigation, policy analysis, grassroots activism, and technology development. EFF’s substantial interest in this case derives from its longstanding work countering arbitrary or abusive surveillance and urging the application of international human rights standards to government access to communications data. EFF was at the forefront of the global coalition that devised the *International Principles on the Application of Human Rights to Communications Surveillance* in 2014. These principles have been cited in numerous documents, including reports by the Special Rapporteurs on Freedom of Expression from the United Nations and the Inter-American Commission on Human Rights. EFF has also worked with partner organizations across Latin America to improve Internet Service Providers’ practices to better protect privacy and foster transparency on government access to user data.

Fundación Karisma is a Colombian non-profit dedicated to ensuring the protection and promotion of human rights and social justice in relation to the design and use of digital technologies. Karisma works on four programmatic lines: 1) democratisation of knowledge and culture, 2) civic participation, 3) autonomy and dignity, 4) social inclusion. Additionally Karisma has two special labs: The digital security and privacy KLAB and the K-Apropiación that works with communities on technology challenges.

Privacy International (PI) is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples’ personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for

Economic Cooperation and Development, the U.N. Office of the High Commissioner for Human Rights and the U.N. Refugee Agency.

III. SUMMARY OF ARGUMENT

Amici submit this brief for the Honorable Inter-American Court of Human Rights (“Inter-American Court” or “Court”) to examine how, despite intelligence-related legal reforms enacted since 2013, Colombian authorities have systematically and unlawfully intercepted communications of members of the *Corporación Colectivo de Abogados José Alvear Restrepo* (CCAJAR). In this brief, *amici* demonstrate that unlawful communications surveillance by state intelligence agencies violates a constellation of human rights, undermining the cornerstones of democratic societies. *Amici* affirm that Colombian intelligence agents carried out unlawful communications surveillance of CCAJAR members under a legal framework that failed to meet international human rights standards.

Colombia has built an expansive and invasive communications surveillance system and used it to target human rights defenders (HRDs) with the aim of deterring or disrupting their human rights work. Intelligence agencies used communications surveillance to gather personal information about CCAJAR members and their families in violation of the right to privacy and other human rights. In the digital age, the right to privacy has become a necessary precondition for the protection of other rights, including the rights to life and personal integrity as well as the freedoms of association, expression, and movement. In this case, unlawful state surveillance practices also infringed on the rights of the children of CCAJAR members.

Colombia enacted Intelligence Law 1621 in 2013 (“2013 Intelligence Law” or “Intelligence Law”) in response to media revelations that Colombia’s intelligence agencies systematically and unlawfully targeted HRDs and journalists, including members of CCAJAR. Colombia argues before this Court that the Intelligence Law “clearly and precisely establishes the specific circumstances in which [intelligence activities] can be authorized to guarantee that any action conforms to the principles of legality, proportionality and necessity” and “provides safeguards at various levels”¹ Contrary to the State’s assertions, since passage of the Intelligence Law, intelligence agencies have systematically and unlawfully surveilled, harassed, and attacked CCAJAR in violation of their rights and with corrosive consequence for the rights of the individuals and communities they defend. This Court must assess these intelligence activities and the applicable legal framework by looking to the standards of legality, legitimacy, necessity and proportionality as well as procedural safeguards required by the American Convention on Human Rights (“American Convention”).

As states increasingly access technological innovations to monitor individuals’ lives in highly intrusiveways, this case presents an unprecedented opportunity for this Court to examine the compatibility of Colombia’s intelligence practices and legal regime with the American Convention and clarify legal protections for human rights defenders against state surveillance. By clarifying the application of Inter-American standards to communications surveillance now common in the region, this Court will provide redress and protect CCAJAR and other HRDs

¹ Inter-Am. Ct. H.R., Public Hearing in Case Members of José Alvear Restrepo Lawyers’ Collective v. Colombia Part 2, 8:32:28-8:32:49, YOUTUBE (May 13, 2022), <https://youtu.be/8Fiv0Hcl86o>.

from future violations and strengthen protections for individuals and organizations targeted by the State for their legitimate defense of human rights.

IV. ARGUMENT

A. TO THE DETRIMENT OF DEMOCRATIC SOCIETIES, UNLAWFUL AND ARBITRARY STATE SURVEILLANCE VIOLATES A CONSTELLATION OF HUMAN RIGHTS PROTECTED BY THE AMERICAN CONVENTION.

Intelligence agencies gather, analyse, monitor, evaluate, and act on information, often in a covert manner, obtained from domestic and foreign individuals and organizations for national security and other purposes.² Colombian intelligence agencies have unlawfully surveilled political candidates, judges, prosecutors, journalists, and human rights defenders (HRDs) under the banner of national security.³ This brief examines Colombian intelligence agencies' use of domestic, secret surveillance to arbitrarily gather information of these groups in violation of international and domestic law.

In 2013, a Colombian court concluded that Colombia's primary intelligence agency, the Administrative Department of Security (in Spanish, Departamento Administrativo de Seguridad (DAS)):

constituted a real criminal enterprise established to orchestrate the commission of unspecified crimes, which later resulted in the illegal interception of communications, the ongoing use of transmitting and receiving equipment, and the arbitrary and unjust abuse of authority for the end purpose of obtaining, processing, and analyzing private information obtained from NGOs, the attorneys of human rights defenders, lawyers' associations, journalists, and ultimately anyone with leanings or ideologies that clashed with or opposed those of the government in power⁴

Numerous international bodies and experts, including this Court, have directly linked intelligence operations conducted by Colombian intelligence agencies to acts of intimidation and violence committed by state and non-state actors.⁵ Colombia has earned the distinction of being

² Martin Scheinin (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism), *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism: Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, Including on Their Oversight*, Practice 2, U.N. Doc. A/HRC/14/46 (May 17, 2010) [hereinafter U.N. SRCTHR Report of 2010].

³ See, e.g., Merits Report No. 57/19 at ¶ 159, *Corporación Colectivo de Abogados "José Alvear Restrepo" v. Colombia*, Case 12.380 OEA/Ser.L/V/II.172 Doc. 66.

⁴ Inter-Am. Comm'n H.R., *Truth, Justice and Reparation: Fourth Report on Human Rights Situation in Colombia*, ¶ 959, OEA/Ser.L/V/II. Doc. 49/13 (Dec. 31, 2013) [hereinafter Inter-Am. Comm'n on H.R., *Truth, Justice and Reparation*] (citing decision by Third Criminal of Court of the Specialized Circuit of Decongestion in Bogotá).

⁵ David Kaye, et al. (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression et al.), *Communication sent to Colombia by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Special Rapporteur on the Situation of Human Rights Defenders, Special Rapporteur on the Promotion of Truth, Justice, Reparation and Guarantees of Non-repetition, and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights of the Organization of American States*, COL 5/20 (June 15, 2020) (expressing concern about military intelligence activities, including surveillance and targeting of human rights defenders); Merits Report No. 57/19, *supra* note 3, at ¶ 296

one of the world's most dangerous countries for human rights defenders.⁶ In 2018, for example, 40% of the world's murders of HRDs occurred in Colombia.⁷ Illegal surveillance has placed HRDs in the crosshairs, exacerbating their risk of violence.

Since at least 1999, Colombia has used its pervasive surveillance network to monitor CCAJAR members and their families and compile information about every facet of CCAJAR members' professional and personal lives, including their professional and personal movements and activities, finances, travel, contacts, clients, and protection schemes. The surveillance of CCAJAR members and their families' communications undoubtedly violated their rights to privacy, life, personal integrity as well as freedoms of association, expression, movement, and the rights of the child.

The surveillance practices against CCAJAR members and their families, and the human rights violations associated with them, have intensified in degree and scale as a result of the use of advanced surveillance technology.

1. Colombia has built a pervasive communications surveillance system with expansive technical capabilities.

Over the course of the country's six-decade war, Colombia has built a formidable intelligence apparatus with massive surveillance capabilities. In 2011, the National Directorate of Intelligence (in Spanish, *Dirección Nacional de Inteligencia* (DNI)) took the place of the DAS as Colombia's main intelligence agency, after revelations that DAS intelligence agents had systematically spied on critics and political opponents and conspired with right-wing paramilitary forces to kill HRDs. In addition to the DNI, intelligence units exist within the National Army, Navy, Air Force, Police, the General Command of the Armed Forces, and the Financial Information and Analysis Unit. These intelligence agencies are under intense pressure to produce intelligence and in constant competition for resources and surveillance tools.⁸

(highlighting that “intelligence activities had illegitimate ends that contravened the [American Convention on Human Rights] and included delivery of information collected about [CCAJAR] members to paramilitary groups.”); Hum. Rts. Comm., *Concluding observations on the Sixth Periodic Report of Colombia*, ¶ 16, U.N. Doc. CCPR/C/COL/CO/6 (Aug. 4, 2010) [hereinafter *HRC Concluding Obs. on Colombia (2010)*] (observing the involvement of intelligence agents in threats and surveillance of judges and recommending that Colombia “create robust controls and oversight systems for its intelligence service and establish a national mechanism to purge intelligence files, in consultation with victims and relevant organizations”); Manuel Cepeda Vargas v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 213, ¶ 216 (May 26, 2010) (ordering Colombia to investigate those responsible for the extrajudicial killing of the victim, including the alleged participation of intelligence agents); U.N. High Comm’r for Hum. Rts., *Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in Colombia*, ¶¶ 14-15, U.N. Doc. A/HRC/13/72 (Mar. 4, 2010) (observing that unlawful intelligence activities targeting human rights defenders “included wiretapping of phones and Internet lines, surveillance, harassment and threats, theft of information and break-ins into offices and homes”); Comm. Against Torture, *Concluding Observations on the Fourth Periodic Report of Colombia*, ¶ 15, U.N. Doc. CAT/C/COL/CO/4 (May 4, 2010) (urging Colombia to “take immediate steps to discontinue the harassment and surveillance of judges by intelligence agents”).

⁶ Michel Forst (Special Rapporteur on the Situation of Human Rights Defenders), *Visit to Colombia: Report of the Special Rapporteur on the Situation of Human Rights Defenders*, ¶ 20, U.N. Doc. A/HRC/43/51/Add.1 (Dec. 26, 2019). Since Colombia signed the peace accords with FARC-EP in 2016, violence against HRDs has “increased steadily.” Inter-Am. Comm’n H.R., *Human Rights Defenders and Social Leaders in Colombia*, ¶ 42, OEA/Ser.L/V/II 29 (2019) [hereinafter *HRDs in Colombia*].

⁷ FRONT LINE DEFENDERS, FRONTLINE DEFENDERS GLOBAL ANALYSIS 4 (2018), <https://www.frontlinedefenders.org/en/resource-publication/global-analysis-2018>.

⁸ PRIVACY INTERNATIONAL, SHADOW STATE: LAW AND ORDER IN COLOMBIA 7, 39 (2015), https://privacyinternational.org/sites/default/files/2017-12/ShadowState_English.pdf [hereinafter SHADOW STATE].

Intelligence agencies engage in a range of communications surveillance practices.⁹ As described in greater detail below in section B(1)(b), while international law permits targeted surveillance in limited circumstances and with strict safeguards, mass surveillance is an inherently disproportionate interference with the international human right to privacy. But in the last few years, law enforcement and intelligence services in Colombia have purchased tools to expand their pervasive spying network and capture large amounts of communications data.¹⁰ This section describes the technological capabilities Colombia has developed to unlawfully and arbitrarily search, collect, and retain massive amounts of personal information about private individuals, including CCAJAR members and their families.

Colombia employs both targeted and mass surveillance tools. Colombian authorities collect, monitor, and intercept, in real-time, individual audio and data communications from mobile and landline phones. Established in 2000, the system, known as “Project Esperanza,” is administered by the Attorney General’s Office. Interceptions carried out through this system must be requested in writing by an analyst, authorized by the Attorney General’s Office, and previously authorized or reviewed by a judge within 36 hours.¹¹ However, there is evidence that the DAS used Project Esperanza technology to intercept phone data without prior authorization or judicial oversight and shared information acquired through the Project Esperanza system with paramilitary groups.¹²

Although Colombian authorities had claimed that the Project Esperanza system was the only method used by law enforcement to intercept communications, in 2015 it was revealed that the Police Intelligence Directorate (in Spanish, *Dirección de Inteligencia Policial*, “DIPOL”) had direct access to communication networks or systems. Through the Integrated Recording System (‘IRS’) (in Spanish, *Sistema Integrado de Grabación Digital* (SIGD)), the police had the capacity to intercept communications signals, including internet and phone communication signals that travel “via network probes connected to a monitoring centre platform, called the [IRS].”¹³ The IRS “was conceived to go beyond the interception of preassigned targets (blancos preasignados) to collect ‘massive’ communications traffic across 16 trunk lines and generate new targets.”¹⁴ The data is processed by monitoring centers with “powerful computers that display connections between people, their conversations and events, and build profiles of individuals and

⁹ Frank La Rue (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 6(a), U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) [hereinafter U.N. SRFOE Report of 2013].

¹⁰ Communications data includes “information about an individual’s communications (e-mails, phone calls and text messages sent and received, social networking messages and posts), identity, network accounts, addresses, websites visited, books and other materials read, watched or listened to, searches conducted, resources used, interactions (origins and destinations of communications, people interacted with, friends, family, acquaintances), and times and locations of an individual, including proximity to others.” *Id.* at ¶ 6(b).

¹¹ SHADOW STATE, *supra* note 8, at 23. See also Vivian Newman Pont, *Legal Interceptions: More Questions Than Answers*, DEJUSTICIA (Nov. 26, 2012), <https://www.dejusticia.org/en/legal-interceptions-more-questions-than-answers/>.

¹² See, e.g., Rodrigo Silva Vargas, ‘Ventilador de la parapolítica’ involucra a Luis Camilo Osorio, CARACOL RADIO (Nov. 2, 2007), https://caracol.com.co/radio/2007/11/02/nacional/1193982780_501669.html (quoting testimony by the former director of information for the DAS before Colombia’s Congress “La información del proyecto Esperanza fue enviada por Jorge Noguera [the former director of the DAS], por mi intermedio, a miembros de las Autodefensas” (“The information from the Esperanza project was sent by Jorge Noguera [the former director of the DAS], through me, to members of the Self-Defense Forces”).

¹³ SHADOW STATE, *supra* note 8, at 15.

¹⁴ *Id.* at 37.

their contacts.”¹⁵ Police have abused the system by surveilling the communications of journalists investigating police corruption and sexual misconduct, for example.¹⁶

Colombia’s security forces and intelligence agencies also have direct access to “mass internet traffic surveillance capacities.”¹⁷ Launched in 2007 and upgraded in 2014, the *Plataforma Única de Monitoreo y Análisis* (PUMA) is a “a phone and internet monitoring system linked directly to the service providers’ network infrastructure by a probe that copies vast amounts of data and sends it directly to [a] monitoring facility.”¹⁸ Through PUMA, state agencies can intercept and retain “all communications transmitted on the high-volume cables that make up the backbone on which all Colombians rely to speak to and message each other.”¹⁹ PUMA enables the intelligence services to directly intercept “what is spoken, written or sent from e-mails, Facebook, Twitter, Line, Viber, Skype, and, in short, any type of communication undertaken via the internet.”²⁰ PUMA not only has the capacity to capture users’ communications traffic but “to appropriate the target’s device, control it and find everything that is there or in the surroundings.”²¹ In 2015, a group monitoring communications surveillance in Colombia observed that “PUMA is poised to become the most powerful and sophisticated . . . mass communications monitoring system in Colombia.”²²

Colombian intelligence services also have conducted intrusion operations which exploit software, data, computer systems, or networks to gain unauthorized access to user information and devices. These targeted strategies rely on deployments of malware, spyware, and monitoring devices to collect information about specific individuals.²³ For example, intelligence services have used technology, also referred to as Trojans, to infect “a target’s device” and “capture data on a target’s device, remotely switch on and off webcams and microphones, copy files and typed passwords.”²⁴ In 2020, news reports revealed that the Colombian military had used malware

¹⁵ *Id.* at 15.

¹⁶ Adriaan Alsema, *Colombia Police ‘Wiretapping, Shadowing and Intimidating Journalists’*, COLOMBIA REPORTS (Dec. 3, 2015), <https://colombiareports.com/colombias-police-wiretapping-and-intimidating-journalists/>.

¹⁷ SHADOW STATE, *supra* note 8, at 14. According to this report, “Esperanza allows the Fiscalía to connect to telecommunications providers’ servers, to receive and package real-time call information to transmit into a central monitoring room. The signal is then dispatched to other monitoring rooms controlled by the Fiscalía’s Technical Investigations Unit (Cuerpo Técnico de Investigación, ‘CTI’), the Police and DAS, when it was functional.” *Id.* at 21. *See also* *Dónde Estan Mis Datos?*, FUNDACIÓN KARISMA 11 (2021), <https://web.karisma.org.co/donde-estan-mis-datos-2021/> (stating that Colombian authorities use technology to access telecommunications users’ data through an open door to companies’ telecommunications infrastructure); *id.* at 21-22 (observing that telecommunication companies report that the Attorney General’s Office had direct access to mobile phone users’ data).

¹⁸ FUNDACIÓN KARISMA, FUNDACIÓN KARISMA’S RESPONSE TO CALL FOR INPUT TO A REPORT ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE BY THE U.N. HIGH COMMISSIONER FOR HUMAN RIGHTS 4 (2018), <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Karisma.pdf>.

¹⁹ SHADOW STATE, *supra* note 8, at 27.

²⁰ *Policía podrá Interceptar Facebook, Twitter y Skype en Colombia*, EL TIEMPO (June 22, 2013), <https://www.eltiempo.com/archivo/documento/CMS-12890198>.

²¹ *In Colombia, PUMA Is Not What It Seems*, DIGITAL RIGHTS LAC (2015), <https://digitalrightslac.derechosdigitales.org/en/en-colombia-el-puma-no-es-como-lo-pintan/>.

²² SHADOW STATE, *supra* note 8, at 31.

²³ There is evidence that Colombia’s military intelligence has purchased various intelligence tools. According to the magazine *Semana*, a forensic report submitted to Colombia’s Supreme Court described “various computer tools that were found in the raid” of the military’s cyberintelligence unit, including malware and intrusion tools. *El Informe Forense de las Carpetas Secretas*, SEMANA (May 12, 2020), <https://www.semana.com/nacion/articulo/el-informe-forense-de-las-carpetas-secretas/670853/>.

²⁴ SHADOW STATE, *supra* note 8, at 43. *See also* U.N. SRFOE Report of 2013, *supra* note 9, at ¶ 62.

called “Invisible Man” (in Spanish, “Hombre Invisible”) to spy on government officials and HRDs.²⁵

Colombian intelligence operations have also used mobile monitoring devices (“Cell Site Simulators,” also known as “IMSI catchers”) “that allow for localised indiscriminate interception of all mobile phone calls and text messages in a specific location.”²⁶ Commonly known as “stingrays,” these devices “transmit a strong wireless signal that entices nearby phones to connect to it and transmit communications data and content”²⁷

Although a lack of state transparency and accountability makes it impossible to know precisely the types of surveillance practices that intelligence agencies conducted, what technologies they used, and the identity of all their targets, it is undeniable that illegal surveillance of CCAJAR did not disappear with the DAS. Since 2013, CCAJAR members have encountered tell-tale signs of surveillance when they spoke on the phone, used their computers, or were in public. Reports by Colombian authorities and media confirmed that intelligence agencies continue to target CCAJAR members. On December 18, 2019, the Investigation Chamber of the Supreme Court of Justice and judicial police from the Special Investigations Directorate of the Attorney General’s Office raided the military’s cyberintelligence unit.²⁸ Although military officers attempted to impede their inspection and destroy or conceal evidence,²⁹ judicial authorities seized computer software and surveillance tools allegedly used by military intelligence units to conduct illegal surveillance.³⁰ In the months that followed, media published evidence that several military intelligence units had conducted illegal surveillance to create profiles of journalists, social leaders, opposition politicians, judges, and HRDs, including CCAJAR members.³¹ According to the Inter-American Special Rapporteur on Freedom of Expression (“I-A SR on FOE”), “surveillance tasks included the illegal interception of communications, and monitoring through ‘StingRay’ [and malware].”³² These revelations led to the resignation of Army Commander General Nicasio Martínez and other high-ranking officials

²⁵ *Lo que quería el Ejército con ‘Hombre invisible’ que hizo chuzadas reveladas por Semana*, PULZO (Jan. 14, 2020), <https://www.pulzo.com/nacion/como-funciona-software-hombre-invisible-que-uso-ejercito-para-chuzar-PP828082>. According to one official who participated in the illegal interceptions, “the ‘Invisible Man’ allowed him to get into ‘any computer, access to WhatsApp and Telegram Web, download archived and deleted chat conversations, photos and, in general, what was stored in the memory of the infected machine,’” without leaving a trace. *Id.*

²⁶ SHADOW STATE, *supra* note 8, at 15. For more information about the capability of Cell Site Simulators, see Yomna N, *Gotta Catch ‘Em All: Understanding How IMSI-Catchers Exploit Cell Networks*, ELECTRONIC FRONTIER FOUNDATION (June 28, 2019), <https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks>; PRIVACY INTERNATIONAL, *IMSI CATCHERS : PI’S LEGAL ANALYSIS* (2020), <https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis>

²⁷ PRIVACY INTERNATIONAL, *DEMAND/SUPPLY: EXPOSING THE SURVEILLANCE INDUSTRY IN COLOMBIA* 36 (2015), https://privacyinternational.org/sites/default/files/2017-12/DemandSupply_English.pdf.

²⁸ Pedro Vaca Villareal (Special Rapporteur for Freedom of Expression), *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*, ¶ 407, OEA/Ser.L/V/II Doc. 28 (Mar. 30, 2021) <http://www.oas.org/en/iachr/docs/annual/2020/Chapters/rele-en.PDF> [hereinafter I-A SRFOE Report of 2021].

²⁹ “¡Tapen, tapen, tapen!”: así fue el allanamiento de la Corte Suprema a una instalación del Ejército, SEMANA (Jan. 13, 2020), <https://www.semana.com/nacion/multimedia/nuevas-chuzadas-del-ejercito-en-colombia/647868/>.

³⁰ I-A SRFOE Report of 2021, *supra* note 28, at ¶ 408 (quoting from a report by the Colombia’ Attorney General’s Office regarding the raid which states that the military intelligence “has the ability to access email accounts” and “intervene in communications”).

³¹ *Las Carpetas Secretas*, SEMANA (May 5, 2020), <https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/>; *Chuzadas sin Cuartel*, SEMANA (Jan. 1, 2020), <https://www.semana.com/nacion/articulo/chuzadas-por-que-se-retiro-el-general-nicacio-martinez-del-ejercito/647810/>.

³² I-A SRFOE Report of 2021, *supra* note 28, at ¶ 405.

and prompted President Iván Duque to order the Defense Minister “to carry out a rigorous investigation of the intelligence work of the last 10 years”³³ The I-A SR on FOE has expressed concern that these criminal investigations “have not progressed significantly.”³⁴

2. Colombia’s communications surveillance system has far-reaching implications for a constellation of human rights protected by the American Convention.

The legal notion of the right to privacy first emerged in response to the technological innovations of the 19th century, including the invention of photography and the advent of mass media.³⁵ In 2013, the impact of state surveillance technologies on privacy and other human rights came into full view with the revelations of Edward Snowden concerning the widespread and global surveillance practices carried out by governments. Since Snowden’s revelations, domestic laws have not kept pace with constantly developing technologies that offer states “the ability to closely profile and monitor the behaviour of individuals in new ways and to an unprecedented extent.”³⁶ As “large amounts of transactional data by and about individuals”³⁷ has become available, states “have expanded their powers to conduct surveillance, lowering the threshold and increasing the justifications for such surveillance.”³⁸ International and regional human rights bodies have observed that current domestic legal frameworks provide individuals with “only limited protection against excessive surveillance.”³⁹

Intelligence activities have enormous implications for a range of rights. In the digital age, the right to privacy has become “a necessary precondition for the protection of fundamental values, including liberty, dignity, equality and freedom from government intrusion,” “an essential ingredient for democratic societies,”⁴⁰ and the gateway to the protection of other rights.⁴¹ Accordingly, this Court should assess the impact of state surveillance of CCAJAR members and their families on their right to privacy as well as the realization of other human

³³ *Id.* at ¶ 409.

³⁴ *Id.* at ¶ 410.

³⁵ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195

(1890) (one of the first articulations of the legal right to privacy stating “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-top.’”)

³⁶ Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Report of the Special Rapporteur on the Right to Privacy*, ¶ 33, U.N. Doc. A/HRC/40/63 (Oct. 16, 2019) [hereinafter U.N. SRRP Report of 2019].

³⁷ U.N. SRFOE Report of 2013, *supra* note 9, at ¶15.

³⁸ *Id.* at ¶ 16.

³⁹ Hum. Rts. Comm., *Concluding Observations on the Fourth Periodic Report of the United States of America*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014) [hereinafter *HRC Concluding Obs. on the U.S.*] (expressing concern about the collection of bulk communications metadata by state intelligence agencies, the secrecy of oversight systems, and the lack of access to effective remedies by affected persons). *See also* Roman Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R. (Dec. 4, 2015), <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22002-10793%22%5D%7D>; Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Report of the United Nations Special Rapporteur on the Right to Privacy*, ¶ 15, U.N. Doc. A/HRC/34/60 (Sept. 6, 2017) [hereinafter U.N. SRRP Report of 2017] (remarking that after the Snowden revelations states have “pass[ed] new laws on [government surveillance] that contain only minor improvements in limited areas, if any at all. In general, those laws have been drafted and rushed through the legislative process to legitimize practices that should never have been implemented”).

⁴⁰ U.N. SRRP Report of 2019, *supra* note 36, at ¶ 51.

⁴¹ *See* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 16, U.N. Doc. A/HRC/29/32 (May 22, 2015) [hereinafter U.N. SRFOE Report of 2015].

rights enshrined by the American Convention, including the rights to life, personal integrity, access to information, and the freedoms of expression, association, and movement.

In assessing interference with these rights, this Court should also consider that the aim of the communication surveillance undertaken by Colombia was not to protect national security or public order but to deter and disrupt human rights work. The right to defend human rights is protected by various international instruments and principles.⁴² This Court has affirmed the importance of human rights work as “fundamental for the strengthening of democracy and the rule of law,”⁴³ and held that States must take certain actions to protect human rights defense work, including to “facilitate the means for human rights defenders to carry out their activities freely, to protect them when they are threatened [and] abstain from imposing obstacles that obstruct their work”⁴⁴ Colombia has disregarded these duties and used communications surveillance to attack, threaten, discredit, intimidate, and silence human rights defenders.

a. Communications surveillance interferes with the right to privacy.

The right to privacy is a fundamental, universal right protected by international and domestic laws.⁴⁵ The International Covenant on Civil and Political Rights (ICCPR) was the first international treaty to codify the right to privacy in international human rights law, requiring state parties to refrain from subjecting individuals to “arbitrary or unlawful interference” with their “privacy, family, home or correspondence,” or “unlawful attacks on [their] honor and reputation.”⁴⁶ Other international human rights treaties contain similar language to protect the privacy of children,⁴⁷ migrant workers,⁴⁸ and persons with disabilities.⁴⁹ Regional treaties similarly prohibit arbitrary and abusive interference with “private life,” family, home, or correspondence.⁵⁰

In the digital age, human rights bodies have interpreted the right to privacy to extend to informational privacy, “covering information that exists or can be derived about a person and her

⁴² See, e.g., G.A. Res. 53/144, Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms (Mar. 8, 1999); G.A. Res. 1671 (XXIX-O/99), Human Rights Defenders in the Americas, Support for the Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas (June 7, 1999); G.A. Res. 2517 (XXXIX-O/09), Human Rights Defenders: Support for the Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas (June 4, 2009).

⁴³ Valle Jaramillo et al. v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 192, ¶ 87 (Nov. 27, 2008).

⁴⁴ Escher et al. v. Brazil, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 200, ¶ 172 (Jul. 6, 2009).

⁴⁵ U.N. High Comm’r for Hum. Rts., *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, ¶¶ 12-13, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter OHCHR Report of 2014].

⁴⁶ International Covenant on Civil and Political Rights art. 17, *opened for signature* Dec. 16, 1966, 999 U.N.T.S.171. See also G.A. Res 217A (III) art. 12, Universal Declaration of Human Rights (Dec. 10, 1948)

⁴⁷ Convention on the Rights of the Child art. 16, *opened for signature* Nov. 20, 1989, 1577 U.N.T.S. 3.

⁴⁸ International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families art. 14, *opened for signature* Dec. 18, 1990, 2220 U.N.T.S. 3.

⁴⁹ Convention on the Rights of Persons with Disabilities annex 1, art. 22, *opened for signature* Dec. 13, 2005, 2515 U.N.T.S. 3.

⁵⁰ Organization of American States, American Convention on Human Rights art. 11, *opened for signature* Nov. 22, 1969, O.A.S.T.S. No. 36; 1144 U.N.T.S. 123 [hereinafter American Convention on Human Rights]. The European Convention for the Protection of Human Rights and Fundamental Freedoms specifies that state interference with the right to privacy must be authorized by law and “necessary in a democratic society.” ETS 5, art. 8 (1953) [hereinafter European Convention].

or his life and the decisions based on that information . . . ”⁵¹ The protection of informational privacy requires that the private sphere, where individuals presumptively “should have an area of autonomous development, interaction and liberty,”⁵² includes not only “private, secluded spaces, such as the home of a person, but extends to public spaces and information that is publicly available.”⁵³ Accordingly, privacy protections extend to not only the “substantive information contained in communications,” but also the metadata which may provide “an insight into an individual’s behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication.”⁵⁴

Under the American Convention, the right to privacy is a qualified right that may be restricted but only in “a very carefully delimited way.”⁵⁵ Interferences with the right to privacy are permissible only if they are neither unlawful nor arbitrary.⁵⁶ In *Escher v. Brazil*, the Inter-American Court recognized the “inherent danger of abuse” of a surveillance system.⁵⁷ The mere existence of secret surveillance, according to international experts, constitutes an intrusion on the right to privacy⁵⁸ and an intensifying threat for meaningful personal autonomy.⁵⁹

While modern technologies have made it much easier for states “to find out how we act” and “reduce our freedom to act as we please,”⁶⁰ states have failed to adopt “detailed rules, practical procedures and appropriate oversight mechanisms to ensure an independent, reliable and efficient control of surveillance, both nationally and globally.”⁶¹ This ineffective regulatory environment has drawn the attention of the international community. Since 2014, the U.N. Human Rights Committee (HRC) has raised concerns about arbitrary or unlawful privacy limitation in nearly all of its concluding observations or assessments of national efforts to

⁵¹ U.N. High Comm’r for Hum. Rts., *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, ¶ 5, U.N. Doc. A/HRC/39/29 (Aug. 3, 2018) [hereinafter OHCHR Report of 2018]. See also U.N. SRFOE Report of 2013, *supra* note 9, at ¶ 81 (stating that “[t]he interception and retention of data on private communications infringes upon the right to privacy.”).

⁵² OHCHR Report of 2018, *supra* note 51, at ¶ 5.

⁵³ *Id.* at ¶ 6 (citing to Hum. Rts. Comm., *Concluding Observations on the Seventh Periodic Report of Colombia*, ¶ 32, U.N. Doc. CCCPR/C/COL/CO/7 (Nov. 17, 2016) [hereinafter *HRC Concluding Obs. Colombia (2016)*]).

⁵⁴ OHCHR Report of 2018, *supra* note 51, at ¶ 6 (quoting OHCHR Report of 2014, *supra* note 45, at ¶ 19). See *Escher*, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 144 (establishing that privacy protections extend to “any element of the communication process for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls”); Edison Lanza (Special Rapporteur for Freedom of Expression), *Standards for a Free, Open and Inclusive Internet*, ¶ 189, OEA/Ser.L/V/II CIDH/RELE/INF.17/17 (Mar. 15, 2017) [hereinafter *I-A SRFOE Internet Standards*] (explaining that metadata, “like the information on telephone communications protected by the case law of the inter-American system, . . . is separate from the content yet still highly revelatory of personal relationships, habits and customs, preferences, lifestyles, etc.”); *id.* at ¶ 21 (stating that the “standards developed in both the Inter-American and the European system aim at protecting not only the content of communications but also the data about the communications, or the metadata in the case of the Internet . . .”).

⁵⁵ U.N. SRRP Report of 2019, *supra* note 36, at ¶ 11.

⁵⁶ *Id.*

⁵⁷ *Escher*, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 118. See also Hum. Rts. Comm., *General Comment No. 16: Article 17 (Right to Privacy)*, in *Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies*, ¶¶ 3-4, U.N. Doc. HRI/GEN/Rev.9 (Apr. 8, 1988).

⁵⁸ OHCHR Report of 2018, *supra* note 51, at ¶ 7 (citing Roman Zakharov, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39).

⁵⁹ U.N. SRRP Report of 2019, *supra* note 36, at ¶ 10 (stating that “[i]nfringement of privacy is often part of a system which threatens other liberties. It is often carried out by State actors to secure and retain power, but also by non-State actors, such as individuals or corporations wishing to continue to control others.”).

⁶⁰ *Id.* at ¶ 8 (quoting from PAUL SIEGHART, *PRIVACY AND COMPUTERS* 24 (1976)).

⁶¹ Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Report of the United Nations Special Rapporteur on the Right to Privacy*, ¶ 53, U.N. Doc. A/HRC/37/62 (Oct. 25, 2018) [hereinafter U.N. SRRP Report of 2018].

implement legal obligations under the ICCPR.⁶² In its concluding observations regarding Colombia, for example, the HRC urged the State to “[a]dopt effective measures to prevent illegal surveillance activities” and “take the necessary steps to ensure that any interference with a person’s privacy, including interference via the electromagnetic spectrum, is in keeping with the principles of legality, necessity and proportionality.”⁶³

Inter-American case law has made an important contribution to the development of the right to privacy.⁶⁴ However, with the exception of *Escher v. Brazil*, this Court’s judgments have primarily focused on physical intrusions on the right to privacy and therefore has not examined the implications of technological surveillance practices on and the protections of the human rights enshrined under the American Convention in this context. This case provides an opportunity for the Court to develop and clarify standards related to interference with the right to privacy arising from digital communications surveillance.

b. Communications surveillance interferes with the rights to life and personal integrity.

The American Convention enshrines the rights to life and personal integrity.⁶⁵ This Court has also affirmed that a “State has the obligation to adopt all reasonable measures required to guarantee the rights to life, to personal liberty, and to personal integrity” of HRDs.⁶⁶ To this end, the Inter-American Court has established that states have the obligation to ensure HRDs are able to carry out their work freely, to protect HRDs who are threatened and attacked, and to effectively investigate violations against HRDs.⁶⁷

International bodies and experts have recognized that communications surveillance can imperil life and security.⁶⁸ The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (“U.N. SR on FOE”) has observed that “[i]nadequate national frameworks create a fertile ground for arbitrary and unlawful infringements” on human rights by intelligence agencies.⁶⁹ In turn, “surveillance of individuals – often journalists, activists, opposition figures, critics and others exercising their

⁶² See PRIVACY INTERNATIONAL, GUIDE TO INTERNATIONAL LAW AND SURVEILLANCE, AT 272-274 (3RD ED. 2021), <https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance>.

⁶³ See *HRC Concluding Obs. on Colombia (2016)*, *supra* note 53, at ¶ 33. See also *HRC Concluding Obs. on Colombia (2010)*, *supra* note 5, at ¶16-17 (noting reports of illegal surveillance by intelligence agencies and urging Colombia to “create robust controls and oversight systems for its intelligence service . . .”).

⁶⁴ See, e.g., *Escher*, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44; *Kimel v. Argentina*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 177 (May 2, 2008).

⁶⁵ American Convention on Human Rights, *supra* note 50, arts. 4, 5.

⁶⁶ *Valle Jaramillo*, Inter-Am. Ct. H.R. (ser. C) No. 192, *supra* note 43, at ¶ 90.

⁶⁷ *Id.* at ¶ 91 (citing *Matter of the Monagas Detention Center (“La Pica”)*, Provisional Measures, Order, ¶ 14, (Inter-Am. Ct. H.R. Feb. 9, 2006), https://www.corteidh.or.cr/docs/medidas/lapica_se_02_ing.pdf; *Nogueira de Carvalho et al. v. Brazil*, Preliminary Objections and Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 161, ¶ 77 (Nov. 28, 2006); and *Case of the Persons Deprived of Liberty in the “Dr. Sebastião Martins Silveira” Prison in Araraquara, São Paulo*, Provisional Measures, Order, ¶ 24, (Inter-Am. Ct. H.R. Sept. 30, 2006), https://www.corteidh.or.cr/docs/medidas/araraquara_se_02_ing.pdf).

⁶⁸ U.N. SRRP Report of 2018, *supra* note 61, at ¶ 13.

⁶⁹ U.N. SRFOE Report of 2013, *supra* note 9, at ¶ 3.

right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings.”⁷⁰

In this case, the Inter-American Commission on Human Rights (“Inter-American Commission”) and representatives of the victims argue that Colombia’s intelligence agencies used communications surveillance to harass, intimidate, and attack members of CCAJAR and their families.⁷¹ Specifically, in bringing this case before this Court, the Inter-American Commission concluded that intelligence operations “put [CCAJAR] members at greater risk” and generated state responsibility “for the acts of violence, threat, and harassment” against CCAJAR members.⁷²

c. Communications surveillance interferes with the right to freedom of expression and thought.

The Inter-American Court has conferred broad protection to the right to freedom of thought and expression established by Article 13 of the American Convention; not only does it protect the right to express thoughts, but also the right and freedom to seek, receive, and disseminate information.⁷³ Three aspects of the right to freedom of expression are of particular relevance to this case because of the political nature of the expression that was surveilled and Colombia’s efforts to deter and disrupt human rights work through communications surveillance.

First, the importance of freedom of expression is one of the bedrock principles of democracy and human rights.⁷⁴ The U.N. SR on FOE has emphasized the serious implications of communications surveillance for democratic societies, noting that “[c]ommunications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society.”⁷⁵

Second, international bodies and courts have placed a high value on “uninhibited expression”⁷⁶ and raised concerns about the corrosive effect of surveillance on public debate.⁷⁷ Surveillance creates a chilling effect by “instill[ing] fear and inhibition as part of the political

⁷⁰ David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Surveillance and Human Rights*, ¶ 1, U.N. Doc. A/HRC/41/35 (May 28, 2019) [hereinafter U.N. SRFOE Report of 2019].

⁷¹ See generally, Merits Report No. 57/19, *supra* note 3.

⁷² *Id.* at ¶ 296.

⁷³ See *Herrera Ulloa v. Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 107, ¶ 108 (Jul. 2, 2004).

⁷⁴ The European Court has repeatedly affirmed the significance of freedom of expression, stating that the rights is an “one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment.” *Süre v. Turkey* (No. 3), App. Nos. 23927/94 and 24277/94, Eur. Ct. H.R., ¶ 57 (1999), <https://hudoc.echr.coe.int/fre?i=001-58278>.

⁷⁵ U.N. SRFOE Report of 2013, *supra* note 9, at ¶ 81.

⁷⁶ Hum. Rts. Comm., *General Comment No. 34: Article 19: Freedoms of Opinion and Expression*, ¶ 34, U.N. Doc. CCPR/C/GC/34 (Sept. 11, 2011).

⁷⁷ Frank William La Rue, Cataline Botero (Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights), *Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression*, ¶ 5 (June 21, 2013), <https://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&IID=1> [hereinafter *Joint Declaration on Surveillance*].

culture, and it forces individuals to take precautions in communicating with others.”⁷⁸ In chilling free expression, surveillance degrades public debate in a democratic society, especially when concerning figures in the public and political domain.

Digital technologies offer states the unprecedented capacity to conduct invasive, targeted or mass, low-cost surveillance in secrecy, and with unlimited duration.⁷⁹ The U.N. SR on FOE has argued that

Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one’s mind. And yet, today, holding opinions in digital space is under attack.⁸⁰

The U.N. SR on FOE has expressed particular concern over how “[s]urveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.”⁸¹ Similarly, the European Court of Justice of the European Union (CJEU) has noted the effect of data retention by governments “on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression”⁸²

To prevent or mitigate the chilling effect of surveillance, the United Nations Special Rapporteur on the Right to Privacy (“U.N. SR on Privacy”) has stated: “It is crucial that fundamental human rights, particularly privacy, freedom of expression and the right to information, remain at the core of any assessment of governmental surveillance measures of all types and kinds.”⁸³ The U.N. SR on FOE has insisted on national laws that limit state surveillance to the “most exceptional circumstances and exclusively under the supervision of an independent judicial authority.”⁸⁴ Despite growing technological capabilities, states have failed

⁷⁸ Catalina Botero Marino (Special Rapporteur for Freedom of Expression), Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, ¶ 150, OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13 (Dec. 31, 2013) [hereinafter I-A SRFOE Report of 2013].

⁷⁹ U.N. SRFOE Report of 2013, *supra* note 9, at ¶ 33 (stating that “[t]echnological advancements mean that the State’s effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.”).

⁸⁰ U.N. SRFOE Report of 2015, *supra* note 41, at ¶ 20.

⁸¹ *Id.* at ¶ 21.

⁸² Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen, Sec’y of State for the Home Dep’t v. Watson*, ECLI:EU:C:2016:970, ¶ 101, (Dec. 21, 2016) [hereinafter Cases C-203/15 and C-698/15, *Tele2 v. Post-och*]. *See also* *Rotaru v. Romania*, App. No. 28341/91, Eur. Ct. H.R., ¶ 46 (May 4, 2000), <https://hudoc.echr.coe.int/eng?i=001-58586>; David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), *Report on the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, ¶ 56, U.N. Doc. A/HRC/32/38 (May 11, 2016).

⁸³ U.N. SRRP Report of 2017, *supra* note 39, at ¶ 35.

⁸⁴ Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Mission to the former Yugoslav Republic of Macedonia*, ¶ 92, U.N. Doc. A/HRC/26/30/Add.2 (Apr. 1, 2014).

to regulate the use of communications surveillance in a way that complies with their obligations under international and regional human rights law.⁸⁵ States have also failed to ensure democratic controls on the use, acquisition and export of private surveillance tools. These controls and human rights principles are even more relevant in view of the particular force they play in cases of targeted surveillance when expression in the public interest is implicated.⁸⁶

Third, this Court’s recognition that the freedom of expression embodies a public right of access to state-held information should be core to its assessment of the impact of communications surveillance on Article 13 protections.⁸⁷ This Court has held repeatedly that democratic societies are “governed by the principle of maximum disclosure, which establishes the presumption that all information is accessible”⁸⁸ The burden rests on the state to demonstrate that any information withheld fits into Article 13’s “limited system of exceptions.”⁸⁹ The state has a positive obligation to either provide the information requested or provide a response that justifies the restriction. Moreover, this Court has determined that “authorities cannot resort to mechanisms such as official secret or confidentiality of the information, or reasons of public interest or national security, to refuse to supply the information”⁹⁰

d. Communications surveillance interferes with the freedom of association and movement.

Article 16 of the American Convention establishes the “right to associate freely” and prohibits restrictions unless “established by law” and “necessary in a democratic society.” This Court has recognized the “special scope and nature” of the right to association which has both an individual and a social dimension.⁹¹ The individual dimension includes “the right and freedom to associate freely with other persons, without the interference of the public authorities limiting or obstructing the exercise of the respective right,”⁹² while the social dimension “authoriz[es] individuals . . . to act collectively to achieve very diverse purposes, provided they are legitimate.”⁹³

Accordingly, this Court has found that the state may not intervene to limit or obstruct the exercise of the right to association, nor may the state exercise pressure or interfere in the achievement of a common licit goal.⁹⁴ Additionally, this Court has emphasized the important

⁸⁵ I-A SRFOE Report of 2013, *supra* note 78, at ¶¶ 153, 155, 164, 166.

⁸⁶ U.N. SRFOE Report of 2019, *supra* note 70, at ¶ 46.

⁸⁷ Claude Reyes et al. v. Chile, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 151, ¶¶ 84-85 (Sept. 19, 2006). *See also id.* at ¶ 77.

⁸⁸ *Id.* at ¶ 92.

⁸⁹ *Id.*

⁹⁰ Gomes-Lund v. Brazil, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 11.552, ¶ 202 (Nov. 24, 2010). *See also* Corte Suprema de Justicia [C.S.J.] [Supreme Court], septiembre 1, 2020, Sentencia T-374/20, ¶ 4.4 (Colom.), <https://www.corteconstitucional.gov.co/relatoria/2020/T-374-20.htm> (recognizing that victim’s have procedural right in accordance with due process, the effective administration of justice, and the right to truth to access criminal files and actively participate in criminal proceedings).

⁹¹ Huilca Tecse v. Peru, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 121, ¶ 69 (Mar. 3, 2005).

⁹² *Id.*

⁹³ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶169. *See also* Huilca Tecse, Inter-Am. Ct. H.R. (ser. C) No. 121, *supra* note 91, at ¶ 71.

⁹⁴ Cantoral-Huamani and García-Santa Cruz v. Peru, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 167, ¶ 144 (Jul. 10, 2007).

role of human rights defenders in democratic societies to impose a positive obligation on the state to create the legal and factual conditions necessary to ensure that those who expose human rights violations can carry out their activities freely.⁹⁵

The U.N. SR on Privacy has underscored the fundamental relationship between the rights to privacy and association and the health of democratic societies, stating that “[t]he loss of privacy can lead to a loss of . . . confidence in government and institutions established to represent the public interests, and to withdrawal from participation, which can adversely impact and undermine representative democracies.”⁹⁶ This Court has also recognized the corrosive impact of state surveillance on the opportunity for collective action that the American Convention seeks to guarantee. In *Escher v. Brazil*, the Court established that the State had created a climate of fear that impeded “the free and normal exercise of the right to freedom of association” by unlawfully intercepting, monitoring, and disclosing telephone conversation by members of human rights organizations.⁹⁷

Despite the dangerous implications of surveillance for the health of democracies and the protection of human rights defenders and in contravention of international standards, states often enact “overly broad and vague surveillance laws [that] fail to target specific individuals on the basis of a reasonable suspicion.”⁹⁸ In violation of the freedom of association, “States have harnessed technology to monitor and hamper the work of human rights defenders and civil society actors . . . [by] hacking phones and computers, issuing death and rape threats, disseminating doctored images, temporarily suspend[ing] targets’ accounts, hijacking hashtags, spreading conspiracy theories, accusations of treason and promoting virulently discriminatory sentiments.”⁹⁹ The purpose of these tactics, according to the U.N. Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, is “to intimidate civil society actors, destroy their credibility and legitimacy[,] . . . undermine the ability of civil society organizations and activists to share or receive information and communicate with others,” and “create incentives for self-censorship, while threatening individuals’ personal security and integrity.”¹⁰⁰

⁹⁵ Yarce et al. v. Colombia, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 325, ¶ 271 (Nov. 22, 2016). *See also* Valle Jaramillo, Inter-Am. Ct. H.R. (ser. C) No. 192, *supra* note 43, at ¶ 91.

⁹⁶ U.N. SRRP Report of 2019, *supra* note 36, at ¶ 100.

⁹⁷ *Escher*, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶¶ 178-180.

⁹⁸ Maina Kiai (Special Rapporteur on the Rights to Freedom of Peaceful assembly and of Association), *Report of the Special Rapporteur on the Rights to Rreedom of Peaceful Assembly and of Association on His Follow-up Mission to the United Kingdom of Great Britain and Northern Ireland*, ¶ 71, U.N. Doc. A/HRC/35/28/Add.1 (June 8, 2017) (expressing concern about the overly broad definition of “domestic extremism” which had led to “the reported [police] targeting of peaceful protestors as ‘domestic extremist’” and the inclusion of their identifies in intelligence databases). *See also* Clément Nyaletsossi Voule (Special Rapporteur on the Rights to Rreedom of Peaceful Assembly and of Association), *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, ¶ 57, U.N. Doc. A/HRC/41/41 (May 17, 2019) [hereinafter U.N. SRFPA Report of 2019] (stating that “[s]urveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision”); Hum. Rts. Comm., *General Comment No. 37 on the Right of Peaceful Assembly (Article 21)*, ¶ 61, U.N. Doc. CCPR/C/GC/37 (Sept. 17, 2020) (stating that in the context of peaceful assemblies, state surveillance “must not result in suppressing rights or creating a chilling effect” and “must strictly conform to applicable international standards, including on the right to privacy, and may never be aimed at intimidating or harassing participants or would-be participants in assemblies.”).

⁹⁹ U.N. SRFPA Report of 2019, *supra* note 98, at ¶ 43.

¹⁰⁰ *Id.* at ¶ 44.

Moreover, the praxis of human rights requires that HRDs have freedom of movement and the ability to choose their place of work and residence.¹⁰¹ Article 22 of the American Convention establishes “the right of all persons lawfully within a State to move freely within that State and to choose their place of residence; and the right of such persons to enter, to remain in, or to leave the State’s territory without any unlawful interference.”¹⁰² The provision of legal representation, in particular, necessitates a close relationship and communication between lawyers and the victims they represent. The Court has held that “the right to freedom of movement and residence can be violated by de facto restrictions if the State has not established the conditions or provided the means to allow that right to be exercised.”¹⁰³ In this case, CCAJAR members were forced to limit their activities, to change their residences, and into exile due to the acts of violence, threats, and harassment they suffered as a result of state intelligence operations. Persecution imposed restrictions on movement that obstructed the freedom of the CCAJAR members to freely associate with other persons and engage in a collective enterprise of defending human rights.

This case illustrates the insidious effects of surveillance on association and movement. For decades, the cloud of surveillance loomed over every decision of CCAJAR members, limiting their personal autonomy and hindering their human rights activities.

e. Communications surveillance imperils the rights of children.

Article 19 of the American Convention requires that every minor child have the “right to measures of protection required by [their] condition as a minor on the part of [their] family, society, and the state.”¹⁰⁴ This Court has repeatedly held that children “have the same rights as all human beings . . . and also special rights derived from their condition, and these are accompanied by specific duties of the family, society, and the State.”¹⁰⁵ In the view of this Court, Article 19 imposes a special status on the state as guarantor of the rights of the child.¹⁰⁶ Accordingly, the Court has interpreted Article 19 to impose a state obligation to take all necessary measures to ensure the effective exercise of the rights of the child, removing any obstacles, and taking into account the particular circumstances and challenges children face in the enjoyment of their rights.¹⁰⁷ Moreover, this Court has applied a higher standard in assessing state conduct that violates physical, mental, or moral integrity because children require special protection given their state of development.¹⁰⁸

¹⁰¹ Inter-Am. Comm’n H.R., *Report on Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II.124 Doc. 5 rev.1 ¶ 101 (2006).

¹⁰² Merits Report No. 57/19, *supra* note 3, at ¶ 329.

¹⁰³ Valle Jaramillo, Inter-Am. Ct. H.R. (ser. C) No. 192, *supra* note 43, at ¶ 139.

¹⁰⁴ American Convention on Human Rights, *supra* note 50, art. 19.

¹⁰⁵ Juridical Condition and Human Rights of the Child, Advisory Opinion OC-17/02, Inter-Am. Ct. H.R. (ser. A) No. 17, ¶ 54 (Aug. 28, 2002).

¹⁰⁶ *Gómez Paquiyauri Brothers v. Peru*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 110, ¶¶ 124, 163, 164, 171 (Jul. 8, 2004).

¹⁰⁷ *Villagrán Morales et. al v. Guatemala*, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 63, ¶¶ 144, 191 (Nov. 19, 1999); *Chitay Nech et. al v. Guatemala*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 212, ¶ 169 (May 25, 2010); *Juvenile Reeducation Institute v. Paraguay*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 112, ¶ 161 (Sept. 2, 2004).

¹⁰⁸ *Furlan and Family v. Argentina*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 246, ¶¶ 125-27 (Aug. 31, 2012). With regards to the right to privacy of children, the Inter-American Court has found

Violations of children’s privacy have far-reaching implications for the exercise of other rights. The U.N. SR on Privacy has observed that

Children’s rights are universal, indivisible, interdependent and interrelated. Their right to privacy enables their access to other rights critical to developing personality and personhood, such as the rights to freedom of expression and of association and the right to health, among others. Children’s privacy relates to their bodily and mental integrity, decisional autonomy, personal identity, informational privacy and physical/spatial privacy. (citations omitted)¹⁰⁹

With regard to informational privacy, the United Nations Committee on the Rights of the Child (“CRC Committee”) has urged states to “take all necessary measures to ensure that the gathering, storage and use of sensitive personal data are consistent with its obligations under Article 16 of the American Convention.”¹¹⁰ More specifically, the CRC Committee has recommended that

Effective measures are adopted to ensure that such information does not reach the hands of persons who are not authorized by law to receive, possess or use it [and that] [c]hildren and parents under its jurisdiction have the right to access their data and to request rectification or elimination of information, when it is incorrect or has been collected against their will or processed contrary to the provisions of the Law¹¹¹

State surveillance has distinct implications for children. The CRC Committee has emphasized that the right to privacy is “vital to children’s agency, dignity and safety and for the exercise of their rights,”¹¹² and observed that mass surveillance has “adverse consequences on children, which can continue to affect them at later stages of their lives.”¹¹³ The consequences of surveillance and retention of data obtained through surveillance may extend for decades. In the cases of illegal or mismanaged targeted surveillance of children, their individual development may have irreparable consequences. Children are particularly vulnerable to stigmatization. The label of “criminal” or “subversive” as a result of being target of illegal and arbitrary state surveillance could profoundly impact their ability to access education, healthcare, employment, and other rights. In light of these impacts, the CRC Committee has upheld the state obligation to “ensure that children and their parents or caregivers can easily access stored data, rectify data

a violation of the right to privacy when the minor relatives of the victims were subjected “to hatred, public contempt, persecution and discrimination” after the State of Peru wrongly castigated victims of terrorism. *Gómez Paquiyauri Brothers*, Inter-Am. Ct. H.R. (ser. C) No. 110, *supra* note 106, at ¶¶ 182, 253 (7).

¹⁰⁹ Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Report of the Special Rapporteur Artificial intelligence and privacy, and children’s privacy*, ¶ 71, U.N. Doc. A/HRC/46/37 (Jan. 21, 2021).

¹¹⁰ Comm. on the Rts. of the Child, *Concluding Observations on the Combined Third and Fourth Periodic Review of France*, ¶ 51, U.N. Doc. CRC/FRA/CO/4 (June 22, 2009) [hereinafter *Comm. on the Rts. of the Child Report of 2009*]. *See also* Comm. on the Rts. of the Child, *Concluding Observations on the Second Periodic Report of Kuwait*, ¶ 18, U.N. Doc. CRC/C/KWT/CO/2 (Oct. 29, 2013) (urging state party to “develop and implement a policy to protect the privacy of all children who have been registered in the national database”); Comm. on the Rts. of the Child, *Concluding Observations on the Combined Third and Fourth Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, ¶ 37(a), U.N. Doc. CRC/C/GBR/CO/4 (Oct. 20, 2008) (recommending “that children are protected against unlawful and arbitrary with their privacy including by introducing stronger regulations for data protection”).

¹¹¹ Comm. on the Rts. of the Child Report of 2009, *supra* note 110, at ¶ 51.

¹¹² Comm. on the Rts. of the Child, *General Comment No. 25 on Children’s Rights in Relation to the Digital Environment*, ¶ 67, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021) [hereinafter *Comm. on the Rts. of the Child General Comment No. 25*].

¹¹³ *Id.* at ¶ 68.

that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations.”¹¹⁴ These rights to access and rectification of children’s data in possession of the State require having knowledge of its collection, monitoring and storage. Therefore, provision of remedies in cases of abuse and illegal targeted surveillance of children are very relevant in this context.

The Commission’s merits report indicates that intelligence operations targeted CCAJAR members and their families, including their children.¹¹⁵ This case presents the Court with an opportunity to craft robust protections to protect the rights of the child from interference by intelligence agencies. To this end, this Court should recognize a presumption against state surveillance of children. It should also impose strict restrictions to ensure that any measures the state takes that interfere with a child’s right to privacy take into account “the best interests of the child” and the child’s “special rights” as required by international standards, specifically the protections established by this Court.¹¹⁶ In addition to the safeguards required under international human rights law for state surveillance of any individual, the use of surveillance against children should be accompanied by a number of additional protections, including: careful exceptionality and proportionality assessments; strict and more consistent judicial controls; and special limits on the retention of children’s data.

B. COLOMBIA’S FAILURE TO ADEQUATELY REGULATE COMMUNICATIONS SURVEILLANCE BY INTELLIGENCE AGENCIES VIOLATES RIGHTS PROTECTED BY THE AMERICAN CONVENTION.

For decades, Colombia has used invasive surveillance tools to intercept the private communications of CCAJAR members and their families. In response to criticism of its practice of surveilling HRDs, Colombia enacted Intelligence Law 1621 in 2013 (“2013 Intelligence Law” or “Intelligence Law”).¹¹⁷ In its filings to this Court, Colombia insists that this law “clearly and precisely establishes the specific circumstances in which [intelligence activities] can be authorized to guarantee that any action conforms to the principles of legality, proportionality and necessity” and “provides safeguards at various levels”¹¹⁸

The Intelligence Law does not explicitly authorize Colombian intelligence agencies to intercept private communications. In fact, Colombian law does not contemplate that any authority is empowered to engage in the interception of communications for purposes other than criminal investigations. Nevertheless, Colombia’s intelligence agencies have systematically engaged in intelligence activities unsanctioned by law, exploited the vagueness of key provisions of the Intelligence Law related to electromagnetic spectrum monitoring, and taken advantage of weak oversight in violation of the American Convention. Colombia provides no explanation for

¹¹⁴ *Id.* at ¶ 72.

¹¹⁵ Merits Report No. 57/19, *supra* note 3, at ¶¶ 177-179. U.N. bodies have repeatedly expressed concern over the involvement of children in intelligence activities. See *HRC Concluding Obs. on Colombia (2016)*, *supra* note 53, at ¶ 41; Comm. on the Rts. of the Child, *Concluding Observations on the Combined Fourth and Fifth Periodic Reports of Colombia*, ¶ 65(e), U.N. Doc. CRC/C/COL/CO/4-5 (Mar. 6, 2015).

¹¹⁶ Convention on the Rights of the Child, *supra* note 47, at arts. 3, 16; Advisory Opinion OC-17/02, *supra* note 105, at ¶ 59.

¹¹⁷ Merits Report No. 57/19, *supra* note 3, at ¶ 59.

¹¹⁸ Public Hearing in Case Members of José Alvear Restrepo Lawyers’ Collective v. Colombia Part 2, *supra* note 1, at 8:32:28-8:32:49.

how unlawful surveillance of CCAJAR members continued after the dissolution of the DAS, and merely insists that the Intelligence Law is adequate.

To assess the Colombian government's claim that its current legal framework is adequate, this Court should look to Inter-American and international human rights standards that establish minimum requirements for ensuring a comprehensive regulatory framework on state communications surveillance systems and activities.¹¹⁹ While international human rights law clearly requires restrictions and limitations on the use of surveillance tools and interferences with the right to privacy, the details regarding the frameworks that adequately limit surveillance are still developing. This Court is in a unique position to set standards in this area. Where there are conflicting standards or gaps in international law, this Court should assess the context and historical practices in the country in question. This Court should take into account Colombia's troubling history of abusive surveillance practices and apply the highest standards of protection possible.¹²⁰ An examination of the Colombian Intelligence Law, in conjunction with laws and policies on telecommunications data retention and access, data protection, foreign data transfers, and public access to information, demonstrates that Colombia falls far short of its international obligations, placing the work and lives of HRDs and their families at high risk. The consequences of unchecked surveillance of HRDs, including CCAJAR members, are profoundly threatening to Colombia's democracy and to individuals working on matters of public interest.

1. This Court must examine Colombia's surveillance against the most protective international human rights standards.

- a. Communications surveillance by intelligence authorities must be regulated to meet the standards of legality, legitimacy, suitability, necessity, and proportionality established by the American Convention.*

The American Convention requires that any state activity that interferes with the rights protected under the Convention must satisfy the fundamental principles of legality, legitimacy, suitability, proportionality, and necessity.¹²¹ This Court has applied these principles in examining whether state communications surveillance conforms to the American Convention.¹²² Similarly, the European Court of Human Rights ("European Court") and the HRC have affirmed these principles repeatedly in assessing legal frameworks that regulate state surveillance activity,

¹¹⁹ This Court has historically relied on jurisprudence by other human rights bodies to interpret the scope and content of the concept of necessity. *See, e.g.*, Herrera Ulloa, Inter-Am. Ct. H.R. (ser. C) No. 107, *supra* note 73, at ¶¶ 121-122, 125-126 (considering international human rights standards to establish proper restrictions on freedom of expression); Mapiripán Massacre v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 134, ¶ 153 (Sept. 15, 2005) (considering international standards to establish the scope and content of the rights of the child).

¹²⁰ *See, e.g.*, Ekimdzhiev v. Bulgaria, App. No. 70078/12, Eur. Ct. H.R., ¶ 293 (Jan. 11, 2022), <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-214673%22%5D%7D> (reasoning that courts must examine "the actual operation of the surveillance regime" and "the existence or absence of actual abuse" when assessing whether laws offer effective guarantees against abusive surveillance).

¹²¹ American Convention on Human Rights, *supra* note 50, arts. 11(2), 13(2), 30, 32(2).

¹²² Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 129; Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 76 (Jan. 27, 2009).

including surveillance regimes established for purposes of protecting national security.¹²³ This Court must examine whether Colombia's surveillance activities and laws satisfy these principles.

First, under the principle of legality, any interference with human rights caused by state surveillance must be accessible and foreseeable. This requires that any such interference be “clearly established by law,” and the interference is permissible only if done in accordance with laws.¹²⁴ The interference must be authorized or “contemplated” by law.¹²⁵ If authorities engage in activity that is not authorized by law, or activity that is explicitly prohibited by it, then this results in a violation of the principle of legality.¹²⁶

The principle of legality also requires, according to this Court, that domestic laws authorizing interference with human rights protected by the Convention be precise and clear so that individuals can foresee how they will be applied.¹²⁷ This Court and the European Court have stated that “clear, detailed rules” are especially important in the secretive context of state surveillance, where there is a heightened risk of arbitrary application of the laws and abuse by the state.¹²⁸ Clarity and precision become even more critical as technology becomes more sophisticated.¹²⁹ This also requires that the law in question must be publicly accessible.¹³⁰ “Secret rules and interpretations” do not satisfy this standard.¹³¹

To ensure a thorough assessment of the clarity and precision of Colombian laws on surveillance, this Court should look to the list of minimum requirements established in Inter-American jurisprudence and standards. In 2009, this Court articulated a number of elements that domestic laws on surveillance must establish, including: “the circumstances in which the [surveillance] measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed.”¹³² In 2013, the I-A SR on FOE and the U.N. SR on FOE elaborated on this jurisprudence, stating that domestic laws “must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged.”¹³³

¹²³ Big Brother Watch v. United Kingdom, App. No. 58170/13, Eur. Ct. H.R., ¶ 332 (May 25, 2021), <https://hudoc.echr.coe.int/fre?i=001-210077>; Roman Zakharov, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39, at ¶ 227 (analyzing challenge brought by journalist of interception of telephone conversations without prior judicial authorization); Hum. Rts. Comm., *Concluding Observations on the Fifth Periodic Report of Belarus*, ¶ 44, U.N. Doc. CCPR/C/BLR/CO/5, (Nov. 22 2018) [hereinafter *HRC Concluding Obs. on Belarus*].

¹²⁴ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 130; Tristán Donoso, Inter-Am. Ct. H.R. (ser. C) No. 193, *supra* note 122, at ¶ 56.

¹²⁵ *Id.* at ¶ 76.

¹²⁶ *Id.* at ¶ 80 (finding that the disclosure of telephone recordings between attorney and their client to third parties violated the principle of legality).

¹²⁷ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 118; Tristán Donoso, Inter-Am. Ct. H.R. (ser. C) No. 193, *supra* note 122, at ¶ 77; Kimel, Inter-Am. Ct. H.R. (ser. C) No. 177, *supra* note 64, at ¶ 63. *See also* I-A SRFOE Report of 2013, *supra* note 78, at ¶ 153.

¹²⁸ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 118. *See also* Szabo v. Hungary, App. No. 37138/14, Eur. Ct. H.R., ¶ 62 (Jan. 12, 2016), <https://hudoc.echr.coe.int/fre?i=001-160020>.

¹²⁹ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 115; Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 62.

¹³⁰ Hum. Rts. Council Res. 48/4, U.N. Doc. A/HRC/RES/48/4 (Oct. 7, 2021).

¹³¹ OHCHR Report of 2014, *supra* note 45, at ¶ 29.

¹³² Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 131.

¹³³ *Joint Declaration on Surveillance*, *supra* note 77, at ¶ 9.

The European Court has established minimum requirements for domestic laws regulating surveillance, which overlap with standards established by this Court. The European Court requires that domestic laws on surveillance, even within the framework of intelligence gathering for national security purposes, precisely describe: (1) “grounds on which secret surveillance may be resorted to;” (2) “persons who can be placed under surveillance;” (3) “duration of secret surveillance measures;” (4) “authorization procedures;” (5) “procedures for storing, accessing, examining, using . . . the data obtained;” (6) “procedures for . . . communicating . . . surveillance data” to other parties; (7) “procedures for . . . destroying surveillance data;” (6) “oversight arrangements;” (8) “notification measures;” and (9) “remedies.”¹³⁴

Additionally, where, as here, surveillance activities have targeted or risk targeting the communications of HRDs, including lawyers, they should be subject to enhanced protections. This Court and the European Court have acknowledged the necessity of “greater degree of protection” and “the importance of specific procedural guarantees” over privileged communications, including the communications of attorneys and journalists.¹³⁵ Given the nature of the HRDs’ communications, these enhanced protections should apply to all HRDs.¹³⁶

Second, the principle of legitimacy requires that laws that interfere with any right enumerated in the American Convention must “be enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established.”¹³⁷ In other words, any interference with human rights caused by state surveillance must “have a legitimate purpose.”¹³⁸ The American Convention enumerates a number of aims that may qualify as legitimate purposes, including public safety, health, morals, and order, the rights and freedoms of others, and national security.¹³⁹ However, this Court has held that the mere invocation of a legitimate aim does not justify interference with the rights protected by the American Convention. Specifically, this Court found that the invocation of “national security” to characterize as a threat “anyone who genuinely or allegedly supported the fight to change the established order,” including HRDs, infringes on rights and freedoms.¹⁴⁰ This is a maneuver

¹³⁴ Ekimdzhev, App. No. 70078/12, Eur. Ct. H.R., *supra* note 120, at ¶¶ 294-355 (examining legal framework on secret surveillance, including for national security purposes); Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶¶ 55-57.

¹³⁵ Tristán Donoso, Inter-Am. Ct. H.R. (ser. C) No. 193, *supra* note 122, at ¶ 75. *See also* Ekimdzhev, App. No. 70078/12, Eur. Ct. H.R., *supra* note 120, at ¶ 333 (describing the need for heightened protections with regard to the interception of communications that are subject to the legal professional privilege); Sommer v. Germany, App. No. 73607/13, Eur. Ct. H.R., ¶ 56 (Apr. 27, 2017), <https://hudoc.echr.coe.int/eng?i=001-173091> (discussing importance of procedural safeguards for attorney-client communications interceptions in the criminal investigation context); Iordachi v. Moldova, App. No. 25198/02, Eur. Ct. H.R., ¶ 50 (Sept. 24 2009), <https://hudoc.echr.coe.int/fre?i=002-1661> (noting “the absence of clear rules” regulating how authorities should handle communications between attorneys and clients during surveillance); Sedletska v. Ukraine, App. No. 42634/18, Eur. Ct. H.R., ¶¶ 62, (Apr. 1, 2021) (“the [European] Court has repeatedly stated that limitations on the confidentiality of journalistic sources call for the most careful scrutiny.”).

¹³⁶ *See, e.g.*, Hum. Rts. Council Res. 48/4, ¶ 6(k), U.N. Doc. A/HRC/Res/48/4 (Oct. 13, 2021).

¹³⁷ American Convention on Human Rights, *supra* note 50, art. 30.

¹³⁸ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 129.

¹³⁹ American Convention on Human Rights, *supra* note 50, arts. 13(2), 16(2). *See also* International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families art. 19(3), Dec. 18, 1990, 2220 U.N.T.S. 3; European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8(2), ETS No. 005 (1953).

¹⁴⁰ Molina Thiessen v. Guatemala, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 106, ¶ 40(2) (May 4, 2004). *See also* Villamizar Durán et al. v. Colombia, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 364, ¶¶ 64-65 (Nov. 20, 2018) (describing the “national security doctrine” in Colombia, used to target human rights defenders including members of trade unions and the peasant labor movement); Isaza Uribe et al. v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 363, ¶¶ 127-8, 144, 207 (Nov. 20, 2018); Goiburú et al. v.

Colombia has used, and continues to use, to deter and disrupt legitimate human rights works by the members of CCAJAR.¹⁴¹ Given this context, the I-A SR on FOE and the U.N SR on FOE have advised particular scrutiny: “when national security is invoked as a reason for the surveillance of correspondence and personal information, the law must clearly specify the criteria to be used for determining the cases in which such surveillance is legitimate.”¹⁴²

Finally, the American Convention establishes the principles of necessity and proportionality, which require that state surveillance measures be necessary, suitable, and proportional in the specific context, such that they are deemed “necessary in a democratic society.”¹⁴³ Indeed, there is international consensus that the infringement on rights caused by state surveillance must be necessary and proportional.¹⁴⁴ While this Court has not had occasion to elaborate on these principles in the context of surveillance,¹⁴⁵ it has defined “necessary” in other contexts to mean that the chosen means “are absolutely essential to achieve the purpose sought and that, among all possible measures, there is no less burdensome one in relation to the right involved, that would be as suitable to achieve the proposed objective.”¹⁴⁶ Additionally, this Court has established that a proportional infringement on rights is one in which “the sacrifice inherent in the restriction . . . is not exaggerated or excessive in relation to the advantages obtained from this restriction and the achievement of the purposes sought.”¹⁴⁷

Paraguay, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 153, ¶ 61(5) (Sept. 22, 2006) (describing Southern Core’s dictatorial governments use of the “national security doctrine” to target leftist movements and other groups as “common enemies”); Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44 (concurring opinion of Judge Sergio Garcia Ramirez), at ¶ 13 (stating that “[t]o defend their excesses, the ‘classic’ tyrants . . . who oppressed many countries in our hemisphere, invoked reasons of national security, sovereignty, public peace Other, more recent, forms of authoritarianism, invoke public safety and the fight against crime to impose restrictions on rights and to justify the infringement of freedom.”); Chitay Nech, Inter-Am. Ct. H.R. (ser. C) No. 212, *supra* note 107, at ¶ 64 (describing the “‘national security doctrine’ in Guatemala used to target any person or organization that represented any form of opposition to the state”); Case of “Las Dos Erres” Massacre v. Guatemala, Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 211, ¶¶ 71-73 (Nov. 24, 2009) (same).

¹⁴¹ See, e.g., Merits Report No. 57/19, *supra* note 3, at ¶ 64 (describing former President Uribe’s description of CCAJAR’s work as “providing cover for terrorists”); *HRDs in Colombia*, *supra* note 6, at ¶¶ 137-140 (cataloging years-long smear campaigns by public officials against HRDs).

¹⁴² *Joint Declaration on Surveillance*, *supra* note 77, at ¶ 9.

¹⁴³ American Convention on Human Rights, *supra* note 50, arts. 11(2), 13(2), 16(2). See also Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 116; Tristán Donoso, Inter-Am. Ct. H.R. (ser. C) No. 193, *supra* note 122, at ¶ 56.

¹⁴⁴ See Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶¶ 54-55; Case C-293/12, Digital Rights Ireland, Ltd. v. Minister for Communications, ECLI:EU:C:2014:238, ¶ 46 (Apr. 8, 2014) [hereinafter Case C-293/12, DRI v. Minister]; Hum. Rts. Comm., *Van Hulst v. Netherlands*, U.N. Doc. CCPR/C/82/D/903/1999, ¶ 7.6 (Nov. 1, 2004); *HRC Concluding Obs. on the U.S.*, *supra* note 39, at ¶ 22(d); OHCHR Report of 2018, *supra* note 51, at ¶ 10; Martin Scheinin (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism), *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶¶ 17-18, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009); *Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, princ. 1.3, U.N. Doc. E/CN.4/1996/39 (Mar. 22, 1996). See also *Umohoza v. Rwanda*, 2 AfCLR 165, ¶ 132 (African Court on Human and Peoples’ Rights 2017).

¹⁴⁵ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 146.

¹⁴⁶ Chaparro Álvarez and Lapo Íñiguez v. Ecuador, Interpretation of the Judgment on Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 189, ¶ 93 (Nov. 26, 2008)]. The European Court has adopted a similar standard of necessity. See, e.g., *Faber v. Germany*, App. No. 40721/08, Eur. Ct. H.R., ¶¶ 32, 43 (Jul. 24, 2012), <https://hudoc.echr.coe.int/eng/?i=001-112446> (stating that “[t]he test of ‘necessity in a democratic society’ requires the Court to determine whether interference [with the rights to freedom of expression and to peaceful assembly] correspond to a ‘pressing social need’” and that “State has to fulfill positive obligations to protect right of assembly . . . and should find the least restrictive means” possible).

¹⁴⁷ Chaparro Álvarez, Inter-Am. Ct. H.R. (ser. C) No. 189, *supra* note 146, at ¶ 93 (discussing proportionality of restriction on the right to liberty). See also *Kimel*, Inter-Am. Ct. H.R. (ser. C) No. 177, *supra* note 64, at ¶¶ 83, 94 (applying this test to examine proportionality of restriction on the right to freedom of thought and expression); *Claude Reyes*, Inter-Am. Ct. H.R. (ser. C) No. 151, *supra* note 87, at ¶ 91.

b. *This Court should affirm that mass surveillance is incompatible with international human rights standards.*

Many international human rights bodies and experts agree that mass surveillance, as opposed to targeted surveillance, inherently violates the principles of necessity and proportionality, and as a result undermines the essence of the right to privacy. This Court should conform with that assessment. The Inter-American Commission has stated that mass communications surveillance “can never be considered proportionate.”¹⁴⁸ United Nations human rights bodies have also recognized the inherent incompatibility between mass surveillance and human rights standards.¹⁴⁹ In the context of data retention, access, and transfer of communications data, the CJEU has repeatedly recognized that indiscriminate (or non-targeted) *access by* or *transmission to* intelligence agencies of metadata retained by communication service providers, even for purposes of “combating serious crime” or “safeguarding national security” is impermissible.¹⁵⁰ It has also ruled that indiscriminate *retention* of traffic and location data for any purpose other than “safeguarding national security” is impermissible.¹⁵¹ Historically the European Court of Human Rights has also expressed concern regarding mass *domestic* surveillance.¹⁵² More recently, in the context of the U.K.’s mass *foreign* interception regime, while it found that this regime violated the rights to privacy and freedom of expression, it refrained from ruling that it was inherently disproportionate.¹⁵³ But this is at odds with international consensus,¹⁵⁴ and contrary to the HRC which criticized the same U.K. system of surveillance for allowing mass interception of communications and for applying more lenient protections to foreign as opposed to internal communications.¹⁵⁵

¹⁴⁸ Press Release, Inter-Am. Comm’n H.R., *IACHR and its Special Rapporteurship for Freedom of Expression Urge the State of Colombia to Conduct a Diligent, Timely, and Independent Investigation into Allegations of Illegal Surveillance Against Journalists, Justice Operators, Human Rights Defenders*, Press Release No. 118/20 (May 21, 2020), https://www.oas.org/en/iachr/media_center/PReleases/2020/118.asp.

¹⁴⁹ Hum. Rts. Comm., *Concluding Observations on the Sixth Periodic Report of Hungary*, ¶ 43, U.N. Doc. CCPR/C/HUN/CO/6 (May 9, 2018) [hereinafter *HRC Concluding Obs. on Hungary*] (expressing “concern[] that the State party’s legal framework on secret surveillance for national security purposes . . . allows for mass interception of communications”); OHCHR Report of 2018, *supra* note 51, at ¶ 17 (stating that indiscriminate mass surveillance is “not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures.”); David Kaye, et al. (Special Rapporteur on Freedom of Opinion and Expression et al.), *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*, ¶ 8(a) (May 4, 2015), <http://www.osce.org/fom/154846> [hereinafter *Joint Declaration on FOE*].

¹⁵⁰ Case C-623/17, *Priv. Int’l v. Sec’y of State for Foreign and Commonwealth Affs. and Others*, ECLI:EU:C:2020:790, ¶¶ 78-81 (Oct. 6, 2020) [hereinafter *Case C-623/17, Priv. Int’l v. Sec’y of State*]; Case C-140/20, *G.D. v. Comm’r of An Garda Síochána et al.*, ECLI:EU:C:2022:258, ¶ 105 (Apr. 5, 2021).

¹⁵¹ Case C-293/12, *DRI v. Minister*, *supra* note 144, at ¶¶ 56–59. Though rejecting indiscriminate retention of metadata for purposes of “combating serious crime,” the CJEU has permitted states to require communications service providers to indiscriminately retain traffic and location data for purposes of “safeguarding national security,” subject to strict safeguards including effective review by an independent body. *See* Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net v. Premier Ministre*, ECLI:EU:C:2020:791, ¶¶ 137-39 (Oct. 6, 2020) [hereinafter *Cases C-511/18 et al, La Quadrature du Net*].

¹⁵² *See, e.g.*, Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 67 (expressing “serious concern” about the possibility of “the unlimited surveillance of a large number of citizens”).

¹⁵³ *Big Brother Watch*, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 376.

¹⁵⁴ *Id.* at ¶¶ 11 (partly concurring partly dissenting opinion of Judge Pinto de Albuquerque) (observing that “if there is a consensus in Europe on non-targeted bulk interception, the consensus is that it should be prohibited, but this has been ignored by the Court.”).

¹⁵⁵ Hum. Rts. Comm., *Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, ¶ 24, U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17 2015) [hereinafter *HRC Concluding Obs. on the U.K.*].

- c. *Communications surveillance must be subject to prior judicial authorization and independent oversight to safeguard against abuse.*

This Court has affirmed the importance of “rigorous” controls over intelligence services and activities.¹⁵⁶ While the Colombian Constitution requires prior judicial authorization for the “interception” or “recording” of private communications,¹⁵⁷ Colombian statutory law—the Intelligence Law—exempts intelligence agencies from this requirement when engaging in other surveillance activities, such as electromagnetic spectrum monitoring (“EMS monitoring”) and accessing data retained by communications service providers (“CSP”).¹⁵⁸ Although this Court has not had occasion to elaborate on the precise standards required for proper authorization of, or oversight over, communication surveillance under the American Convention, longstanding Inter-American jurisprudence on due process protections, and the disturbing history of abusive surveillance practices in Colombia, should impel this Court to require that *any* surveillance activity in Colombia be subject to *prior judicial* authorization.¹⁵⁹ Additionally, this Court should conform with international consensus that surveillance regimes must be overseen effectively “by an independent, external body.”¹⁶⁰

The European Court, the HRC, and human rights experts agree that oversight of surveillance activities must be conducted by independent bodies through multiple stages. In the context of examining a surveillance regime intended to prevent or detect crime, safeguard economic interests, and protect national security, the European Court identified three stages at which independent oversight is crucial: “when the surveillance is first ordered, while it is being carried out, or after it has been terminated.”¹⁶¹ Similarly, the HRC has stressed the importance of an authorization process for the surveillance of communications, and has also instructed states to develop independent and effective oversight mechanisms of surveillance regimes.¹⁶² These procedural safeguards are rooted in international consensus.

There are three main reasons this Court should uphold a requirement of prior judicial authorization of state communications surveillance. First, there is international consensus that prior judicial authorization of any surveillance activity is “an important safeguard against arbitrariness.”¹⁶³ Indeed, the Inter-American Commission has endorsed the I-A SR on FOE’s view that:

¹⁵⁶ Myrna Mack-Chang v. Guatemala, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 101, ¶ 284 (Nov. 25, 2003).

¹⁵⁷ CONSTITUCIÓN POLÍTICA DE COLOMBIA [C.P.] art. 15, www.georgetown.edu/pdba/Constitutions/Colombia/col91.html.

¹⁵⁸ See Section B(2)(a) below.

¹⁵⁹ This Court has required prior judicial authorization to protect the rights of individual facing arrest and detention (Maritza Urrutia v. Guatemala, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 103, ¶ 67 (Nov. 27, 2003)), subjected to body searches (Fernández Prieto and Tumbeiro v. Argentina, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 411, ¶ 109 (Sept. 1, 2020)), and as a guarantee of privacy rights (Escué Zapata v. Colombia, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 165, ¶ 94 (Jul. 4, 2007)).

¹⁶⁰ Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 197. See also *HRC Concluding Obs. on Belarus*, *supra* note 123, at ¶ 44; G.A. Res. 68/167, ¶ 4, (Dec. 18, 2013); *Joint Declaration on Surveillance*, *supra* note 77, at ¶ 9; U.N. SRRP Report of 2019, *supra* note 36, at ¶ 46(b).

¹⁶¹ Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 336.

¹⁶² *HRC Concluding Obs. on Belarus*, *supra* note 123, at ¶ 44; *HRC Concluding Obs. on Hungary*, *supra* note 149, at ¶ 44. See also *Joint Declaration on Surveillance*, *supra* note 77, at ¶ 9.

¹⁶³ ECtHR, Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 351. See also Roman Zakharov, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39, at ¶ 249; Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 77;

[D]ecisions to undertake surveillance activities that invade the privacy of individuals *must be authorized by independent judicial authorities*, who must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued States must ensure that the judicial authority is specialized and competent to make decisions on the legality of the communications surveillance, the technologies used, and its impact on the sphere of rights that could be involved.¹⁶⁴

Second, requiring prior judicial authorization is also supported by longstanding Inter-American jurisprudence on due process protections.¹⁶⁵ This Court has understood the due process guarantees established by Article 8 of the American Convention as “‘a series of requirements that must be observed by the procedural bodies’ so that a person may defend himself adequately against any act of the State that could affect his rights.”¹⁶⁶ This Court should view prior judicial authorization as a necessary protection against the “inherent danger of abuse” of a secret surveillance system.¹⁶⁷

Moreover, this Court has emphasized that the right to privacy requires strong protection.¹⁶⁸ In *Escher v. Brazil*, this Court established the importance of independent supervision of communications surveillance and the significant role of judges in examining *ex parte* applications for surveillance measures

In proceedings whose juridical nature requires the decision to be issued without hearing the other party, the grounds and justification must show that all the legal requirements and other elements that justify granting or refusing the measure have been taken into

Hum. Rts. Comm., *Concluding Observations on the Seventh Periodic Report of Germany*, ¶ 43, U.N. Doc. CCPR/C/DEU/CO/7 (Nov. 11, 2021). Despite acknowledging it as an important safeguard, neither the European Court nor the CJEU have required prior *judicial* authorization for surveillance measures but have required prior *independent* authorization. *See* Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 351 (“bulk interception should be authorized by . . . a body which is independent of the executive.”); Case C-293/12, *DRI v. Minister*, *supra* note 144, at ¶ 62 (holding that to protect the respect for private life access by state authorities to data retained by communication service providers should be “made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued”). *See also* Cases C-203/15 and C-698/15, *Tele2 v. Post-och*, *supra* note 82, at ¶ 120 (stating that “it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body”); Case C-623/17, *Priv. Int’l v. Sec’y of State*, *supra* note 150, at ¶¶ 78- 82 (confirming that EU law, including Cases C-203/15 and C-698/15, *Tele2 v. Post-och*, applies when intelligence agencies seek to access data retained by telecommunications service providers for the purposes of national security).

¹⁶⁴ I-A SRFOE Report of 2013, *supra* note 78, at ¶ 165 (emphasis added). *See* Merits Report No. 57/19, *supra* note 3, at ¶¶ 308, 312 (endorsing I-A SR’s position). *See also* Edison Lanza (Special Rapporteur on Freedom of Expression), *The Right to Information and National Security*, ¶ 58, OEA/Ser.L/V/II CIDH/RELE/INF.24/20 (July 2020) [hereinafter I-A SRFOE Report of 2020] (surveillance activities must follow the requirement of prior judicial authorization).

¹⁶⁵ I-A SRFOE Report of 2013, *supra* note 78, at ¶¶ 164-165 (relying on Article 8 of the American Convention of Human Rights to establish the requirement of prior judicial authorization).

¹⁶⁶ *Ivcher Bronstein v. Peru*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 74, ¶ 102 (Feb. 6, 2001) (citations omitted).

¹⁶⁷ *Escher*, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 118.

¹⁶⁸ *Escué Zapata*, Inter-Am. Ct. H.R. (ser. C) No. 165, *supra* note 159, at ¶ 95 (establishing that “[t]he protection of the private life, family life and residence from arbitrary or abusive interference implies an acknowledgment that there is a personal sphere which must be exempt from and immune to the abusive or arbitrary invasion or attacks by third parties or the public authority.”).

consideration. Hence, the judge must state his or her opinion, respecting adequate and effective guarantees against possible illegalities and arbitrariness in the procedure in question.¹⁶⁹

Third, Colombia's extensive record of spying on political opponents further justifies the requirement of a judicial check against abuse.¹⁷⁰ In *Myrna Mack-Chang v. Guatemala*, this Court recognized the inherent danger of secret surveillance, holding that "[m]easures to control intelligence activities must be especially rigorous because, given the conditions of secrecy under which these activities take place, they can drift toward committing violations of human rights and illegal criminal actions."¹⁷¹ Similarly, the European Court has recognized that "judicial control offer[s] the best guarantees of independence, impartiality and a proper procedure . . . , " particularly "[i]n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole."¹⁷² The record before this Court demonstrates that Colombia has already, for decades, engaged in abusive surveillance practices, and therefore this Court should require it to adopt the best guarantees of independence available.

While prior judicial authorization is necessary, it is only one part of an effective oversight mechanism, as abuses can occur after authorization is granted.¹⁷³ There is international consensus that surveillance regimes must also be regularly overseen, after authorization, by independent and external bodies.¹⁷⁴ According to international best practice, these oversight mechanisms

[M]ay integrate a combination of administrative, judicial and/or parliamentary oversight. Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight

¹⁶⁹ Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 139.

¹⁷⁰ *See, e.g.*, Ekimdzhev, App. No. 70078/12, Eur. Ct. H.R., *supra* note 120, at ¶ 293 (reasoning that courts should consider "existence or absence of actual abuse" in examining state's surveillance system against international human rights standards).

¹⁷¹ Myrna Mack-Chang, Inter-Am. Ct. H.R. (ser. C) No. 101, *supra* note 156, at ¶ 284.

¹⁷² Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 77.

¹⁷³ OHCHR Report of 2014, *supra* note 45, at ¶ 38 (stating that "judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight . . .").

¹⁷⁴ Ekimdzhev, App. No. 70078/12, Eur. Ct. H.R., *supra* note 120, at ¶¶ 334–47 (examining independence and effectiveness of oversight arrangements separately from examination of authorization procedures); *HRC Concluding Obs. on Belarus*, *supra* note 123, ¶ 44; *HRC Concluding Obs. on Hungary*, *supra* note 149, at ¶ 44. *See also* G.A. Res. 68/167, ¶ 4(d) (Dec. 18, 2013); *Joint Declaration on Surveillance*, *supra* note 77, at ¶ 9.

processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.¹⁷⁵

d. *Targets of unlawful communications surveillance must have access to effective remedies, which requires notice of surveillance and the ability to correct or erase the information collected.*

Article 25 of the American Convention provides that “[e]veryone has the right to simple and prompt recourse, or any other effective recourse, to a competent court or tribunal for protection against acts that violate his fundamental rights recognized by the constitution or laws or by this Convention”¹⁷⁶ This Court has described this right as “one of the fundamental pillars not only of the American Convention, but of the very rule of law in a democratic society,”¹⁷⁷ and established that “the right of access to justice is a peremptory norm of international law.”¹⁷⁸ In accordance with the principle of effective judicial protection and this Court’s well-established jurisprudence, the American Convention obligates states to establish judicial remedies that “are accessible to [everyone], without any undue obstacles or delays, so that they may achieve their purpose promptly, simply and fully.”¹⁷⁹ The remedies must be effective, meaning that they must be actually capable of redressing human rights violations.¹⁸⁰ This Court has concluded that “the inexistence of an effective remedy for the violations of the rights recognized in the Convention entails a violation of the Convention by the State Party”¹⁸¹ This Court must determine whether Colombian law provides targets of unlawful state surveillance access to effective remedies in light of this well-established jurisprudence.¹⁸²

Notice is a *conditio sine qua non* for ensuring the right of individuals to challenge communications surveillance. In both the criminal and immigration context, this Court has held that the failure to provide notice is a violation of the due process guarantees codified by Article 8

¹⁷⁵ OHCHR Report of 2018, *supra* note 51, at ¶ 40. *See also The Global Principles on National Security and the Right to Information (The Tshwane Principles)*, OPEN SOCIETY JUSTICE INITIATIVE, Principle 31 (2013), <https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles> [hereinafter *Tshwane Principles*]; U.N. SRCTHR Report of 2010, *supra* note 2, at ¶ 13, Practice 7; G.A. Res. 75/291, The United Nations Global Counter-Terrorism Strategy: seventh review, ¶ 106 (July 30, 2021).

¹⁷⁶ American Convention on Human Rights, *supra* note 50, art. 25. *See also* G.A. Res 217A (III) art. 8, Universal Declaration of Human Rights (Dec. 10, 1948); International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families art. 2(3), Dec. 18, 1990, 2220 U.N.T.S. 3.; American Declaration of the Rights and Duties of Man art. XVIII, O.A.S., Res. XXX (1948), O.A.S. Off. Rec. OEA/Ser.LV/I.4 Rev. (1965).

¹⁷⁷ Castillo Páez v. Perú, Merits, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 34, ¶ 82 (Nov. 3, 1997).

¹⁷⁸ Goiburú, Inter-Am. Ct. H.R. (ser. C) No. 153, *supra* note 140, at ¶ 131.

¹⁷⁹ Lagos del Campo v. Perú, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 340, ¶ 174 (Aug. 31, 2013).

¹⁸⁰ *See* Velásquez Rodríguez v. Honduras, Preliminary Objections, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 1, ¶ 93 (June 26, 1987); Case of the Xákmok Kásek Indigenous Community v. Paraguay, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 214, ¶ 140 (Aug. 24, 2010); Case of Abrill Alosilla et al. v. Perú, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 223, ¶ 75 (Mar. 4, 2011).

¹⁸¹ Kaliña and Lokono Peoples v. Suriname, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 309, ¶ 237 (Nov. 25, 2015).

¹⁸² The European Court of Human Rights has included access to effective remedies as a component of its assessment of any secret surveillance regime. *See* Ekimdzhev, App. No. 70078/12, Eur. Ct. H.R., *supra* note 120, at ¶¶ 352–355 (examining whether bulgarian surveillance regime provided an effective remedy for individuals complaining of unlawful surveillance).

of the American Convention.¹⁸³ In accordance with this Inter-American case law, the Court should establish the obligation to provide notice in the surveillance context. This Court has repeatedly held that the minimum guarantees established by Article 8 of the American Convention defines due process for “the determination of rights and obligations of a civil, labor, fiscal or any other nature.”¹⁸⁴ Moreover, this Court has understood that due process requirements “must be observed at the different procedural stages to ensure that the individual is able to defend his rights adequately vis-à-vis any act of the State adopted by any public authority, whether administrative, legislative or judicial, that affects those rights.”¹⁸⁵

In *Szabo v. Hungary*, while examining a legal framework on domestic intelligence gathering for national security purposes, the European Court noted the significant role of notice: “there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively.”¹⁸⁶ Similarly, the CJEU held, in a case challenging indiscriminate metadata retention by communications service providers and unfettered access to that metadata by state authorities, that notice to any individual whose data has been accessed by state authorities is “necessary to enable the persons affected to exercise, *inter alia*, their right to a legal remedy” under the European privacy directive.¹⁸⁷ It concluded, “competent national authorities to whom access to the retained data has been granted must notify the persons affected . . . as soon as that notification is no longer liable to jeopardise the investigations being undertaken”¹⁸⁸

The European Court has accepted in some cases that as an alternative to notice, states can simply ensure that anyone who “suspects” that they have been surveilled have standing in court.¹⁸⁹ While it is important as a safeguard against abuse to ensure that Colombian law provides standing to challenge unlawful surveillance to those who suspect but might not know they have been surveilled, it is not sufficient. Surveillance activities by intelligence agencies

¹⁸³ See, e.g., *Vélez Lóor v. Panama*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 218, ¶ 180 (Nov. 23, 2010) (holding the failure to notify a detainee of his right to appeal created legal uncertainty that “made the exercise of the right to appeal a judgment impracticable” and constituted “*per se*” a violation of the Convention); *Tibi v. Ecuador*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 114, ¶¶ 188-89 (Sept. 7, 2004) (finding that the failure to notify the victim “in a timely and complete manner” of criminal charges denied him the opportunity to adequately prepare his defense in violation of the American Convention); *López Álvarez v. Honduras*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 141, ¶ 149 (Feb. 1, 2006); *Barreto Leiva v. Venezuela*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 206, ¶ 28 (Nov. 17, 2009).

¹⁸⁴ *Constitutional Court v. Peru*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 71, ¶ 70 (Jan. 31, 2001). See also *Ivcher Bronstein*, Inter-Am. Ct. H.R. (ser. C) No. 74, *supra* note 166, at ¶ 103; *Vélez Lóor*, Inter-Am. Ct. H.R. (ser. C) No. 218, *supra* note 183, at ¶ 142; *Nadege Dorzema et al. v. Dominican Republic*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 251, ¶ 157 (Oct. 24, 2012); *Constitutional Tribunal (Camba Campos et al.) v. Ecuador*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 268, ¶ 166 (Aug. 28, 2013); *Pacheco Tineo Family v. Bolivia*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 272, ¶ 130 (Nov. 25, 2013).

¹⁸⁵ *Ruano Torres et al. v. El Salvador*, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 303, ¶ 151 (Oct. 5, 2015).

¹⁸⁶ *Szabo*, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 86. Because Hungarian law did not provide for notification of any kind, or any remedies in case of abuse, the European court concluded that that the legislation fell short of ensuring adequate safeguards. *Id.*

¹⁸⁷ Cases C-203/15 and C-698/15, *Tele2 v. Post-och*, *supra* note 82, at ¶ 121.

¹⁸⁸ *Id.* See also OHCHR Report of 2014, *supra* note 45, at ¶ 40 (underscoring the importance of notice and standing to challenge surveillance “in determining access to effective remedy”).

¹⁸⁹ *Roman Zakharov*, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39, at ¶ 234. See also *Big Brother Watch*, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 357.

targeting HRDs were not discovered until years later.¹⁹⁰ While some had reason to suspect they were being surveilled, others, including the families of CCAJAR members, did not. Therefore, this Court should look to the more protective approach that the European Court applied in *Szabo v. Hungary*,¹⁹¹ and that the CJEU has endorsed.

The right to an effective remedy from unlawful state surveillance practices also requires that individuals subjected to surveillance have the ability to access data that the government has collected, and to correct or erase it. The Inter-American Commission has adopted this requirement in its Declaration of Principles on Freedom of Expression.¹⁹² European Courts and human rights experts have affirmed this obligation in cases related to communications interception and personal data transfers,¹⁹³ emphasizing this requirement in the context of surveillance of communications between lawyers and clients.¹⁹⁴

e. The public must have the right of access information on state surveillance practices, which is a crucial safeguard against abuse.

This Court has affirmed that Article 13 of the American Convention “protects the right of the individual to receive [state-held] information and the positive obligation of the State to provide it, so that the individual may have access to such information or receive an answer that includes a justification when, for any reason permitted by the Convention, the State is allowed to restrict access to the information in a specific case.”¹⁹⁵ Recognizing that the principle of maximum disclosure is a touchstone of democratic societies that enables public scrutiny, this Court has compelled States “[to establish] the presumption that all information is accessible, subject to a limited system of exceptions” and has shifted the burden of proof to the state to justify withholding information from the public.¹⁹⁶ But restrictions on the right to access information on vague and overbroad “national security” grounds is impermissible, and falls short of the requirements of legality, legitimacy, necessity, and minimum safeguards.¹⁹⁷

In the surveillance context, there is well-established international consensus on the importance of the right to access information for ensuring public oversight over government surveillance activity.¹⁹⁸ When the surveillance is unlawful, as in this case, international experts

¹⁹⁰ See, e.g., Merits Report No. 57/19, *supra* note 3, at ¶¶ 131- 159.

¹⁹¹ *Szabo*, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 86.

¹⁹² Inter-Am. Comm’n H.R., *Declaration of Principles on Freedom of Expression*, Res., 108th Sess., Principle 3 (Oct. 2000), <http://www.cidh.oas.org/Relatoria/showarticle.asp?artID=26&IID=1> [hereinafter *Declaration of Principles on FOE*].

¹⁹³ Case C-362/14, Maximilian Schrems v. Data Protection Comm’r, ECLI:EU:C:2015:650, ¶ 95 (Oct. 6, 2015) [hereinafter *Case C-362/14, Schrems v. Data Protection*] (holding that legislation must provide the “possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data” in conformity right to effective judicial protection). See also OHCHR Report of 2018, *supra* note 51, at ¶ 41 (stating that those subjected to surveillance are entitled to notification, an explanation, and the opportunity to correct and/or delete personal information, “provided that information is not needed any longer to carry out any current or pending investigation . . .”).

¹⁹⁴ See *supra* note 135.

¹⁹⁵ Claude Reyes, Inter-Am. Ct. H.R. (ser. C) No. 151, *supra* note 87, at ¶ 77.

¹⁹⁶ *Id.* at ¶ 92.

¹⁹⁷ See I-A SRFOE Report of 2020, *supra* note 164, at ¶ 23 (criticizing the Colombian Law of Transparency and the Right of Access to National Public Information as insufficiently precise); *Tshwane Principles*, *supra* note 175, Principles 2–3; *Joint Declaration on Surveillance*, *supra* note 77, at Point 12.

¹⁹⁸ Roman Zakharov, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39, at ¶ 283 (holding that the activities of surveillance oversight bodies must be open to public scrutiny); I-A SRFOE Report of 2020, *supra* note 164, at ¶ 58 (describing how the lack

assert that “the public should be fully informed” and “[i]nformation about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.”¹⁹⁹

2. Colombia’s existing legal framework regulating intelligence activities enables abusive surveillance practices in violation of the American Convention.

Colombia points to a suite of domestic laws enacted in the 2010s to argue that the State is now regulating its intelligence agencies in accordance with the American Convention.²⁰⁰ In reality, this legal framework is manifestly inadequate and highly deferential to the same agencies that have, for decades, used communications surveillance to target HRDs. Since 2013, intelligence units have continued to intercept the electronic communications of CCAJAR members with impunity. Agencies acted outside of the law and were not sufficiently restrained by the 2013 Intelligence Law which authorizes intelligence agencies to engage in EMS monitoring and to access data retained by CSPs for vague purposes and in an undefined manner, with inadequate oversight mechanisms, and allows those agencies to retain collected material for long periods of time. Inadequate laws on data protection, correction, erasure, and transfers further exacerbate the vulnerability of individuals placed under unlawful surveillance by depriving them of access to remedies. These laws impede public scrutiny by establishing anemic guarantees for the public to access information on state communications surveillance. Together, this legal framework preserves a secretive, expansive, and unaccountable surveillance state in Colombia.

- a. *The Intelligence Law gives Colombian authorities wide latitude to surveil HRDs for vague purposes, in an undefined manner, and for an indefinite period, with inadequate safeguards against abuse.*

Colombia has not argued that the surveillance of members of CCAJAR occurred within any criminal investigation process, therefore the applicable legal framework can be found in the 2013 Intelligence Law. This law regulates state surveillance activity *outside* of the context of criminal investigations.²⁰¹ The Colombian Constitution requires judicial authorization prior to

of access to information and transparency regarding state surveillance activities create barriers for state accountability); G.A. Res. 69/166, The Right to Privacy in the Digital Age (Dec. 18, 2014) (calling on states to “establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data”); *Joint Declaration on Surveillance*, *supra* note 77, at Point 12.

¹⁹⁹ *Tshwane Principles*, *supra* note 175, Principle 10(E)(3). *See also Joint Declaration on Surveillance*, *supra* note 77, at ¶ 14.

²⁰⁰ Merits Report No. 57/19, *supra* note 3, ¶¶ 28; Public Hearing in Case Members of José Alvear Restrepo Lawyers’ Collective v. Colombia Part 2, *supra* note 1, at 8:31:02-8:33:32.

²⁰¹ Though beyond the scope of this brief, the legal framework regarding the process for communication interception for the purpose of criminal investigations is also deficient. Article 15 of Colombia’s constitution requires prior judicial authorization before communications are intercepted or recorded. CONSTITUCIÓN POLÍTICA DE COLOMBIA [C.P.] art. 15, www.georgetown.edu/pdba/Constitutions/Colombia/col91.html. However, in certain circumstances, the Constitution and the CPC allow the attorney general to order interception of communications (except those of the defendant’s), for purposes of criminal investigation, and requires the prosecutor to obtain judicial authorization 36 hours after interception is carried out. *Id.* at art. 250; L. 906 art. 235-237, septiembre 1, 2004, DIARIO OFICIAL (Colom.). This exemption for prior judicial authorization weakens judicial oversight and opens the door to abuse by prosecutors. *See, e.g.,* KATITZA RODRIGUEZ, VERIDIANA ALIMONTI,

the “interception” or “recording” of communications.²⁰² While the Intelligence Law does not explicitly authorize intelligence agencies to “intercept” communications outside of the context of criminal investigations, the law exempts intelligence authorities from the requirement of prior judicial authorization and other procedural safeguards when they are monitoring the EMS or accessing data retained by CSPs. The overbreadth and vagueness of each of these surveillance activities, and the lack of safeguards constraining intelligence authorities, violate international human rights law and create ample room for abuse.

i. The vagueness and overbroad language of the Intelligence Law invites unlawful state surveillance.

The Intelligence Law fails to describe with clarity the purposes for which intelligence agencies can surveil individuals, whether through EMS monitoring or accessing data retained by CSPs. Article 4 of the Intelligence Law includes a list of purposes for which intelligence and counterintelligence activities are sanctioned, including safeguarding “the democratic regime, territorial integrity, sovereignty, security and defense of the Nation;” protecting the country and its people “against threats such as terrorism, crime, organized crime, drug trafficking, kidnapping, trafficking in arms, ammunition, explosives and other related materials, money laundering . . . ;” and protecting Colombia’s “natural resources and economic interests.”²⁰³ The law includes no further explanation of what may constitute threats, including, for example, a “national security threat,” that may justify surveillance.

While the European Court has found the term “national security” to be a sufficiently precise justification for surveillance,²⁰⁴ the I-A SR on FOE and other human rights experts have cautioned against such indeterminateness, warning that “national security reasons tend to be invoked to place human rights defenders, journalists, members of the media, and activists under surveillance.”²⁰⁵ This Court must look to the context of the Latin American region, including Colombia, and reject the dangerously permissive approach taken by the European Court. As the Inter-American Commission notes in its Merits Report, Colombian public officials, including former President Álvaro Uribe Vélez, have consistently used the pretext of national security to categorize HRDs, including members of CCAJAR, as threats.²⁰⁶ Colombian intelligence agencies have also used this as a core strategy in suppressing public dissent.²⁰⁷

This Court has repeatedly recognized the catastrophic consequences of states using the pretext of national security and the concept of “internal enemy” to target civilian populations,

NECESSARY AND PROPORTIONATE, THE STATE OF COMMUNICATION PRIVACY IN COLOMBIA 7 (2020), <https://necessaryandproportionate.org/uploads/2020-colombia-en-faq.pdf#question5>.

²⁰² C.P. art. 15.

²⁰³ L. 1621 art. 4, abril 17, 2013, DIARIO OFICIAL (Colom.) [hereinafter 2013 Intelligence Law].

²⁰⁴ Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 365 (holding that “the Court is satisfied that the said regime pursued the legitimate aims of protecting national security . . .”).

²⁰⁵ I-A SRFOE Report of 2013, *supra* note 78, at 72. *See also* OHCHR Report of 2018, *supra* note 51, at ¶ 35 (noting that “[v]ague and overbroad justifications, such as unspecific references to “national security” do not qualify as adequately clear laws.”).

²⁰⁶ Merits Report No. 57/19, *supra* note 3, at ¶¶ 64, 171.

²⁰⁷ *Id.* at ¶ 138 (observing that G-3 Special Strategic Intelligence Group worked to “monitor[] organizations and people opposed to government policies” in order to “restrict or neutralize their activities.”).

particularly human rights defenders, in Colombia²⁰⁸ and elsewhere in Latin America.²⁰⁹ Allowing intelligence agencies with broad discretionary authority, with no further guidance in the law, to determine what might constitute threats to the regime and to national security, endangers HRDs in Colombia. The Court must not countenance such a dangerous approach.

ii. The Intelligence Law has failed to prevent unlawful communication interception by intelligence agencies.

The 2013 Intelligence Law has failed to prevent Colombian intelligence agencies from engaging in communication “interception”—an activity that is not authorized outside of the criminal investigation process under Colombian law. The Colombian Constitution prohibits “interception” of private communications without prior judicial authorization.²¹⁰ The Criminal Procedure Code (CPC) enables law enforcement authorities in the course of criminal investigations to “intercept” communications, while the Intelligence Law authorizes intelligence agencies to engage in other types of surveillance—EMS monitoring and accessing subscriber information and metadata retained by CSPs.²¹¹ According to the Intelligence Law, EMS monitoring is distinct from “interception of private mobile or fixed telephone conversations, as well as private data communications,” which is not authorized by the Intelligence Law, and is instead subject to the requirements under Article 15 of the Colombian Constitution and the CPC, and can only be carried out in the framework of judicial procedures.”²¹² Simply put, the Intelligence Law does not authorize intelligence agencies to “intercept” private communications.

Nonetheless, the filings to this Court indicate that the communications of HRDs, including CCAJAR, have in fact been intercepted since 2013, when the Intelligence Law was passed.²¹³ As Colombian law does not authorize intelligence agencies to intercept communications, these actions have no basis in law, and thereby violate the principle of legality which requires any interference to human rights caused by surveillance to be carried out “in accordance with law,” and prohibits states from engaging in interferences that are not “contemplated” by law.²¹⁴

This reality also contradicts Colombia’s claims that laws enacted after the dissolution of the DAS “clearly and precisely establishes the specific circumstances in which [intelligence activities] can be authorized to guarantee that any action conforms to the principles of legality, proportionality and necessity”²¹⁵ The Intelligence Law fails to define with any clarity what constitutes EMS monitoring, stating only that “EMS monitoring” is exempt from the

²⁰⁸ See, e.g., Villamizar Durán, Inter-Am. Ct. H.R. (ser. C) No. 364, *supra* note 140, at ¶¶ 64-65; Isaza Uribe, Inter-Am. Ct. H.R. (ser. C) No. 363, *supra* note 140, at ¶¶ 127-8. Moreover, this Court has determined that greater transparency with regards to the parameters of national security doctrine is an indispensable feature of Colombia’s transition to peace. *Id.* at ¶ 207.

²⁰⁹ See *supra* note 140.

²¹⁰ C.P. art. 15.

²¹¹ 2013 Intelligence Law, *supra* note 203, arts. 17, 44.

²¹² *Id.* art. 17. As described above, the procedures for carrying out interception for the purpose of criminal investigations, which are laid out in Article 250 of the Constitution and Articles 235-237 of the CPC are also deficient. See *supra* note 201.

²¹³ See, e.g., Public Hearing in Case Members of José Alvear Restrepo Lawyers’ Collective v. Colombia Part 2, *supra* note 1, at ¶¶ 7:52:30-7:59:53.

²¹⁴ Tristán Donoso, Inter-Am. Ct. H.R. (ser. C) No. 193, *supra* note 122, at ¶¶ 76, 80.

²¹⁵ Public Hearing in Case Members of José Alvear Restrepo Lawyers’ Collective v. Colombia Part 2, *supra* note 1, at 8:32:28-8:32:49.

requirements of Article 15 of the Constitution because, the Intelligence Law self-servingly declares, “[m]onitoring does not constitute interception of communications.”²¹⁶

The Intelligence Law does not define the term “EMS monitoring,” what technology would be used to engage in “EMS monitoring,” how it is distinct from “interception,” or how it might avoid interference with private communications. In the absence of a clear definition, the HRC has cautioned that EMS monitoring under the Intelligence Law “could result in instances in which private communications conveyed via the electromagnetic spectrum are intercepted without the benefit of a rigorous assessment of the legality, necessity and proportionality of such interceptions.”²¹⁷

In reviewing the constitutional validity of this provision in 2012, the Colombian Constitutional Court interpreted EMS monitoring as an activity that “consists of carrying out a random and *indiscriminate* tracking task This implies the *incidental capture of communications in which circumstances are revealed* that make it possible to avoid attacks and control risks for the defense and security of the Nation Technically, it would be a kind of tracking of shadows, images and sounds represented in frequencies of electromagnetic radiation and radio waves.”²¹⁸ Despite acknowledging that EMS monitoring “implies the incidental capture of communications,” that are used to “reveal circumstances,” the Constitutional Court reached the inconsistent conclusion that EMS monitoring “cannot involve interception or registering private communications since this requires a judicial warrant in the cases and with the formalities provided for by law Therefore, monitoring of the electromagnetic spectrum is limited by fundamental rights and subject to the system of checks and balances set forth in the Constitution These rights cannot be violated under the pretext of conducting this activity.”²¹⁹

This Court must consider the timing of the Colombian Constitutional Court’s ruling, which was issued in 2012. This was before the Edward Snowden revelations of 2013, which revealed the pervasive state abuse of mass surveillance and intelligence-gathering capabilities in the United States and elsewhere, which in turn instigated human rights bodies to develop the standards that make up today’s core international human rights jurisprudence on intelligence and surveillance.²²⁰ These standards clarify that indiscriminate and even often “incidental” capture of communications constitute a disproportionate interference with human rights,²²¹ and international

²¹⁶ 2013 Intelligence Law, *supra* note 203, art. 17.

²¹⁷ Hum. Rts. Comm., *Concluding Observations on the Seventh Periodic Report of Colombia*, ¶ 32, U.N. Doc. CCPR/C/COL/CO/7 (Nov. 17, 2016).17, 2016). *See also* U.N. High Comm’r for Hum. Rts., *Annual Report of the United Nations High Commissioner for Human Rights on the situation of human rights in Colombia*, ¶ 84, U.N. Doc. A/HRC/34/3/Add.3 (Mar. 14, 2017) [hereinafter OHCHR Report of 2017] (emphasizing that “the Government must clarify the scope and regulation of the power to monitor the electromagnetic spectrum foreseen under the Intelligence Law . . . to ensure the legality, proportionality and necessity of data collection about individuals and public acceptance of such power”).

²¹⁸ Corte Constitucional [C.C.] [Constitutional Court], julio 12, 2012, Sentencia C-540, 3.9.17.2.3, Gaceta de la Corte Constitucional [G.C.C.] (Colom.) (emphasis added). *See also* Hum. Rts. Comm., *List of issues in relation to the seventh periodic report of Colombia: Replies of Colombia to list of issues in relation to the seventh period report of Colombia*, ¶¶ 95-96, U.N. Doc. CCPR/C/COL/Q/7/Add.1 (Aug. 18, 2016).

²¹⁹ C.C., Sentencia C-540, *supra* note 218, at 3.9.17.2.3.

²²⁰ *See, e.g.*, Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 8 (Judge Pinto de Albuquerque, partly concurring and partly dissenting opinion) (describing the “plethora of authoritative documents on bulk interception” published by the Council of Europe, European Union, U.N. Human Rights Committee, and other international human rights experts “after the Snowden scandal erupted”).

²²¹ *See supra* notes 148-155.

human rights law provides that the same protections should apply to all data, including metadata.²²² The Colombian Constitutional Court simply did not have the benefit of relying on international consensus that has developed since 2013, and which the Court must look to today.

In any case, the Constitutional Court’s reasoning is both circular (ruling that monitoring is not interception because, under the Constitution, it simply cannot be), and unworkable. The EMS carries a range of waves, including radio waves which are used to transmit communications between electronic devices, such as Wi-Fi.²²³ EMS monitoring can involve the capture, “recording, processing, and evaluation” of these waves.²²⁴ Privacy International has previously noted,

Even if one contends that the means of ‘monitoring’ the electromagnetic spectrum without violating the privacy of communications exist, they pertain to an extremely narrow set of activities such as heat detection tools, and direction-finding tools and antenna. All other forms of ‘monitoring’ the electromagnetic spectrum necessitate an interference with a communication of a type that means that it is not possible to conclude anything other than that the monitoring has resulted in the communication being intercepted.²²⁵

Neither the Intelligence Law nor the Constitutional Court’s reasoning sufficiently defines how Colombia will engage in EMS monitoring in a manner that guarantees non-interference with private communications. Indeed, the Colombian Constitutional Court itself notes that EMS monitoring could include “the incidental capture of communications.”²²⁶ It thereby fails to prevent Colombian intelligence authorities from improperly categorizing a wide range of surveillance activities as EMS monitoring to avoid the procedural safeguard required under Article 15 of the Colombian Constitution.

- iii. The Intelligence Law gives intelligence authorities ill-defined power to access metadata retained by communication service providers in violation of the principle of proportionality.

In addition to EMS monitoring, the Intelligence Law also gives authorities ill-defined power to access communications data, or “metadata,” retained by CSPs. Under Article 44 of the Intelligence Law, authorities are empowered to access the “communication history of the linked telephone subscribers, the technical identification data of the subscribers . . . as well as the location of the cells in which the terminals are located and any other information that contributes to their location.”²²⁷ The director of the intelligence agency is empowered to submit the

²²² See *infra* note 230.

²²³ Congressional Research Service, *Overview of Department of Defense Use of the Electromagnetic Spectrum 2* (2021), <https://crsreports.congress.gov/product/pdf/R/R46564/8>.

²²⁴ Ali Boyacı et al, *Monitoring, Surveillance, and Management of the Electromagnetic Spectrum: Current Issues in Electromagnetic Spectrum Monitoring*, 18 *ELECTRICA* 100, 101 (2018), <https://electricajournal.org/Content/files/sayilar/28/100-108.pdf>.

²²⁵ PRIVACY INTERNATIONAL, *THE RIGHT TO PRIVACY IN COLOMBIA*, 5, n. 13 (2016), https://privacyinternational.org/sites/default/files/2017-12/HRC_colombia.pdf.

²²⁶ C.C., Sentencia C-540, *supra* note 218, at 3.9.17.2.3.

²²⁷ 2013 Intelligence Law, *supra* note 203, art. 44.

request.²²⁸ The Intelligence Law does not clearly or precisely define what data is encompassed by the “communication history” or “identification data” of the subscribers.²²⁹ As with EMS monitoring, Article 44 of the Intelligence Law states that “interception of communications will be subject to . . . Article 15 of the Constitution and the [CPC].” However, this distinction between communication “interception” and acquisition of metadata has no basis in international human rights law. Since passage of the Intelligence Law, widespread international consensus has developed recognizing that metadata contains information that is just as sensitive as that contained in the content of communications and that intelligence agencies’ access to metadata constitutes an interference with human rights.²³⁰ By giving intelligence agencies ill-defined powers to access metadata outside of the safeguards of the Colombian Constitution, the Intelligence Law violates the principles of necessity and proportionality.

iv. The Intelligence Law fails to properly limit who may be subject to communications surveillance.

The Intelligence Law does not establish what relationship must exist between the enumerated threats that justify intelligence activities, including EMS monitoring and access to metadata retained by CSPs, and *the persons* who may be subjected to such activities.²³¹ Additionally, the Constitutional Court has interpreted EMS monitoring to involve “indiscriminate tracking” and the “incidental capture of communications.”²³² This gives insufficient guidance and risks enabling the surveillance of a broad category of individuals, many of whom may only be tangentially connected to the alleged threat, and many more who may not be connected at all. The Inter-American Commission, the CJEU, the HRC, and U.N. human rights experts have stated that mass, indiscriminate surveillance, including access to metadata retained by CSPs, is impermissible under international human rights law.²³³ Similarly, in the context of domestic surveillance, the European Court has agreed with this consensus.²³⁴ While

²²⁸ *Id.*

²²⁹ FUNDACIÓN KARISMA, UN RASTREADOR EN TU BOLSILLO: ANÁLISIS DEL SISTEMA DE REGISTRO DE CELULARES EN COLOMBIA 27 (2017), <https://nomascelusvigilados.karisma.org.co/para-leer/informe-de-investigaci%C3%B3n.html>.

²³⁰ See Escher, Inter-Am. Ct. H.R. (ser. C) No. 200, *supra* note 44, at ¶ 144 (establishing that privacy protections extend to “any element of the communication process for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls”); *I-A SRFOE Internet Standards*, *supra* note 54, at ¶ 189 (explaining that metadata, “like the information on telephone communications protected by the case law of the inter-American system, . . . is separate from the content yet still highly revelatory of personal relationships, habits and customs, preferences, lifestyles, etc.”); Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 363 (stating that “the Court is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content. It therefore considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content.”); Cases C-203/15 and C-698/15, *Tele2 v. Post-och*, *supra* note 82, at ¶ 99 (establishing that metadata “taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them In particular, that data provides the means . . . of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.”); *HRC Concluding Obs. on the U.S.*, *supra* note 39, at ¶ 22 (expressing concern regarding the adverse impact on the right to privacy caused by the collection of communications metadata and content); OHCHR Report of 2018, *supra* note 51, at ¶ 6; G.A. Res. 69/166, *supra* note 198, at 2.

²³¹ *Contra Szabo*, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 67.

²³² C.C., Sentencia C-540, *supra* note 218, at ¶ 3.9.17.2.3.

²³³ See *supra* notes 148-155.

²³⁴ *Szabo*, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 67 (expressing serious concern that domestic laws failed to require a connection between the person to be surveilled and the threat and impermissibly allowed surveillance of “indeed any

the European Court has contradicted this international consensus by permitting mass interception of foreign communications, it has nevertheless continued to underscore the importance of *some* limit on who is liable to be surveilled.²³⁵

- v. The Intelligence Law is unclear on the permitted duration of surveillance and enables data retention for excessively long periods of time.

Contrary to the requirement that laws precisely define the duration of surveillance and the length of time that collected material can be retained,²³⁶ Colombian law is unclear on the permitted duration of surveillance the Intelligence law also unclear on both of those points, violating the principles of necessity and proportionality. The European Court has noted that storage of material on an individual's private life in and of itself constitutes an interference with the right to privacy, and therefore must be limited by the principles of necessity and proportionality.²³⁷ Additionally, the European Court as well as U.N., European, Inter-American, and African human rights experts agree that the duration of retention must also be limited in accordance with the principles of necessity and proportionality.²³⁸ The Colombian Intelligence Law does not properly limit how long the agencies can retain collected material.²³⁹ Moreover, it permits agencies to keep those materials classified for thirty (30) years, which can be extended by the President alone, with no clear oversight by an independent authority, for another fifteen (15) years.²⁴⁰ The Intelligence Law also does not clearly limit the duration of surveillance.

Finally, in addition to retention of data collected by intelligence agencies, Colombian law also requires third party CSPs to indiscriminately retain metadata for long periods of time. Under Article 44 of the Intelligence Law, intelligence authorities are empowered to request metadata from CSPs for up to five years. Additionally, Article 4 of Decree 1704 of 2012 Telecommunications Regulations requires CSPs to keep their users' information – including their identity, billing address, and type of connection – up to date and store it for at least five

person” and “pav[ed] the way for the unlimited surveillance of a large number of citizens” for national security purposes); Roman Zakharov, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39, at ¶ 265 (finding that intelligence law was inadequate partly because it did “not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. As a result, courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed.”).

²³⁵ See, e.g., Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 375 (stating that U.K. bulk surveillance regime only applied to communications that were sent or received outside the U.K., restricting “albeit to a limited extent . . . the categories of people liable to have their communications intercepted”).

²³⁶ See, e.g., Ekimdzhev, App. No. 70078/12, Eur. Ct. H.R., *supra* note 120, at ¶ 305 (holding that while Bulgarian law is clear on the maximum permitted duration of surveillance, the “sheer length of that period” – two years – renders it insufficient); *id.* ¶ 329 (Bulgarian law was insufficiently clear on how evidentiary material collected through surveillance would be destroyed); *Joint Declaration on FOE*, *supra* note 149, at ¶ 8(b).

²³⁷ Rotaru, App. No. 28341/91, Eur. Ct. H.R., *supra* note 82, at ¶¶ 46-48.

²³⁸ See Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 422 (examining the duration of storage of retained material); *Joint Declaration on FOE*, *supra* note 149, at ¶ 8(b).

²³⁹ 2013 Intelligence Law, *supra* note 203, art. 33. *Contra* Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 403 (finding the U.K. surveillance regime adequate because material was generally deleted after a few months, but stating that it “would have been desirable” for this shorter retention period to be included in the legislation instead of the maximum retention period of two years).

²⁴⁰ This provision of the law has been criticized by the I-A SR on FOE for being ambiguous and disproportionate because it allows intelligence authorities to label all its documents as classified without regard to its contents, and without clear or adequate processes for classification. I-A SRFOE Report of 2020, *supra* note 164, at ¶¶ 25-27.

years.²⁴¹ Article 5 of Decree 1704 requires CSPs to furnish prosecutors in criminal matters with information “such as sectors, geographic coordinates and power, among others, that help determine the geographic location of the terminal equipment or devices involved in communication.”²⁴² Finally, Resolution 912 of 2008 require CSPs to allow the National Police (Dijin) access to users’ information, including names and identification, residence, activation date.²⁴³ Together, these laws require CSPs to retain a broad range of metadata – including users’ identity information, geolocation, and communication history – to be accessed by intelligence authorities for up to five years.

Mass, indiscriminate metadata retention is a disproportionate infringement on the right to privacy.²⁴⁴ In 2014, the CJEU examined an EU metadata retention directive’s compatibility with the EU Charter of Fundamental Rights, specifically the right to privacy.²⁴⁵ The CJEU held that the directive was incompatible with the principle of necessity because it required mass, indiscriminate metadata retention, and did not establish time-period restrictions, in addition to other limitations.²⁴⁶ The CJEU specified that the EU directive impermissibly required retention of metadata for a minimum period of six months and a maximum of 24 months, but included no distinction among the categories of metadata retained that are more or less useful, nor did it establish objective criteria to determine how long (between six months and 24 months) any particular metadata should be retained.²⁴⁷ Similarly, the HRC has established that data retention policies constitute an interference with the right to privacy and that as a general rule, states should “refrain from imposing mandatory retention of data by third parties.”²⁴⁸ By requiring mass, indiscriminate metadata retention of the entire Colombian population and by failing to include any criteria to limit the type of data retained, Colombian law violates the principles of necessity and proportionality.

- vi. The Intelligence Law exempts intelligence agencies from any meaningful process of authorization, oversight, or notification, exacerbating the threats posed by the excessive discretion delegated to those agencies.

The excessive discretion that the Intelligence Law grants to intelligence authorities in determining who, why, what, and how they can surveil, is further exacerbated by the lack of any

²⁴¹ Decree 1704 art. 4, agosto 15, 2012 DIARIO OFICIAL (Colom.).

²⁴² *Id.* art. 5.

²⁴³ Resolution 912 of 2008 Por la cual se reglamenta el suministro de información de suscriptores y usuarios autorizados para el uso de las telecomunicaciones al igual que las redes de los concesionarios y licenciatarios [Resolution 912 of 2008 By which the supply of information of subscribers and authorized users for the use of telecommunications is regulated, as well as the networks of concessionaires and licensees], Resolution 912, enero 15, 2009, DIARIO OFICIAL (Colom.).

²⁴⁴ As described above, there is international consensus that interference with metadata is as intrusive as interference with the content of communications. *See supra* note 230.

²⁴⁵ Case C-293/12, *DRI v. Minister*, *supra* note 144, at ¶ 18.

²⁴⁶ *Id.* at ¶¶ 56-59. *But see* Cases C-511/18 et al, *La Quadrature du Net*, *supra* note 151, at ¶ 139 (stating that states may require communications service providers to indiscriminately retain certain communications data for purposes of national security only if strict safeguards are met, including review by an independent authority).

²⁴⁷ Case C-293/12, *DRI v. Minister*, *supra* note 144, at ¶ 63.

²⁴⁸ *HRC Concluding Obs. on the U.S.*, *supra* note 39, at ¶ 22(d.). OHCHR Report of 2014, *supra* note 45, at ¶ 26 (stating that “[m]andatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers’ communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.”).

meaningful safeguards against abuse. Intelligence agencies routinely disregard safeguards and the law exempts certain surveillance activities (EMS monitoring and access to data retained by CSPs) undertaken by intelligence authorities from prior judicial authorization; fails to establish adequate oversight mechanisms over intelligence authorities; and promotes secrecy and lack of accountability by omitting a notification requirement.

The Intelligence Law's authorization process for intelligence activities is dangerously inadequate. Under Article 14 of the Law,

Intelligence and counterintelligence activities must be authorized by order of operations or work mission issued by the directors of the agencies, or heads or deputy heads of the unit, section or agency, according to the equivalent in each agency, and must include planning.

The level of authorization required for each operation or work mission will increase depending on its nature and possible impact, the type of objective, the level of risk for sources or agents, and the possible limitation of fundamental rights. Each body will define, in accordance with its internal structure and taking into account the criteria established in this article, who is the head or deputy head of the unit, section or agency in charge of authorization, in each case taking into account the Constitution and the Law.²⁴⁹

Likewise, when intelligence agencies seek to access metadata retained by CSPs, Article 44 of the Law simply states that “directors of the intelligence agencies, or those they delegate, will be in charge of submitting [the request for information] in writing to the telecommunications service operators.”²⁵⁰

These processes are entirely internal and do not require an authority outside of the intelligence agency to authorize surveillance activities by intelligence agencies, including EMS monitoring or accessing data held by CSPs. Instead, each agency determines for itself what level of authorization is required, depending, for example, on its own assessment of the extent to which a measure might limit fundamental rights. At no point does a judicial entity approve surveillance activities by intelligence agencies.

In the context of accessing the content of communications, in *Szabo v. Hungary*, the European Court examined the validity of an authorization process which required the intelligence agency, subordinate to the Ministry of Home Affairs, to request authorization from the Ministry of Justice. The court held that the process was inadequate, as “supervision by a political responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees.”²⁵¹ In the context of access to metadata, in *Digital Rights Ireland v. U.K.*, the CJEU determined that the EU metadata retention directive failed to provide adequate safeguards against abuse, partly because “access by the competent national authorities to the data

²⁴⁹ 2013 Intelligence Law, *supra* note 203, art. 14.

²⁵⁰ *Id.* art. 44.

²⁵¹ *Szabo*, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 77. *See also* Roman Zakharov, App. No. 47143/06, Eur. Ct. H.R., *supra* note 39, at ¶¶ 258–59 (stating that “authorising of telephone tapping by a non-judicial authority may be compatible with the Convention . . . provided that that authority is sufficiently independent from the executive . . .”).

retained [by CSPs] is not made dependent on a prior review carried out by a court or by an independent administrative body.”²⁵²

The Intelligence Law also lacks any meaningful guidance on the content of authorizations. Article 15 of the Law simply points the decision maker to the vague purposes outlined in Article 4, the principles of intelligence activities outlined in Article 5 (which lists the principles of necessity, suitability, and proportionality), and “a planning program,” which is to be established by intelligence authorities.²⁵³ The requesting authority is not required to provide a reasoned request, and the permitting authority is not required to state whether or how the surveillance measure meets the principles of legality, legitimacy, necessity, or proportionality. Nor does the law require the permitting authority to identify in its authorization who or what is to be surveilled, or for how long. Without such requirements, the law fails to ensure that the surveillance measures employed under the law comply with Inter-American jurisprudence.²⁵⁴

Aside from the failures of the authorization process, the Intelligence Law also lacks an effective, independent oversight mechanism. Articles 18–26 set out the manner of supervision over intelligence activities. Article 18 requires the various intelligence agencies to prepare a confidential annual report that verifies

the application of the principles, limits and purposes set forth in this law in the authorization and development of intelligence and counterintelligence activities; the adequacy of intelligence doctrine, procedures and methods to what is established in this law; as well as the verification of the updating, correction and removal of intelligence and counterintelligence data and files.²⁵⁵

Intelligence agencies are to submit this report to the Minister of Defense and the Legal Commission for Monitoring of Intelligence and Counterintelligence Activities (“Legal Commission”), and in some cases directly to the President.²⁵⁶ Intelligence agents are to report irregularities to the head of the intelligence agency, or to the “Head of the Office of Internal Control.”²⁵⁷ The Minister of Defense and the President are part of the executive, and therefore not independent bodies. Neither, of course, are the head of the intelligence agency itself, or the head of the office of internal control of the agency, independent from the agency.

²⁵² Case C-293/12, *DRI v. Minister*, *supra* note 144, at ¶ 62. *See also* Case C-746/18, *H. K. v. Prokuratuur*, ECLI:EU:C:2021:152, ¶¶ 26, 59 (Mar. 2, 2021) (holding that “the public prosecutor’s office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings” was not a sufficiently independent agency for the purposes of “authoris[ing] access of a public authority to traffic and location data for the purposes of a criminal investigation.”).

²⁵³ 2013 Intelligence Law, *supra* note 203, art. 15.

²⁵⁴ Escher, *Inter-Am. Ct. H.R. (ser. C) No. 200*, *supra* note 44, at ¶ 139 (requiring that “decisions adopted by domestic bodies that could affect human rights must be duly founded and justified,” specifying that the decisions “should explain the grounds on which they were based, taking into consideration the arguments and the body of evidence provided to the proceedings,” and concluding that “the judge must state his or her opinion, respecting adequate and effective guarantees against possible illegalities and arbitrariness in the procedure in question”). *See also* I-A SRFOE, *supra* note 78, at ¶ 165 (stating that judicial authorization “must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued”); Merits Report No. 57/19, *supra* note 3, at ¶¶ 308, 312 (endorsing I-A SR’s position).

²⁵⁵ 2013 Intelligence Law, *supra* note 203, art. 18.

²⁵⁶ *Id.*

²⁵⁷ *Id.* art. 18(4).

While the Legal Commission is indeed an external body made up of 8 members of parliament, four senators and four congressional representatives,²⁵⁸ its supervision powers are very limited and fail to constitute meaningful oversight. The Intelligence Law authorizes the Legal Commission to meet with military and intelligence leadership, obtain information about intelligence priorities, and issue an annual, confidential “credibility and trust study.”²⁵⁹ In violation of international standards, the Legal Commission lacks the authority or obligation to “proactively investigate and monitor the activities of those who conduct surveillance,” to “access . . . the products of surveillance,”²⁶⁰ or to publicly report its findings.²⁶¹ Thus, the only external body that has any oversight over Colombian intelligence activities is legally inadequate.

The Legal Commission is also inoperative. Although established in 2013, human rights organizations and the press have reported that the Legal Commission is effectively not functional.²⁶² In 2017, Dejusticia, Fundación Karisma, and Privacy International reported that despite “several reported cases of unlawful surveillance of communications of politicians, journalists and human rights activists” there have not been any effective investigations of these incidents.²⁶³ In May 2020, the Colombian press reported that members had not met formally or discussed intelligence issues because, according to the chair of the Commission: “[it] has not been possible to engage in substantive discussions, precisely because we have not been able to ensure [the] confidentiality [of those discussions].”²⁶⁴

Finally, the Intelligence Law does not require individuals subjected to surveillance to be notified once notice no longer jeopardizes the purpose for surveillance.²⁶⁵ A similar flaw prompted the European Court to conclude that a Hungarian intelligence law fell “short of

²⁵⁸ *Id.* art. 21.

²⁵⁹ *Id.* arts. 22(1), 23.

²⁶⁰ OHCHR Report of 2018, *supra* note 51, at ¶ 40; U.N. High Comm’r for Hum. Rts., *Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in Colombia*, ¶ 25, U.N. Doc. A/HRC/19/21/Add.3 (Jan. 31 2012) [hereinafter OHCHR Report of 2012] (stating that “[n]oteworthy challenges to the implementation of this law are the weak mandate of the congressional commission and the lack of effective internal control mechanisms.”).

²⁶¹ OHCHR Report of 2018, *supra* note 51, at ¶ 40. *See also* Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 82 (finding that a ministerial report about the functioning of the national security services falls short of adequate safeguards because it is not available to the public). As a contrast, the United Kingdom’s Investigatory Powers Commissioner’s Office (IPCO) is an independent body headed by a Commissioner, and it has the obligation to publish annual reports, including “(1) statistics on the use of investigatory powers; (2) information about the results of such use; (3) information about the operation of safeguards in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic information . . .” Investigatory Powers Act 2016, c. 25, § 234 (U.K.).

²⁶² *See* KATITZA RODRÍGUEZ PEREDA, ELECTRONIC FRONTIER FOUNDATION, *COMPARATIVE ANALYSIS OF SURVEILLANCE LAWS AND PRACTICES IN LATIN AMERICA* 98 (2016), https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016.pdf (stating that Legal Commission “is not functioning”); Juan Sebastian Lombo, *El Fantasma de la Comisión de Inteligencia*, EL ESPECTADOR (May 25, 2020), <https://www.elespectador.com/noticias/politica/el-fantasma-de-la-comision-de-inteligencia> (reporting in May 2020 that members of the Commission have not had the opportunity to formally meet).

²⁶³ DEJUSTICIA, FUNDACIÓN KARISMA AND PRIVACY INTERNATIONAL, *THE RIGHT TO PRIVACY IN COLOMBIA* STAKEHOLDER REPORT UNIVERSAL PERIODIC REVIEW 30TH SESSION – COLOMBIA, ¶ 59 (2017), <https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=5412&file=EnglishTranslation> [hereinafter STAKEHOLDER REPORT].

²⁶⁴ *El Fantasma de la Comisión de Inteligencia*, *supra* note 262.

²⁶⁵ *Contra* Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 86 (requiring notice to the persons concerned “as soon as notice can be carried out without jeopardizing the purpose of the [surveillance]. . . .”); Cases C-203/15 and C-698/15, *Tele2 v. Post-och*, *supra* note 82, at ¶ 121.

securing adequate safeguards.”²⁶⁶ There, the Court rejected the government’s argument that other legal safeguards related to “data storage, processing, and deletion” and the possibility of “individual complaints” were sufficient substitutes for this requirement.²⁶⁷ Similarly here, Colombia has a habeas data law that regulates data storage, processing, and deletion, described in greater detail in section B(2)(b)(i) below. But that law provides no protection to individuals subjected to surveillance for purposes of intelligence gathering, for reasons discussed below. In the present case, CCAJAR members were not officially notified that they had been subjects of surveillance, but instead they have found out through media reports, including one published as recently as 2020.²⁶⁸ This reporting demonstrates that in the absence of notification, the State has continued collecting and retaining sensitive information about CCAJAR members, placing their lives, and their work at risk.

b. Colombian law regulating data processing, correction, erasure, and data transfers exacerbate the risks posed to members of CCAJAR and their families.

The legal framework described above is prone to the same abuses that have for decades resulted in the surveillance of members of CCAJAR and retention of data related to their communications and personal lives for extraordinarily long periods of time. Despite repeated recommendations from the Inter-American Commission and U.N. bodies, intelligence authorities have denied CCAJAR members access to the data stored in state intelligence archives. Moreover, a process created by the 2013 Intelligence Law to purge the data collected on HRDs by unlawful surveillance activities was opaque and ineffective. Finally, inadequate safeguards against improper foreign data transfers have rendered the data that the state intelligence have collected vulnerable to global exploitation.

i. Colombian laws give HRDs no opportunity to correct or erase the data that the state has collected on them.

Under Colombian law, there are two mechanisms through which individuals can have intelligence data that the state has improperly collected on them corrected or erased. That is through the 2012 Habeas Data Law or through the National System for Purging Intelligence Archives. Both mechanisms fail to provide HRDs with adequate remedies because the former excludes any information collected for national security, intelligence, or counterintelligence purposes, and the latter lacks independence and transparency.

The Habeas Data Law regulates the ability of individuals to know, update, and correct information gathered about them, but excludes any database “whose purpose is national security and defense” or databases that contain “intelligence and counterintelligence information.”²⁶⁹ As discussed above in section B(2)(a), intelligence authorities have claimed the authority to engage

²⁶⁶ Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶ 86.

²⁶⁷ *Id.* at ¶ 87.

²⁶⁸ *Las Carpetas Secretas*, *supra* note 31.

²⁶⁹ L. 1581 art. 8(a), octubre 18, 2012, DIARIO OFICIAL (Colom.) [hereinafter 2012 Habeas Data Law]; L. 1712 art. 19(a), marzo 6, 2014, DIARIO OFICIAL p. 1 (establishing a “national defense and security” exception to the right to access information).

in surveillance for the purpose of “national security,” and subsequently to categorize retained data as classified for up to 45 years.²⁷⁰ Similarly, intelligence authorities can also claim that information obtained through such surveillance activities are deemed necessary for national security and are thereby exempt from the protections of the Habeas Data Law. This violates the widely-accepted international standard that individuals should be able to correct the information that the state has collected about them.²⁷¹ The Inter-American Commission and U.N. human rights bodies have repeatedly reminded Colombia of this requirement.²⁷² The Inter-American Commission has directed Colombia to “ensure effective access to the right to habeas data for [HRDs] so that they can have access to their data in intelligence files so as to be able to request that it be corrected, updated, or . . . removed”²⁷³

In 2010, the U.N. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism recommended that States should also be “legally required to delete or update any information that is assessed to be inaccurate . . . ,”²⁷⁴ and an independent institution should oversee the process of purging intelligence files.²⁷⁵ In 2012, the U.N. Office of the High Commissioner for Human Rights (“OHCHR”) observed that “measures must be adopted in order to comprehensively reform intelligence services and transform the institutional culture that led to the commission of human rights violations,”²⁷⁶ and urged Colombia to purge its intelligence files in manner consistent with human rights standards.²⁷⁷

Colombia has failed in this obligation. In 2013, the Intelligence Law established the Advisory Committee for Purging Intelligence Archives (“the Advisory Committee”). The Advisory Committee consisted of private and public authorities, including members from intelligence agencies.²⁷⁸ The role of the Advisory Committee was to prepare a report in which it was to recommend the criteria to retain or erase intelligence data.²⁷⁹ The OHCHR recommended that these criteria be open to public debate prior to initiating purging,²⁸⁰ but when the Advisory Committee completed its mandate, it did not make those criteria public, impeding public scrutiny over intelligence agencies’ processing of personal data, its rectification, and reparations to individuals whose personal data was unlawfully collected.²⁸¹

²⁷⁰ 2013 Intelligence Law, *supra* note 203, art. 33.

²⁷¹ *Declaration of Principles on FOE*, *supra* note 192, Principle 3; Case C-362/14, Schrems v. Data Protection, *supra* note 193, at ¶ 95; U.N. SRCTHR Report of 2010, *supra* note 2, at ¶ 37.

²⁷² Inter-Am. Comm’n H.R., *Truth, Justice and Reparation*, *supra* note 4, at ¶ 1188; OHCHR Report of 2012, *supra* note 260, at ¶ 25; U.N. High Comm’r for Hum. Rts., *Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in Colombia*, ¶ 125, U.N. Doc. A/HRC/4/48 (March 5, 2007).

²⁷³ Inter-Am. Comm’n H.R., *Chapter V: Follow-up to Recommendations Made by the IACHR in Its Country or Thematic Reports*, in *Annual Report 2018*, 579 (2018), <http://www.oas.org/en/iachr/docs/annual/2018/docs/IA2018cap.5CO-en.pdf>.

²⁷⁴ U.N. SRCTHR Report of 2010, *supra* note 2, at Practice 24.

²⁷⁵ *Id.* at Practice 25, ¶ 39.

²⁷⁶ OHCHR Report of 2012, *supra* note 260, at ¶ 26.

²⁷⁷ *Id.* at ¶ 118(e). See also Hum. Rts. Comm., *Consideration of reports submitted by States parties under article 40 of the Covenant*, ¶ 16, U.N. Doc. CCPR/C/COL/CO/6 (Aug. 4, 2020).

²⁷⁸ 2013 Intelligence Law, *supra* note 203, at art. 30.

²⁷⁹ *Id.*

²⁸⁰ OHCHR Report of 2017, *supra* note 217, at ¶ 83.

²⁸¹ STAKEHOLDER REPORT, *supra* note 263, at ¶ 74; PRIVACY INTERNATIONAL, *THE STATE OF PRIVACY IN COLOMBIA* (2019), <https://privacyinternational.org/state-privacy/58/state-privacy-colombia>. Moreover, before the the National System was established, Colombia’s military informed the Office of the High Commissioner on Human Rights that it had begun to purge its archives of information about human rights defenders and other targets of illegal surveillance, raising concerns that “evidence of human rights violations may have been erased.” OHCHR Report of 2017, *supra* note 217, at ¶ 83.

After the Advisory Committee completed its mandate, Decree 2149 of 2017 created the National System for Purging Intelligence Archives (“the National System”).²⁸² The National System established a set of “instances, activities, resources, definitions, programs, and institutions that allow for the updating, correction, or removal of intelligence files.”²⁸³ Though the Advisory Committee for Purging Intelligence Archives recommended in its report to the State that the vetting body have a “civilian character, autonomous and independent of the security agencies of the National Government,” the National System was run by state officials, including from intelligence agencies.²⁸⁴ Through its creation of a mechanism that lacks transparency and independence, Colombia has failed to fulfil its responsibility to ensure that the information gathered as a result of surveillance of CCAJAR members’ communications is erased.

ii. Colombian laws provided inadequate safeguards against improper foreign data transfers.

Information sharing itself constitutes an interference with fundamental human rights, and therefore, to be consistent with international standards, any intelligence-sharing measures must meet substantive requirements under international law, and procedural requirements to safeguard against abuse.²⁸⁵ In addition to meeting the requirements of legality, legitimacy, proportionality, and necessity, the European Court, the HRC, and human rights experts agree that intelligence sharing arrangements must be subject to effective and independent oversight mechanisms.²⁸⁶

The HRC has recognized that intelligence-sharing measures must be subject to prior judicial authorization and independent oversight.²⁸⁷ The European Court has also required: (1) that domestic law must clearly set out the circumstances under which the foreign transfer may take place, (2) that the transferring state must ensure that the receiving state has adequate

²⁸² Decree 2149, diciembre 20, 2017, DIARIO OFICIAL (Colom.)

²⁸³ *Id.* art. 2.2.3.12.1.1.

²⁸⁴ Gustavo Gallon, *Inteligencia en Beneficio del Gobierno y de Toda la Sociedad*, EL ESPECTADOR (May 6, 2020), <https://www.elespectador.com/opinion/columnistas/gustavo-gallon/inteligencia-en-beneficio-del-gobierno-y-de-toda-la-sociedad-column-918263/>.

²⁸⁵ Opinion 1/15, Draft Agreement between Canada and the European Union, ECLI:EU:C:2017:592, ¶ 125 (Jul. 26, 2017); Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 362; OHCHR Report of 2018, *supra* note 51, at ¶ 21; Hum. Rts. Comm., *Concluding Observations on the Seventh Periodic Report of Sweden*, ¶ 37, U.N. Doc. CCPR/C/SWE/CO/7 (Apr. 28, 2016).

²⁸⁶ Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 362 (establishing that the transmission of data collected through bulk interception “should also be subject to independent control.”); Szabo, App. No. 37138/14, Eur. Ct. H.R., *supra* note 128, at ¶¶ 78-79 (stating that the transfer and sharing among governments of intelligence obtained through secret surveillance required the particular attention of “external supervision and remedial measures”); Hum. Rts. Comm., *Concluding Observations on the Initial Report of Pakistan*, ¶ 35, U.N. Doc. CCPR/C/PAK/CO/1 (Aug. 23, 2017) [hereinafter *HRC Concluding Obs. on Pakistan*] (expressing concern about Pakistani law that provides for “the sharing of information and cooperation with foreign governments without judicial authorization or oversight”); *HRC Concluding Obs. on the U.K.*, *supra* note 155, at ¶ 24(c) (stating that the U.K. should “[e]nsure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases”); UN SRRP Report of 2019, *supra* note 36, at 9-10, n. 17 (encouraging states “to amend their laws to empower their independent oversight authorities to consult with other independent oversight authorities in other states, and follow up on all cases of data exchanged with another state, irrespective of whether they are located in the receiving or sending State . . .”).

²⁸⁷ *HRC Concluding Obs. on Pakistan*, *supra* note 286, at ¶ 35; *HRC Concluding Obs. on the U.K.*, *supra* note 155, at ¶ 24.

safeguards against abuse, and (3) that there are heightened safeguards with regard to the transfer of “material requiring special confidentiality,” for example journalistic content.²⁸⁸ And finally, the CJEU has recognized the importance of notifying individuals when their data is shared with foreign governments in order to ensure respect for private life.²⁸⁹

There are indications that Colombia has impermissibly shared unlawfully gathered personal information, including information related to CCAJAR, with foreign governments. Colombian laws provide Colombian authorities with excessive discretion to share information gathered through abusive communications surveillance practices.

Indeed, Colombian law and policy contains worryingly little information on how Colombia monitors and assesses the adequacy of data protection laws of other countries with which Colombia shares data. Title VIII of the Habeas Data Law governs the transfer of data to third countries. The law requires that “the transfer of personal data of any kind to countries that do not provide adequate levels of data protection is prohibited . . . ,” and invests the Superintendence of Industry and Commerce (SIC) with the authority to determine what constitutes adequacy.²⁹⁰ Yet, as described in the External Circular 005 issued by the SIC in 2017, Colombia considers that the United States, a country widely criticized for its failure to grant safeguards to foreigners’ personal data, provides adequate levels of data protection.²⁹¹ Neither the Habeas Data Law nor the Circular describe the circumstances under which the transfers may take place; require authorities to demonstrate, before sharing the data, that data sharing fulfils the principles of legality, legitimacy, necessity, proportionality; require any authorization or oversight over the data being shared; require notification of individuals who are subject to such data sharing; or provide for any remedies to those whose data has been transferred. For all of these reasons, Colombia’s laws on data sharing fail to satisfy fundamental international standards.

²⁸⁸ Big Brother Watch, App. No. 58170/13, Eur. Ct. H.R., *supra* note 123, at ¶ 362.

²⁸⁹ Opinion 1/15, *supra* note 285, at ¶ 220 (requiring the notification of individuals whose data is shared between governments).

²⁹⁰ 2012 Habeas Data Law, *supra* note 269, at ¶ 26.

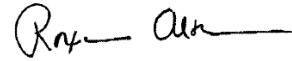
²⁹¹ Industrio y Comercio Superintendencia, *Circular Externa No. 005 [External Memorandum]*, ¶ 3.2, August 10, 2017, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Circular_Externa_5_Ago_10_2017.pdf. See DEJUSTICIA, RESPONSE TO CALL FOR INPUTS ON HUMAN RIGHTS CHALLENGES RELATING TO THE RIGHT TO PRIVACY IN THE DIGITAL AGE IN COLOMBIA 10, n. 6 (2018), <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Dejusticia.pdf> (describing the inadequacy of Colombia's standards on data transfer).

V. CONCLUSION

For the reasons stated above, amici Article 19, Electronic Frontier Foundation, Fundación Karisma, and Privacy International urge the Inter-American Court of Human Rights to find that Colombia's existing legal framework regulating intelligence activities and the unlawful and arbitrary surveillance of CCAJAR members and their families conducted by Colombian authorities violate Articles 4 (right to life), 5 (right to personal integrity), 8 (right to due process), 11 (right to privacy), 13 (right to freedom of expression and access to information), 16 (right to association), 19, (rights of the child), 22 (right to freedom of movement), and 25 (right to judicial protection) of the American Convention on Human Rights.

Date: May 24, 2022

Respectfully submitted,



Roxanna Altholz
Co-Director
International Human Rights
Law Clinic
Berkeley Law
Counsel for Amici



Astha Sharma Pokharel
Teaching Fellow
International Human Rights
Law Clinic
Berkeley Law
Counsel for Amici