PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
26th Session - Venezuela (Bolivarian Republic of)

The Right to Privacy in Venezuela (Bolivarian Republic of)

Submitted by Acceso Libre, the International Human Rights Clinic at Harvard Law School, and Privacy International

March 2016

Introduction

1. This Universal Periodic Review (UPR) stakeholder report is a submission by **Privacy International** (PI), the **International Human Rights Clinic at Harvard Law School** (IHRC), and **Acceso Libre**.

    - **PI** is a human rights organisation that works to advance and promote the right to privacy around the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

    - The **IHRC** seeks to protect and promote human rights and international humanitarian law through documentation; legal, factual, and strategic analysis; litigation before national, regional, and international bodies; treaty negotiations; and policy and advocacy initiatives. The IHRC works to protect the human rights of clients and communities around the world; through supervised practice, Harvard Law School students learn the responsibilities and skills of human rights lawyering.

    - **Acceso Libre** is a volunteer-based Venezuelan organisation devoted to the promotion and protection of human rights in the digital environment, from freedom of speech and privacy, to access to information and culture. It focuses on reporting, documenting, and educating on threats that might be affecting these rights, aiming towards policy change and legal reform.

2. Together **PI**, the **IHRC**, and **Acceso Libre** wish to bring their concerns about the protection and promotion of the right to privacy in Venezuela before the Human Rights Council for consideration in Venezuela's upcoming review. This stakeholder report highlights five areas of concern:

    - The main legislation governing communications surveillance in Venezuela falls short of international human rights standards and Venezuela's intelligence agencies, which lack independent oversight, have conducted surveillance based on political considerations.

    - Courts have relied on evidence obtained from anonymous "patriotas cooperantes" (cooperating patriots) to prosecute perceived opponents of the government, and senior government officials have used personal information

gathered by cooperating patriots to intimidate government critics and human rights defenders.

- The executive exercises significant influence over the telecommunications sector, leaving private communications and personal information at risk of illegitimate political interference.

- Mandatory SIM card registration and data retention requirements placed on telecommunications companies are measures that contravene international human rights standards on the right to privacy as they are neither necessary to achieve a legitimate aim nor proportionate to the aim pursued.

- In the absence of a robust data protection framework, the use of biometric technologies around the sale of basic goods in supermarkets and pharmacies, as well as in voting systems, creates privacy risks.

3. In its resolution on the right to privacy in the digital age, adopted by consensus on 18 December 2014, the United Nations (UN) General Assembly called on all states "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law."[1] The UPR offers a significant opportunity for states to demonstrate that they are implementing this recommendation, by systematically reviewing states' compliance with their obligations to respect and protect the right to privacy. In the first UPR cycle, there was no mention of the right to privacy in Venezuela's National Report or the Working Group report.[2]

The Right to Privacy

4. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[3] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals.[4] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[5]

1 "The right to privacy in the digital age," UN General Assembly Resolution, A/RES/69/166 (18 December 2014). The same language appears in a similar resolution passed in the 2013 General Assembly session: "The right to privacy in the digital age," UN General Assembly Resolution, A/RES/68/167 (18 December 2013).

2 National report submitted in accordance with paragraph 15 (a) of the annex to Human Rights Council resolution 5/1, Venezuela (Bolivarian Republic of), July 2011, A/HRC/WG.6/12/VEN/1; Report of the Working Group on the Universal Periodic Review, Venezuela (Bolivarian Republic of), December 2011, A/HRC/19/12.

3 Universal Declaration of Human Rights, art 12; United Nations Convention on Migrant Workers, art 14; Convention on the Rights of the Child, art 16; International Covenant on Civil and Political Rights, art 17; African Charter on the Rights and Welfare of the Child, art 10; American Convention on Human Rights, art 11; African Union Principles on Freedom of Expression, art 4; American Declaration of the Rights and Duties of Man, art 5; Arab Charter on Human Rights, art 21; European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8; Johannesburg Principles on National Security, Free Expression and Access to Information; Camden Principles on Freedom of Expression and Equality.

4 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, A/HRC/17/34.

5 See Universal Declaration of Human Rights, art 29; Human Rights Committee, General Comment No 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9; Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988; see also Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009.

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing, and sharing personal data, the right to privacy has evolved to encapsulate state obligations related to the protection of personal data.[6] A number of international instruments enshrine data protection principles, and many domestic legislatures have incorporated such principles into national law.[7]

Domestic Law on Privacy

6. The Venezuelan constitution contains several provisions aimed at guaranteeing protection and respect for the right to privacy.[8] Additionally, under Venezuela's constitution, ratified treaties have constitutional rank, elevating Article 17 of the International Covenant on Civil and Political Rights, which protects the right to privacy, to constitutional status.[9]

7. Article 48 of Venezuela's constitution provides:

> The secrecy and inviolability of private communications in all forms are guaranteed. The same may not be interfered with except by order of a competent court, with observance of applicable provisions of law and preserving the secrecy of the private issues unrelated to the pertinent proceedings.

8. Article 60 states:

> Every person is entitled to protection of his or her honour, private life, intimacy, self-image, confidentiality and reputation. The use of electronic information shall be restricted by law in order to guarantee the personal and family privacy and honour of citizens and the full exercise of their rights.

9. Venezuela lacks data protection legislation and does not have a data protection authority to investigate breaches of data protection principles and order redress. Nonetheless, decisions by the Venezuelan courts, and provisions in the Venezuelan constitution and other laws, have established some data protection principles in law. Under Article 28 of the constitution, citizens have the right to access information and data concerning them that is held by state or private entities; citizens also have the right to know the purposes for which data is collected and how it will be used. Two laws address the management and exchange of personal data between government agencies: an Act that regulates the exchange of data, information, and documents between government organs and agencies, and the Info-Government Act, which is

6 Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy).

7 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data; Guidelines for the regulation of computerized personal data files (UN General Assembly Resolution 45/95 and E/CN.4/1990/72). As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map, 8 December 2014, available at http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416.

8 Constitution of the Bolivarian Republic of Venezuela, available at http://www.cne.gob.ve/web/normativa_electoral/constitucion/indice.php; the full text of the Constitution is available in English at http://venezuela-us.org/live/wp-content/uploads/2009/08/constitucioningles.pdf. All translations from Spanish to English in this report are unofficial.

9 Ibid, art 23. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]." Human Rights Committee, General Comment No 16: Article 17 (Right to Privacy), para 1.

largely concerned with setting up mechanisms to promote effective data security in government.[10] Neither establishes a data protection regime.

10. Congressional efforts to enact a Law for the Protection of Data and Habeas Data ceased in 2005.[11] Since 2005, the legislative vacuum has been filled by the Constitutional Chamber of the Supreme Court through a series of binding decisions that have developed the right to data protection and information self-determination, as well as a procedure for individuals to obtain information the government holds about them (the habeas data procedure).[12] The Constitutional Chamber has recognised that the right to data protection "is an autonomous fundamental right … whose cardinal objective, is to allow all persons to control access and use by third parties of personal data and to prevent its use for a different purpose."[13]

11. Despite the constitutional jurisprudence in this area of law, there is major concern about recent developments in the judiciary. In a 2015 report, the International Commission of Jurists found a "profound deterioration of judicial independence" and observed that "[t]here is a clear divide between the constitutionally established responsibilities and international commitments of Venezuela and [reality]."[14] Based on surveys to assess how the general public experiences the rule of law, the World Justice Project Rule of Law Index 2015 ranked Venezuela last out of 102 countries.[15]

Areas of Concern

Surveillance Law and Practices

Legislation governing communications surveillance

12. The Law on the Protection of the Privacy of Communications is the main piece of legislation authorising communications surveillance in Venezuela.[16] Police or officials from other agencies involved in "the administration of justice" (a phrase that includes intelligence agencies) may request an authorisation from a first instance judge to "prevent, interrupt, intercept, or record communications" for the purposes of investigating specified crimes.[17] Authorisations are initially valid for no more than sixty

10 Bolivarian Republic of Venezuela, Official Gazette No 39.945, 15 June 2012 (Chapter I of Title III and Title V derogated), available at http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-sobre-Acceso-e-Intercambio-Electr%C3%B3nico-de-Datos.pdf; Bolivarian Republic of Venezuela, Official Gazette No 40.274, 17 October 2013, art 23, available at http://www.redtv.gob.ve/images/documentos/ley_infogobierno_venezuela_2013.pdf. Other laws that relate to the right to privacy include the Telecommunications' Privacy Protection Law; the Defence of Access to Goods and Services Law; the Data Messages and Electronic Signatures Law; and the Special Law on Computer Crimes. See Baker and McKenzie, Global Privacy Handbook 2013 Edition, 2013, available at http://www.bakermckenzie.com/files/Uploads/Documents/North%20America/DoingBusinessGuide/Houston/bk_globalprivacyhandbook_13.pdf. The Special Law on Computer Crimes criminalises the violation of the privacy of data or personal information incorporated in a computer system or in a system that uses information technology. Bolivarian Republic of Venezuela, Official Gazette No 37.313, October 30, 2001, arts 20-22, available at http://delitosinformaticos.com/legislacion/venezuela.shtml.

11 Privacy International, Suggestions for privacy-relevant questions to be included in the List of Issues on Venezuela, Human Rights Committee, 112th Session, 2014 available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=811&; see also Electronic Privacy Information Center, Privacy and Human Rights Report, 2006.

12 Eligio Rodríguez Marcano, "El derecho fundamental a la protección de datos de carácter personal en Venezuela y su recorrido y reconocimiento desde la Sala Constitucional del Tribunal Supremo de Justicia," Revista Latinoamericana de Proteccion de Datos Personales, 12 September 2015, available at http://www.rlpdp.com/2015/09/el-derecho-fundamental-a-la-proteccion-de-datos-de-caracter-personal-en-venezuela-y-su-recorrido-y-reconocimiento-desde-la-sala-constitucional-del-tribunal-supremo-de-justicia/.

13 Constitutional Chamber of the Supreme Court of Justice, Judgment No 1318, 4 August 2011, available at http://app.vlex.com/#vid/311569838. The Court established that the collection of information should be guided by principles such as consent, legality, accuracy, security, and confidentiality.

14 International Commission of Jurists, Venezuela: The Sunset of Rule of Law, ICJ Mission Report 2015, 2015, p 5, available at http://icj.wpengine.netdna-cdn.com/wp-content/uploads/2015/10/Venezuela-Sunset-of-Rule-of-Law-Publications-Reports-2015-ENG.pdf.

15 "WJP Rule of Law Index 2015," World Justice Project, available at http://worldjusticeproject.org/rule-of-law-index.

16 Bolivarian Republic of Venezuela, Official Gazette No 34.863, 16 December 1991, available at http://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/

17 Ibid, art 6.

days, but the judge may renew the authorisation for subsequent sixty day periods.[18] Aspects of the legislation are problematic from a human rights perspective.

13. Under international human rights standards articulated in the International Principles on the Application of Human Rights to Communications Surveillance, determinations concerning communications surveillance must be made by a competent judicial authority that is independent and impartial.[19] Although the decision to authorise communications surveillance is made by a judge, Venezuelan judges – particularly first instance judges who are often employed on temporary contracts – frequently lack independence and impartiality. In a 2015 report, Human Rights Watch considered that "the [Venezuelan] judiciary has largely ceased to function as an independent branch of government."[20]

14. International human rights standards also require that every communications surveillance determination is made on the grounds that the surveillance is necessary to achieve a legitimate aim and proportionate to the aim pursued.[21] Venezuela's legislation fails to prescribe such a test of necessity and proportionality. It allows surveillance measures to be put in place for the investigation of a range of crimes, including crimes "against the security and independence of the state," a category in the Criminal Code that encompasses offences, such as treason, that are subject to political interpretation by partisan officials.[22]

15. Additionally, according to international human rights standards, as a general matter, every person who is subject to surveillance should be notified of the decision authorising surveillance; delays may be justified only in limited circumstances, such as when notification would seriously jeopardise the purpose of the surveillance, and for a limited time, usually until the reason for the delay no longer exists.[23] However, there is no provision in the legislation requiring authorities to notify individuals or groups that they are or have been the subject of an authorisation. Best practices also highlight the importance of transparency on communications surveillance determinations, in the form of published reports containing aggregated information on authorisations, and public oversight, through independent oversight mechanisms that have the ability to hold authorities accountable.[24] It does not appear that Venezuelan law mandates transparency, nor establishes independent oversight mechanisms.

16. Finally, the legislation fails to provide sufficient clarity about the meaning of key terms. Authorities may "prevent, interrupt, intercept, or record communications," but none of these terms is defined in the legislation, generating ambiguity that creates room for abuse. For example, the term "communications" could be interpreted to exclude "metadata," which can include data such as the subject line of an email, the time it was sent, and the duration of a phone call; taken cumulatively, metadata can

18 Ibid, art 7.
19 See "Competent Judicial Authority," International Principles on the Application of Human Rights to Communications Surveillance, 2014, available at https://en.necessaryandproportionate.org/. The International Principles were developed by a range of civil society groups, as well as industry and international experts in communications surveillance law, policy, and technology. They "provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights." International Principles on the Application of Human Rights to Communications Surveillance.
20 Human Rights Watch, World Report 2015: Venezuela, 2015, available at https://www.hrw.org/world-report/2015/country-chapters/venezuela.
21 See "Legality," "Legitimate Aim," "Necessity," "Adequacy," and "Proportionality," International Principles on the Application of Human Rights to Communications Surveillance.
22 Codigo Penal, GO (5768E), arts 128-142, available at http://www.ministeriopublico.gob.ve/web/guest/codigo-penal.
23 See "User Notification," International Principles on the Application of Human Rights to Communications Surveillance.
24 See "Transparency" and "Public Oversight," International Principles on the Application of Human Rights to Communications Surveillance.

allow authorities to build comprehensive profiles of individuals and communities. The lack of precision regarding key categories of information, such as metadata, could permit state authorities to collect and analyse large amounts of personal data without breaching domestic law. The Special Rapporteur on Freedom of Expression has noted that analysis of metadata "can be both highly revelatory and invasive, particularly when data is combined and aggregated."[25]

17. The Criminal Procedure Code outlines a separate procedure for Public Prosecutors, once they have a criminal case in hand, to seek authorisation from a judge for "the interception or recording of private communications."[26] The maximum duration of surveillance under the Code is set at 30 days. Another law, the Law against Organised Crime and the Financing of Terrorism, allows judges to authorise the interception of phone calls for the purposes of criminal investigations concerning organised crime or the financing of terrorism.[27] This law also states that private telephone companies are required to allow investigators to use their facilities for investigations related to these crimes.[28] It is unclear how these separate interception regimes relate to the general scheme contained in the Law on the Protection of the Privacy of Communications.

Surveillance by intelligence agencies

18. Venezuela's intelligence agencies engage in surveillance practices that violate international human rights standards, as they appear to conduct surveillance based on political considerations and without any independent oversight. Additionally, the mandates of intelligence agencies are largely contained in executive decrees, law that is made exclusively by the President without passing through the National Assembly, Venezuela's parliament.

19. Major intelligence agencies in Venezuela include the General Directorate of Military Intelligence, the Bolivarian National Intelligence Service, and the Strategic Centre for Security and Homeland Protection.[29] These agencies, whose specific mandates and functions frequently change, are collectively tasked with undertaking intelligence-gathering activities for law enforcement and national security purposes, and answer generally to the executive.

<u>General Directorate of Military Intelligence and Counterintelligence</u>

20. The General Directorate of Military Intelligence and Counterintelligence (the General Directorate) has a wide mandate to undertake counterintelligence operations to prevent enemy espionage and intelligence-gathering activities.[30] It also conducts investigations into perceived threats against the President, who is the Commander in Chief of Venezuela's armed forces. Any perceived threats to the military or government are likely targets for surveillance; for example, the General Directorate raided the house of opposition leader Leopoldo López, and that of his parents, in 2014.[31]

25 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, April 2013, A/HRC/23/40, para 15, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

26 Bolivarian Republic of Venezuela, Official Gazette No 6.078, 15 June 2012, arts 204-207, available at: http://www.mp.gob.ve/LEYES/CODIGO_OPP/index.html.

27 Bolivarian Republic of Venezuela, Official Gazette No 39.912, 30 April 2012, available at http://www.oas.org/juridico/PDFs/mesicic4_ven_ley_del_org_finan_terr.pdf.

28 Ibid, art 65.

29 In Spanish: Dirección General de Contrainteligencia Militar, Servicio Bolivariano de Inteligencia Nacional (SEBIN), y Centro

30 Estratégico de Seguridad y Protección de la Patria (CESPPA).
See "Organizacion," Dirección General de Contrainteligencia Militar, available at http://dgim.mil.ve.

31 "Allanan la residencia de Leopoldo López y la de sus padres," Informe21, 16 February 2014, available at http://informe21.com/leopoldo-lopez/allanan-residencia-de-los-padres-de-leopoldo-lopez.

21. The legal framework governing the General Directorate comprises "rules of procedure" issued by executive decree that give the agency broad, insufficiently defined, powers. The rules of procedure state that the Directorate must "discover, prevent, and put down enemy activity," but do not specify the methods the Directorate may use to pursue these goals.[32] The Venezuelan non-governmental organisation Control Ciudadano has suggested that the military intelligence apparatus "clearly resembles that of Latin American military dictatorships, especially those that operated during the life of the so-called doctrine of national security, [an apparatus] characterised by directly depending on the [President's orders] to conduct intelligence and counterintelligence operations, with virtually unlimited and uncontrolled powers."[33]

22. The legal basis of the General Directorate's rules of procedure is controversial. In February 2015, the President issued an executive decree to approve the rules; by issuing an executive decree, he bypassed the need for approval from the National Assembly, allowing him to dictate the rules according to his preferences.[34] Control Ciudadano has argued that the rules of procedure should have been established in a law passed by the National Assembly, rather than issued directly by the President, so that they could be subjected to legislative scrutiny.[35] Any law in Venezuela, including an executive decree, may only be struck down by the nation's highest court, the Supreme Tribunal of Justice; however, that Court rarely rules against the government. (In individual cases, a lower court can declare that a provision does not apply in the particular circumstances of the case, if the court finds a breach of constitutional rights.)

Bolivarian National Intelligence Service (SEBIN)

23. The Bolivarian National Intelligence Service (SEBIN) is a civilian rather than a military agency and is located within the Ministry of the People's Power for the Interior, Justice, and Peace. The SEBIN's purpose is "to implement policies and actions on civil intelligence and counterintelligence" and its functions include: to advise the President, cabinet, and other senior officials on the formulation of national security polices; to contribute to the detection of external and internal threats; and to help other agencies combat organised crime.[36] In 2010, the SEBIN was created through an executive decree out of a previous intelligence agency that had similar functions (the National Directorate of Intelligence and Prevention Services).[37] Although the SEBIN officially reports to the Vice-President, the President seems to exercise significant power over the institution.[38] For example, the President personally promoted several people within

32 Rules of Procedure of the General Directorate of Military Intelligence and Counterintelligence, Decree No 1.605, Bolivarian Republic of Venezuela, Official Gazette No 40.599, 10 February 2015, available at http://www.mp.gob.ve/c/document_library/get_file?p_l_id=29950&folderId=6936036&name=DLFE-8609.pdf.

33 "Comunicado: Maduro oficializa figura del 'enemigo' con reforma de inteligencia military," Asociación Civil Control Ciudadano, 18 February 2015, available at http://www.controlciudadano.org/noticias/detalle.php?notid=12669.

34 Rules of Procedure of the General Directorate of Military Intelligence and Counterintelligence; see "Gaceta N° 40.599: Dictan Reglamento Orgánico de la Dirección General de Contrainteligencia Militar," Finanzas Digital, 11 February 2015, available at http://www.finanzasdigital.com/2015/02/gaceta-n-40-599-dictan-reglamento-organico-de-la-direccion-general-de-contrainteligencia-militar/.

35 "Comunicado: Maduro oficializa figura del 'enemigo' con reforma de inteligencia military," Asociación Civil Control Ciudadano, 18 February 2015.

36 Decree No 7.453, Bolivarian Republic of Venezuela, Official Gazette No 39.436, 1 June 2010, available at http://www.gacetaoficialdelarepublicabolivarianadevenezuela.com/descarga/40616.pdf.

37 Ibid

38 SEBIN is the Vice-President's responsibility according to Decree No 9.308, Bolivarian Republic of Venezuela, Official Gazette No 40.066, 6 December 2012, available at http://www.mp.gob.ve/c/document_library/get_file?p_l_id=40497&folderId=1754678&name=DLFE-5815.pdf.

the agency in 2015.[39] Civil society groups have accused the SEBIN of aggressive and illegal surveillance practices.[40]

24. The SEBIN is known to put individuals under surveillance for political reasons, in violation of international human rights standards that require every surveillance decision to be based on an assessment of necessity and proportionality.[41] In 2015, US President Barack Obama issued an executive order imposing sanctions on Gustavo González López, the head of the SEBIN, for human rights violations; the White House noted that González López "was associated with the surveillance of Venezuelan government opposition leaders."[42] For example, in 2015, opposition politician Maria Corina Machado reported that she was followed by twelve SEBIN agents for two days [43]. Following the 2013 publication of a cache of documents attributed to the SEBIN by Analisis24 (a right-leaning Argentinean news website), Jewish groups have alleged that the SEBIN targets surveillance at the Jewish community in particular.[44]

Strategic Centre for Security and Homeland Protection (CESPPA)

25. The Strategic Centre for Security and Homeland Protection (CESPPA) was established in 2013 through an executive decree and performs both intelligence and law enforcement functions.[45] Gustavo Gonzalez Lopez, the head of the SEBIN, is also the head of the CESPPA. The CESPPA is responsible for collecting and organising information "of strategic interest" to the nation, for the purposes of national security.[46] It also provides direction to other intelligence agencies, including the SEBIN, regarding the status of information: it decides what information should be classified secret, what should be available to the public, and what constitutes a threat to the state.[47] Civil society groups have raised concerns that the CESPPA's creation has increased the state's surveillance capabilities and limited Venezuelans' access to information.[48] The CESPPA is believed to monitor and analyse social media posts in particular.[49]

Surveillance capabilities

26. CitizenLab, an interdisciplinary laboratory at the University of Toronto, has found evidence to suggest that FinFisher, an advanced spyware program sold exclusively

39 "Maduro anunció que condecorará a funcionarios del Sebin y del Cicpc," NTN 24, 13 June 2015, available at http://www.noticias24.com/venezuela/noticia/286516/maduro-anuncio-que-condecorara-a-funcionarios-del-sebin-y-al-cicpc/.

40 See Fabiola Zerpa, "Abran la puerta, es el Sebin," El Nacional, 18 May 2014, available at http://www.el-nacional.com/siete_dias/ARELLANO-DARIO-FUNCIONARIOS-GLIDIS-SEBIN_0_409759164.html; Sandra Benitez, "Spying in Venezuela through Social Networks and Emails," in GISWatch, Communications Surveillance in the Digital Age, 2014, available at http://giswatch.org/en/country-report/communications-surveillance/venezuela.

41 See International Principles on the Application of Human Rights to Communications Surveillance.

42 "Fact sheet: Venezuela Executive Order," The White House, 9 March 2015, available at https://www.whitehouse.gov/the-press-office/2015/03/09/fact-sheet-venezuela-executive-order.

43 "María Corina Machado denuncia persecución del Sebin," El Estímulo, 18 April 2015, available at http://elestimulo.com/blog/maria-corina-machado-denuncia-persecucion-del-sebin/.

44 Gil Shefler, "Documents show Venezuela spying on Jewish Community," Jewish Telegraphic Agency, 4 February 2013, available at http://www.jta.org/2013/02/04/news-opinion/world/documents-show-venezuela-spying-on-jewish-community; see "La Comunidad judía venezolana es espiada por el Sebin,"La Patilla, 25 January 2013, available at http://www.lapatilla.com/site/2013/01/25/la-comunidad-judia-venezolana-es-espiada-por-el-sebin/.

45 Decree 458, Bolivarian Republic of Venezuela, Official Gazette No 40.266, 7 October 2013, available at http://www.mp.gob.ve/c/document_library/get_file?p_l_id=40497&folderId=3207227&name=DLFE-7417.pdf; see also Tamara Pearson, "Opposition Use Presidential Security Decree to Label Venezuelan Government 'Dictatorial'" Venezuelanalysis.com, 22 October 2013, available at http://venezuelanalysis.com/news/10111.

46 Decree 458, 2013, art 8. See also Resolution by which the internal rules of CESPPA are dictated, Bolivarian Republic of Venezuela, Official Gazette No 40.355, 13 February 2014, available at http://www.mp.gob.ve/c/document_library/get_file?p_l_id=29938&folderId=3986195&name=DLFE-7613.pdf.

47 Decree 458, 2013.

48 Edgar López, "Con el Cesppa el gobierno podrá vigilar sin límites," El Nacional, 15 February 2014, available at http://www.el-nacional.com/politica/Cesppa-gobierno-podra-vigilar-limites_0_355764628.html; Silvia Higuera, "New Intelligence Body in Venezuela could put Access to Information at Risk," Journalism in the Americas Blog: The University of Texas at Austin, 16 October 2013, available at: https://knightcenter.utexas.edu/blog/00-14607-new-intelligence-body-venezuela-could-put-access-information-risk.

49 Sandra Benitez, "Spying in Venezuela through Social Networks and Emails," in Communications Surveillance in the Digital Age.

to governments, has been used in Venezuela since at least December 2014[50]. The program relies on a network of disguised servers to collect information from targets, while concealing the location of those actually receiving the collected information. Although FinFisher has been marketed as a legitimate crime-fighting tool, international experience suggests that it can be used in contravention of international human rights standards.[51] Venezuela is also believed to be a client of Blue Coat Systems, a company with links to the surveillance programs of many oppressive regimes.[52] However, there is no information indicating which bodies may have purchased or use these technologies in Venezuela.

"Patriotas Cooperantes" (Cooperating Patriots)

27. "Cooperating patriots" are "alleged informants who, on condition of anonymity, 'cooperate' with investigative authorities, denouncing those who they believe are committing crimes that they claim could affect the stability of state institutions."[53] In some cases, information from cooperating patriots has been admitted in court to support prosecutions of political opponents of the government.[54] In other cases, cooperating patriots act as informants for intelligence agencies, or pass on information to government officials.[55] The information cooperating patriots provide is often of a private nature, concerning private discussions between individuals or details about individuals' private lives.[56] Although the term "cooperating patriots" does not appear in Venezuelan law, government officials encourage Venezuelans to become cooperating patriots. For example, in August 2015, President Nicolás Maduro urged Venezuelans to "turn into millions of cooperating patriots to guarantee the peace and stability of the country."[57]

28. In January 2016, Reuters reported that in the three years since President Maduro came to power, cooperating patriots have "taken an increasingly important role in providing information that leads to arrests of government foes."[58] According to Reuters' investigation, since early 2014, evidence from anonymous cooperating patriots has been produced in at least 20 court cases, potentially in violation of Venezuelan law, which requires the person making an accusation to be identified.[59] In a striking example of this practice, Reuters describes the case of Rodolfo Gonzalez: in April 2014, Gonzalez was arrested by intelligence agents who accused him of masterminding protests against President Maduro; he was arrested because a cooperating patriot allegedly provided the intelligence services with an audio recording in which Gonzalez

50 Bill Marczak et al, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," CitizenLab, 15 October 2015, available at https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/.
51 Ibid.
52 Morgan Marquis-Boire et al, "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," CitizenLab, 15 January 2013, available at https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.
53 "Sin nombre y sin ley," El Universal, 29 March 2015, available at: http://www.eluniversal.com/nacional-y-politica/150329/sin-nombre-y-sin-ley; see also John Manuel Silva, "Patriotas cooperantes: los sapos de la revolución," El Estímulo, 1 July 2015, available at http://elestimulo.com/climax/patriotas-cooperantes-los-sapos-de-la-revolucion/.
54 Ibid.
55 Ibid.
56 Ibid.
57 Quoted in "Maduro: Estas serán las elecciones más difíciles que hemos enfrentado," Mundo24, 4 August 2015, available at http://mundo24.net/tiembla-el-regimen-maduro-estas-seran-las-elecciones-mas-dificiles-que-hemos-enfrentado and Diego Oré, "Venezuela's state informers: patriots or snitches?" Reuters, 29 January 2016, available at http://www.reuters.com/article/us-venezuela-informers-insight-idUSKCN0V71CT.
58 Diego Oré, "Venezuela's state informers: patriots or snitches?" Reuters, 29 January 2016; Diego Oré, "'Patriotas cooperantes': ¿soplones o guardianes de la revolución bolivariana en Venezuela?" infobae, 29 January 2016, available at http://www.infobae.com/2016/01/29/1786443-patriotas-cooperantes-soplones-o-guardianes-la-revolucion-bolivariana-venezuela (longer version of Reuters article, in Spanish).
59 See Law on the Protection of Victims, Witnesses and other persons participating in criminal investigations, Bolivarian Republic of Venezuela, Official Gazette No 38.536, 4 October 2006. Diego Oré, "Venezuela's state informers: patriots or snitches?" Reuters, 29 January 2016; Diego Oré, "'Patriotas cooperantes': ¿soplones o guardianes de la revolución bolivariana en Venezuela?" infobae, 29 January 2016.

discussed "destabilising actions" against the government.[60] For nearly a year, Gonzalez was held in a facility operated by the SEBIN while he waited for trial; he hanged himself in March 2015[61]. His daughter told Reuters, "[I]f you begin to suspect that anything you say can result in an accusation, you will not march or protest, or even talk with a neighbour."[62]

29. Senior government officials use private information allegedly obtained from cooperating patriots to publicly attack opponents and human rights defenders. Diosdado Cabello, who was the President of the National Assembly until January 2016, is the presenter of a popular television program, Con el Mazo Dando, that airs on state television; during the program he frequently makes reference to information provided by cooperating patriots.[63] For example, in nine episodes aired from October to December 2014, Cabello used information allegedly provided by cooperating patriots to publicly accuse 165 individuals and organisations of various crimes.[64] The information Cabello broadcasts is usually of a private nature: it generally includes details about places human rights defenders or opposition politicians have visited, photos, and travel schedules. This information is also published on the program's website.[65] In April 2015, citing the example of Cabello's television program and his use of information from cooperating patriots, a large group of NGOs, including Amnesty International and Human Rights Watch, called on Venezuela to cease "intimidating and harassing human rights defenders, and making unsubstantiated allegations that they are seeking to undermine Venezuelan democracy."[66]

30. Senior government officials have also broadcast recordings of private conversations involving their political opponents, without specifying how they obtained these recordings. In October 2015, during an episode of Con el Mazo Dando, Cabello played a recording of a private conversation between Lorenzo Mendoza, President of Empresas Polar, the largest privately-owned company in Venezuela, and Ricardo Hausmann, Director of the Center for International Development at Harvard Kennedy School, in which the two discussed Venezuela's economic situation and the International Monetary Fund.[67] Subsequently, based on this conversation, 101 government members of the National Assembly filed a criminal complaint against Mendoza and Hausmann for abuse of power, treason, and conspiracy.[68] In 2013, the Minister of Telecommunications, Ernesto Villegas, and the Mayor of Caracas, Jorge Rodriguez, broadcast an edited version of a private conversation between opposition parliamentarian Maria Corina Machado and professor German Carrera Damas.[69]

60 Diego Oré, "Venezuela's state informers: patriots or snitches?" Reuters, 29 January 2016; Diego Oré, "'Patriotas cooperantes': ¿soplones o guardianes de la revolución bolivariana en Venezuela?" infobae, 29 January 2016.
61 Ibid.
62 Quoted in Diego Oré, "'Patriotas cooperantes': ¿soplones o guardianes de la revolución bolivariana en Venezuela?" infobae, 29 January 2016.
63 The phrase "con el mazo dando" is idiomatic. Literally, it can be translated as "hitting with the mallet," but it is part of a longer expression ("a Dios rogando y con el mazo dando") that is usually translated as "God helps those who help themselves."
64 "Caracas: Directores de ONG denunciaron en Fiscalía intervención ilegal de sus comunicaciones," Instituto Prensa y Sociedad Venezuela, 27 May 2015, available at http://ipysvenezuela.org/alerta/caracas-directores-de-ong-denunciaron-en-fiscalia-intervencion-ilegal-de-sus-comunicaciones/.
65 See, for example "Con el Mazo dando, ¿Defensores de derechos humanos o del imperio?" Con el Mazo Dando, 21 October 2015, available at http://www.conelmazodando.com.ve/defensores-de-derechos-humanos-o-del-imperio/.
66 "Venezuela: Stop Harassing Human Rights Defenders: Intimidation Undermines Independent Oversight," 7 April 2015, available at https://www.fidh.org/en/region/americas/venezuela/venezuela-stop-harassing-human-rights-defenders-intimidation; see also "IACHR Expresses Alarm over Intimidation in Venezuela directed against People Who Come before the Inter-American Human Rights System," Inter-American Commission on Human Rights, press release, 20 March 2015, available at http://www.oas.org/en/iachr/media_center/PReleases/2015/032.asp.
67 "Lorenzo Mendoza y Ricardo Haussman se cayeron con 60 mil millones de kilos," Con el Mazo Dando,15 October 2015, available at http://www.conelmazodando.com.ve/lorenzo-mendoza-y-ricardo-haussman-se-cayeron-con-60-mil-millones-de-kilos/.
68 "Denuncian por tres delitos a Lorenzo Mendoza y Ricardo Hausmann," Runrun.es, 21 October 2015, available at http://runrun.es/nacional/231171/denuncian-por-tres-delitos-a-lorenzo-mendoza-y-ricardo-hausmann.html; "AN pide investigar a Mendoza por delitos contra la soberanía, la seguridad y por usurpación," VTV, 21 October 2015, available at http://www.vtv.gob.ve/articulos/2015/10/21/an-pide-investigar-a-lorenzo-mendoza-por-delitos-contra-la-soberania-la-seguridad-y-usurpacion-6340.html.
69 "Espiar teléfonos: Una práctica ilegal que no hace cualquiera," La Razón, 7 July 2015, available at http://www.larazon.net/2015/07/07/espiar-celulares-una-practica-ilegal-que-no-hace-cualquiera/; See also "Transcripción completa del audio de María Corina Machado," PSUV, 26 June 2013, available at http://www.psuv.org.ve/temas/noticias/transcripcion-completa-audio-maria-corina-machado/#.VpR3LZMrLFQ

Executive Influence over the Telecommunications Industry

31. The executive exercises broad control over the telecommunications industry through the state-run National Telecommunications Commission of Venezuela (CONATEL). There is a general perception in Venezuelan society that CONATEL has supported the monitoring of private communications and the persecution of internet users who express dissenting opinions online.[70] Users of social networks have accused CONATEL of monitoring their online activity and passing identifying information along to intelligence agencies, such as the SEBIN.[71] In 2014 SEBIN authorities detained at least eight Twitter users under public incitement charges.[72] (Some of the users allegedly published comments on their Twitter accounts about the murder of a government party parliamentarian.) According to leaked documents, CONATEL provided information to the SEBIN, including IP addresses, that assisted the authorities in locating the users.[73]

32. CONATEL has a legal mandate to require online media outlets and internet service providers to establish mechanisms "to restrict, without delay, the dissemination of messages prohibited under [the relevant law]" and sanction those who do not comply.[74] Prohibited messages include those that "generate anxiety in the population or disturb public order" or "do not recognise legitimately constituted authorities," vague phrases that permit CONATEL to impose significant restrictions on media outlets and internet service providers.[75] Moreover, the ability of the President, in conjunction with senior officials, to appoint or remove members of CONATEL's governing body, together with the fact that the agency is overseen by the Ministry of Popular Power in Communication and Information, which is also controlled by the President and his senior officials, raises concerns about CONATEL's ability to act independently.[76] In 2014, the government established a Vice-Ministry of Social Networks to regulate and monitor social media, thus further extending its control of the internet.[77]

SIM Card Registration and Data Retention Requirements

33. Compulsory SIM card registration and the retention of information about mobile phone users in a centralised database threaten the right to privacy in Venezuela. SIM

70 See Marianne Díaz Hernández, "Documenting Internet blocking in Venezuela," Digital Rights, 24 October 2014, available at http://www.digitalrightslac.net/en/documentando-los-bloqueos-a-internet-en-venezuela/.

71 Ellery Roberts Biddle et al, "Netizen Report: Leaked Documents Reveal Egregious Abuse of Power by Venezuela in Twitter Arrests," Global Voices, 15 July 2015, available at https://advox.globalvoices.org/2015/07/15/netizen-report-leaked-documents-reveal-egregious-abuse-of-power-by-venezuela-in-twitter-arrests/; see also Jesus Alberto Yajure "@Conatel elaboró informes para el @SEBIN_OFICIAL sobre tuiteros detenidos," Runrun.es, 3 July 2015, available at http://runrun.es/rr-es-plus/210909/conatel-elaboro-informes-para-el-sebin_oficial-sobre-tuiteros-detenidos.html.

72 "Venezuela Twitter Crackdown: HRF Condemns Targeted Data Collection by Political Police," Human Rights Foundation, 17 July 2015, available at http://humanrightsfoundation.org/news/venezuela-twitter-crackdown-hrf-condemns-targeted-data-collection-by-political-police-00445.

73 Ellery Roberts Biddle et al, "Netizen Report: Leaked Documents Reveal Egregious Abuse of Power by Venezuela in Twitter Arrests," Global Voices, 15 July 2015; see also Jesus Alberto Yajure "@Conatel elaboró informes para el @SEBIN_OFICIAL sobre tuiteros detenidos," Runrun.es, 3 July 2015. The Director of CONATEL has asserted that the state does not persecute Twitter users: "Director de Conatel dice que el Gobierno no persigue tuiteros," La Patilla, 6 July 2015, available at http://www.lapatilla.com/site/2015/07/06/director-de-conatel-dice-que-el-gobierno-no-persigue-tuiteros/.

74 Law on Social Responsibility in Radio, Television, and Electronic Media, Bolivarian Republic of Venezuela, Official Gazzete No 39.610, 7 February 2011, art 27, available at http://www.conatel.gob.ve/ley-de-responsabilidad-social-en-radio-television-y-medios-electronicos/; see Article 19, Venezuela: Law on Social Responsibility of Radio, Television and Electronic Media, December 2011, available at https://www.article19.org/data/files/medialibrary/2894/11-12-09-ANAL-Venezuela.pdf.

75 Law on Social Responsibility in Radio, Television, and Electronic Media, art 27. Under that law, CONATEL can sanction or initiate administrative proceedings against companies it considers are breaching the law. For commentary on an earlier version of the law (the Law on Social Responsibility on Radio and Television), see Inter-American Commission on Human Rights, Democracy and Human Rights in Venezuela, December 2009, /Ser.L/V/II. Doc. 54 OEA, available at http://www.cidh.oas.org/countryrep/Venezuela2009eng/VE09CHAPIVENG.htm.

76 Organic Law of Telecommunications, Bolivarian Republic of Venezuela, Official Gazette No 39.610, 7 February 2011, arts 39-40; see Article 19, Venezuela: Law on Social Responsibility of Radio, Television and Electronic Media, December 2011.

77 Bolivarian Republic of Venezuela, Official Gazette No 40.435, 6 November 2014; "Gobierno crea viceministerio para Redes Sociales," Ultimas Noticias, 1 December 2014, available at http://www.ultimasnoticias.com.ve/noticias/actualidad/politica/gobierno-crea-viceministerio-para-redes-sociales.aspx; "Designaron as Jessenia Moniz como nueva Viceministra de Redes Sociales," El Universal, 7 November 2014, available at http://www.eluniversal.com/nacional-y-politica/141107/designaron-a-jessenia-moniz-como-nueva-viceministra-de-redes-sociales.

card registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups in a society.[78] It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilities surveillance and makes tracking and monitoring of users easier for authorities, concerns that are especially acute in countries with conflict, political instability, and civil society suppression. Meanwhile, placing extensive mandatory data retention requirements on telephone companies contravenes international human rights standards; mandatory and indiscriminate retention of communications data is a serious interference with the right to privacy that goes beyond what is strictly necessary to respond to legitimate law enforcement needs.[79]

34. Under Venezuelan law, when a person wishes to buy a prepaid SIM card or take out a contract for mobile services, the telecommunications company selling the service must collect a copy of the individual's passport or identity card, take prints of the individual's right index finger and thumb, obtain a signature, and record the individual's address.[80] Venezuelan law requires the company to create an electronic registry containing this information about all its customers; the company must retain information about each customer for the period the customer receives the service and for three months after the customer terminates the service.[81]

35. Companies must also maintain a detailed register of all phone calls made through their networks: the register must contain information such as the numbers involved in a call, the geographic location of callers, and the time, date, and duration of the call.[82] Companies must retain this information for twelve months.[83] The relevant law refers to state security agencies that have research or investigation powers being able to request information from call registries that "[contributes] to investigations that are carried out within the scope of [the agency's] tasks in accordance with the law" and the law requires companies to provide information from their registries on request and without delay.[84] However, the law does not set out a process for requesting information and it is unclear if state security agencies consider that Venezuelan law governing search and seizure procedures requires them to seek a court order to obtain the information.

Biometric Technologies and Other Emerging Initiatives

36. Venezuela has put in place systems to collect and retain biometric data in voting processes and to control sales of basic goods, generating risks to Venezuelans' privacy. Biometric technologies are used to confirm identity by capturing and storing individuals' unique or distinctive physical, biological, or behavioural characteristics.[85] International experience suggests that there are a number of privacy risks surrounding

78 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 2013, para 70; see also Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, May 2015, A/HRC/29/32, para 51.

79 The right to privacy in the digital age, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, 2014, A/HRC/27/37, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; see also Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014.

80 CONATEL, Providence No 572, Official Gazette No 38.157, 1 April 2005, available at http://www.conatel.gob.ve/providencia-administrativa-572-normas-relativas-al-requerimiento-de-informacion-en-el-servicio-de-telefonia-movil-ano-2005/.

81 Ibid, arts 4 and 6.

82 Ibid, art 7.

83 Ibid

84 Ibid, arts 6 and 7.

85 Privacy International, Biometrics: Friend or foe of privacy?, 2014, p 4, available at https://www.privacyinternational.org/sites/default/files/Biometrics_Friend_or_foe.pdf; see also "Biometrics," Privacy International, available at https://www.privacyinternational.org/node/70.

their use: the unregulated retention of biometric data raises the possibility of "function creep" (use of the data for purposes other than those for which it was collected); the mere existence of a database of biometric data could lead to the development of new justifications for its use beyond the original purposes for which consent was given by the individual whose data was collected; the general storage of data renders it vulnerable to theft; and biometric technologies may also be prone to errors (for example, the system may not accurately capture an individual's biometrics in every case).[86]

37. The lack of clear data protection standards and appropriate safeguards around Venezuela's biometric systems exposes Venezuelans to risks of profiling, surveillance, and discrimination. Additionally, in the absence of a comprehensive framework that regulates the enforcement of data protection principles, it is difficult for Venezuelans to obtain information about how their personal data is used and seek redress for breaches of data protection principles.

38. Since 2014, the Venezuelan government has required state-owned and private stores to install biometric equipment and collect customers' biometric information in an effort to address food shortages and prevent smuggling.[87] Whenever a Venezuelan wishes to buy an item from a list of basic priced-controlled goods – which includes rice, flour, milk, and toilet paper – they go to the store (on a day of the week assigned to them according to their identity card number), place their right thumb on a scanner, and buy the item. The biometric system was initially implemented on a voluntary basis in state-run supermarkets, but became mandatory for all state-owned and private supermarkets, as well as pharmacies, in mid-2014.[88] There is little public information on who manages and has access to the data collected and under what circumstances, for what purpose data is used, and for how long it is retained.

39. Biometric technologies are also used in elections: when Venezuelans vote in elections, officials from the National Electoral Power (CNE) scan each voter's right thumb to authenticate their identity.[89] Many Venezuelans are sceptical about the government's claim that the biometric scanners used in supermarkets and pharmacies are different from those used for voting, heightening distrust in biometric technologies and the voting system.[90]

40. Emerging government initiatives that entail the collection of significant amounts of personal information also raise privacy concerns because of the lack of a robust data protection regime and other safeguards to protect privacy. Emerging initiatives

86 Privacy International, Biometrics: Friend or foe of privacy?, 2014, p 4, available at https://www.privacyinternational.org/sites/default/files/Biometrics_Friend_or_foe.pdf; see also "Biometrics," Privacy International, available at https://www.privacyinternational.org/node/70.

87 "Captahuellas en supermercados identifican bachaqueros," El Nacional, 14 September 2015, available at http://www.el-nacional.com/sociedad/Captahuellas-supermercados-rebotan-bachaqueros_0_701929936.html; Marianne Diaz, "Tu huella digital por un kilo de harina: biométrica y privacidad en Venezuela," Digital Rights Latin America & the Caribbean,16 December 2015, available at http://www.digitalrightslac.net/es/tu-huella-digital-por-un-kilo-de-harina-biometrica-y-privacidad-en-venezuela/.

88 Virginia López, "Venezuela to introduce new biometric card in bid to target food smuggling," The Guardian, 21 August 2014, available at http://www.theguardian.com/world/2014/aug/21/biometric-venezuela-food-shortages-smuggling-fingerprints; "Venezuela implementará sistema biométrico para el control de venta de alimentos," CNN, 21 August 2014, available at http://cnnespanol.cnn.com/2014/08/21/venezuela-implementara-sistema-biometrico-para-el-control-de-venta-de-alimentos/.

89 "Electoral Technology in Venezuela," National Electoral Power, available at http://www.cne.gob.ve/web/sistema_electoral/tecnologia_electoral_descripcion.php.

90 "Creció desconfianza en el CNE, pero también la intención de votar," El Nacional, 21 May 2015, available at http://www.el-nacional.com/politica/Crecio-desconfianza-CNE-intencion-votar_0_631737031.html; see "Especial EFE: Máquina electoral con captahuellas aviva desconfianza," El Tiempo, 5 August 2012, available at http://eltiempo.com.ve/venezuela/comicios/especial-efe-maquina-electoral-con-captahuellas-aviva-desconfianza/60790.

include the use of surveillance drones to monitor crowds and traffic, as well as 2015 regulations that require banks to submit details about electronic transactions to a central government authority.[91]

Recommendations

41. We recommend that government of Venezuela should:

- Reform the legal framework governing communications surveillance so that it meets international human rights standards.
- In light of the importance of checking executive powers around surveillance, work to strengthen the independence of the judiciary.
- Reform Venezuela's intelligence agencies so that they are regulated by laws (approved by the National Assembly rather than by executive decree) that clearly prescribe their powers, establish oversight mechanisms, and meet with international human rights standards.
- Ban the use of anonymous "patriotas cooperantes" in court proceedings, establish clear and public rules on the use of informants by the security services, and appropriately sanction officials who unlawfully disseminate personal information or private conversations.
- Reform the law governing CONATEL to bring it into line with international human rights standards and ensure that CONATEL is able to operate independently of the executive.
- Abolish mandatory SIM card registration and review the data retention requirements placed on telecommunications companies.
- Pass comprehensive data protection legislation that meets international standards and establish an independent data protection authority that is appropriately resourced and has the power to investigate data protection breaches and order redress.
- Re-evaluate the use of biometric technologies in voting systems and around the sale of basic goods in supermarkets and pharmacies in order to ensure compliance with international human rights standards.

91 "Gobierno exige a los bancos revelar hasta el alma de sus clients," El Estímulo, 5 November 2015, available at http://elestimulo.com/elinteres/sudeban-exige-a-la-banca-entregar-hasta-el-ultimo-dato-de-sus-clientes/; "Gobierno aplicará el uso de drones para vigilar carreteras," El Carabobeño, 6 February 2016, available at http://www.el-carabobeno.com/noticias/articulo/119429/gobierno-aplicar-el-uso-de-drones-para-vigilar-carreteras; "Drones protagonizan operativo desarrollado por el Gobierno este Carnaval," Efecto Cocuyo, 6 February 2016, available at http://efectococuyo.com/principales/drones-protagonizan-operativo-desarrollado-por-el-gobierno-este-carnaval; Gobierno usará Drones para controlar 'el bachaqueo,'" El Estímulo, 1 February 2016, available at http://elestimulo.com/blog/gobierno-usara-drones-para-controlar-el-bachaqueo/.