Freedom of Expression, Encryption, and Anonymity: Civil Society and Private Sector Perceptions

Joint collaboration to inform the work of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Research Team

World Wide Web Foundation
Renata Avila

Centre for Internet and Human Rights at European University Viadrina
Ben Wagner
Thomas Behrndt

Oficina Antivigilância at the Institute for Technology and Society - ITS Rio
Joana Varon
Lucas Teixeira

Derechos Digitales
Paz Peña
Juan Carlos Lara

About the Research

In order to swiftly provide regional input for the consultation of the United Nations Special Rapporteur on the protection and promotion of the right to opinion and expression, the World Wide Web Foundation[1], in partnership with the Centre for Internet and Human Rights at European University Viadrina, Oficina Antivigilância[2] at the Institute for Technology and Society - ITS Rio[3] in Brazil, and Derechos Digitales[4] in Latin America, have conducted collaborative research on the use of encryption and anonymity in digital communications. The main goal of this initiative was to collect cases to highlight regional peculiarities from Latin America and a few other countries from the Global South, while debating the relationships within encryption, anonymity, and freedom of expression. This research was supported by Bertha Foundation.[5]

The core of the research was based on two different surveys focused on two target groups. The first was a series of interviews among digital and human rights organizations as well as potential users of the technologies to determine the level of awareness about both the anonymity and encryption technologies, to collect perceptions about the importance of these technologies to protect freedom of expression, and to have a brief overview of the legal framework and corporate practices in their respective jurisdictions. The interviews were conducted in over twenty countries from the Global South. The second part of the research was an initial consultation with the private sector by conducting over a dozen interviews to document their attitudes towards the topic.

[1] http://webfoundation.org
[2] https://antivigilancia.org
[3] http://www.itsrio.org
[4] https://www.derechosdigitales.org
[5] http://www.berthafoundation.org

Section 1

Perceptions from Human Rights and Digital Rights Organizations on the Use of Encryption, Anonymity, and Freedom of Expression

The first and main section of this report present cases collected through the first survey, informed by answers from lawyers, human rights defenders, and law and technology experts who responded to an online questionnaire with 15 questions (Annex II). In Latin America, the survey received answers from Brazil, Chile, Mexico, Colombia, Argentina, Ecuador, Peru, Uruguay, Paraguay, Venezuela, the Dominican Republic, El Salvador, Bolivia, Haiti, Honduras, and Costa Rica. The research team also added information from Cuba as one of the earliest countries to regulate encryption in the region. Beyond Latin America, but still focusing on the Global South, interviews were also conducted with public interest lawyers in Pakistan, Palestine, the Philippines, and South Africa. The answers to the questionnaire were collected during a short timeline of two weeks.

It is important to note that, due to the size of the sample, this quick survey is absolutely not intended to be fully representative either of the region of Latin America, nor of the other countries which submitted answers to the questionnaire. Nevertheless, the results provided insight about perceptions of human rights advocates who are at the forefront of the debates surrounding Internet freedoms.

1. Argentina[6]

Recent advancements in encryption technologies have proven pivotal for protecting freedom of expression and anonymity in the digital environment. Efforts to ensure users' capacity to communicate and undertake online transactions securely involve a concurrent commitment to upholding users' right to privacy. In Argentina, however, governmental institutions have made improper use of the technological developments that are rapidly changing digital information management, leaving users vulnerable to personal data breaches.

Personal data is protected under Law No. 25.326, which was passed in 2000 and restated in Regulatory Decree No. 1558/2001.[7] Overseen by the National Commission for the Protection of Personal Data, the Personal Data Protection Law exists to guarantee "comprehensive protection of personal information recorded in files, records, databases, databanks or other technical means of data treatment, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honour and privacy, as well as the access to information." The law defines personal data as any information relating to ascertained or ascertainable individuals or legal entities. This definition does not, however, cover data from opinion polls, statistical research under Law 17.622 (governing the National Institute of Statistics and Censuses), market research, and medical or scientific investigations, so long as the information cannot be linked to an identifiable individual or legal entity.[8]

The law itself does not specify the type of security measures in place for the safeguarding of personal data, although the Commission did layout mandatory security protocol in Directive 11/2006, which requires that data protection breaches be recorded and classified based on three security levels: basic, medium, and critical.[9]

In spite of Argentina's data protection law that ostensibly aims to preserve the integrity of personal data, government practices at the national level have demonstrated an alarming disregard for individual privacy. Mass surveillance was institutionalized at the national level in 2011 by an executive decree that ordered the creation of the Federal System of Biometric Identification (SIBIOS), a centralized, nationwide ID service that enables law enforcement to

[6] This section is partially a contribution by The Center for Studies on Freedom of Expression and Access to Information (CELE). The full submission is added as Annex III.

[7] Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[8] For additional information on the content and scope of the Personal Data Protection Law No. 25.326, see: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

[9] Available at: http://www.jus.gob.ar/media/33445/disp_2006_11.pdf

"cross-reference" information with biometric and other data that was originally collected for the national ID registry.

The SIBIOS initiative gives the Argentine Federal Police access to the National Registry of Persons (RENAPER) database, making available approximately 14 million digitized fingerprints, with the goal of having all 40 million Argentine citizens registered in the SIBIOS in 2015. Provincial officials have reported steady progress in the implementation of the SIBIOS initiative, and security forces are continually trained to make broad use of the system and its accompanying technologies. SIBIOS integrates existing identification databases, collecting the digital images, civil status, blood type, and extensive additional background information of citizens. A range of other security entities, including immigration authorities, airport security, the Argentine National Gendarmerie, and with authorization, provincial security elements, may consult this information. These integrated databases make use of a wide array of new technologies, such as facial recognition identification and mobile fingerprinting devices.[10]

In July 2014, it was reported that Argentines would have to renew their national identity card (DNI) for the third time in five years. Authorities indicated that the new electronic ID card would feature a chip that stores citizens' medical and public transportation history, along with social security information. The upgrade raises significant concerns about privacy encroachments, with some technology and civil liberties experts asserting that the new ID card qualifies as one of the world's most invasive surveillance systems, enabling surveillance at a massive scale in real time.[11]

While Argentine authorities have boasted that the new systems leverage emerging digital technologies to improve national security and streamline data collection, CELE contends that these developments jeopardize individual rights to free expression and privacy, as well as the ability to transact anonymously. The collection of sensitive personal information and widespread tracking at the national level could critically undermine citizens' willingness to exercise their right to freedom of expression. Though civil society groups have voiced their opposition to the State's encroachments, there has been minimal public awareness of the increased surveillance. There must be a sustained, coordinated response from stakeholders to encourage government authorities to consider the implications of identification and other new technologies on freedom of expression, data protection, privacy, and anonymity in the digital era.

[10] See: https://www.eff.org/deeplinks/2012/01/biometrics-argentina-mass-surveillance-state-policy
[11] See: http://panampost.com/belen-marty/2014/07/01/argentinas-national-id-cards-to-store-sensitive-data/

2. Brazil

In Brazil, a Court from the State of Espirito Santo ruled that Apple and Google should remove the application called *Secret* from their online stores. *Secret* allowed messages to be sent between users without them knowing the identity of the others. The judge made his decision by interpreting Article 5, IV of the Brazilian Constitution[12], maintaining that it protects freedom of expression but forbids anonymity. The decision also determined that these two companies should remotely remove installed versions of the application directly from consumers' smartphones, with a fine of R$20,000 (US$7,043) per day if they did not comply.[13]

Google appealed and the decision was suspended by a higher court, which sustained the argument that categorizing *Secret* as anonymous was not completely warranted because the server of the platform was storing the IP numbers of users, which could, ultimately, be used to identify them. It also stressed that remotely removing applications from phones would violate Brazilian laws, which includes privacy protection. Though the decision was reversed, it opened a debate about how to interpret anonymity over the Internet.

This situation gets even more complicated if we consider that anonymity has been interpreted by the government in a discretionary manner. On one hand, anonymity is encouraged by the State in cases of citizens denouncing crimes. On the other hand, specifically regarding the Internet, even with the approval of Marco Civil da Internet[14] guaranteeing safe harbours for intermediaries by exempting them from liability of third party content, we still eventually see intermediaries being convicted due to anonymous comments. The most recent case highlighted in the news was a sentence condemning Google to pay compensation for moral damages in the amount of R$2,500 (US$880) to a lawyer who felt offended by an anonymous comment on Google+.[15]

A general interpretation from current cases shows that while anonymous communications are legal, authorities might ask intermediaries for user data to identify them. If that interpretation prevails in the legal system, Brazilians will only enjoy some sort of pseudo-anonymity in the context of freedom of expression. Such an approach raises particular concerns regarding how this

---

[12] Brazilian Constitution: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

[13] Tech Crunch. "Brazil Court Issues Injunction Against Secret And Calls For App To Be Remotely Wiped". August 20th 2014. http://techcrunch.com/2014/08/20/brazil-court-issues-injunction-against-secret-and-calls-for-app-to-be-remotely-wiped/ Accessed March 11th 2015.

[14] Wikipedia. "Brazilian Civil Rights Framework for the Internet".
http://en.wikipedia.org/wiki/Brazilian_Civil_Rights_Framework_for_the_Internet Accessed March 11th 2015.

[15] Migalhas. "Advogado será indenizado por comentário anônimo na internet" [Portuguese]. February 21st 2015.
http://www.migalhas.com.br/Quentes/17,MI215884,21048-Advogado+sera+indenizado+por+comentario+anonimo+na+internet Accessed March 11th 2015.

interpretation might be extended to the usage of encryption tools important for user safety and privacy protection.

In practice, any expectation of anonymity or of complete exemption of Internet service providers in Brazil gets significantly diluted by the mandatory data retention provision established in Article 15 of Marco Civil, which states: "The Internet application provider that is duly incorporated as a legal entity and carry out their activities in an organized, professional and with economic purposes must keep the application access logs, under confidentiality, in a controlled and safe environment, for 6 months, as detailed in regulation."[16] In case of non-commercial providers, police or administrative authorities may require a precautionary retention of these records, though access to the data depends on a court order.

We should highlight that even the requirement of a court order has not been enough to protect voices of dissent. In the context of protests during the 2014 World Cup, there were incidents in which detained protesters were forced to reveal their social network usernames and passwords. Intelligence agencies and law enforcement authorities have also monitored social networks and Whatsapp, through programs such as Guardião and Mosaico, in addition to allegedly contacting intermediary providers of these services directly to gain access to user data and content of communications which, ultimately, weakens the power of digital tools like cryptography and encrypted standards.[17] Such was the case of many people who were detained during protests surrounding the World Cup. Direct requests are even made through private security companies[18], such as MODULO[19], which was contracted to work with the intelligence centre of Rio de Janeiro, and be responsible for monitoring mega events using several public databases.

Anonymity in the context of social protests has also been questioned under these same the constitutional grounds for freedom of expression. Previous to the World Cup, some of the major states (e.g., Sao Paulo[20], Rio de Janeiro[21] and Porto Alegre[22]), enacted new laws to prohibit the use of masks, and sometimes even helmets and facial painting which could prevent identification of

---

16 See Marco Civil in English https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf Accessed March 11th 2015.

17 Exame. "Abin monta rede para monitorar protestos pela internet" [Portuguese]. June 20th 2013. http://exame.abril.com.br/tecnologia/noticias/abin-monta-rede-para-monitorar-protestos-pela-internet Accessed March 11th 2015.

18 Veja «Empresas de seguraça privada monitoram black blocs» March 24th 2014 http://veja.abril.com.br/noticia/brasil/empresas-de-seguranca-privada-monitoram-black-blocs Accessed: March 11st 2015

19 Modulo Solutions for Governance Risk and Compliance https://www.modulo.com.br/solucoes/gestao-de-eventos-e-incidentes Acessed: March 11th 2015

20 Lei 15556 [Portuguese] http://www.al.sp.gov.br/repositorio/legislacao/lei/2014/lei-15556-29.08.2014.html

21 Lei 6528 [Portuguese] http://gov-rj.jusbrasil.com.br/legislacao/1036049/lei-6528-13

22 Gaúcha. "Aprovado projeto que proíbe uso de máscaras em protestos na capital" [Portuguese] February 26th 2014. http://gaucha.clicrbs.com.br/rs/noticia-aberta/aprovado-projeto-que-proibe-uso-de-mascaras-em-protestos-na-capital-80340.html Accessed March 11th 2015.

protesters. In the case of Rio de Janeiro, the law was questioned, but the Court considered it constitutional, even though the Brazilian Order of Lawyers (Ordem de Advogados do Brasil, OAB) had positioned against it.[23] Other organizations concerned about civil liberties have also opposed to such measures.[24]

During the demonstrations in July 2013, the government of Rio de Janeiro also approved a decree for the creation of a Special Committee to Investigate Acts of Vandalism in Public Demonstrations (CEIV). The decree established that telecommunications companies and Internet service providers would have to deliver user data to a broad range of authorities without judicial order with 24 hours.[25] After concerns expressed by OAB and associations of telecommunications companies, the decree was modified and this particular provision was removed.[26]

Even though expedited procedures for access to user data was not approved, telecommunications companies are required to store more than connection logs of their users. Although there is no national legislation requiring the registering of SIM cards, there is a technical regulation from the National Telecommunications Agency (ANATEL)[27] establishing that mobile service providers should keep the following data about their users: a) name; b) ID or tax number; and c) address. The regulation also establishes that users have the duty to keep their information up-to-date within the providers. Therefore, it is impossible to use even a prepaid SIM card without registering, and users who refuse to provide their personal information may have the service suspended. Furthermore, since the country still doesn't have legislation on data protection, it is unclear how this database is being protected and treated, which is yet another aspect that highlights the major importance for approving a strong bill on data protection.[28]

---

23 Consultor Jurídico. "TJ-RJ considera constitucional proibição de máscaras em protestos"[Portuguese] November 11th 2014. http://www.conjur.com.br/2014-nov-11/tj-rj-considera-constitucional-proibicao-mascaras-protestos. Accessed: March 11th 2015. O Globo. "Tribunal de Justiça Julga Constitucional lei que proibe uso de máscaras em protestos no rio" [Portuguese]. November 10th 2014. http://oglobo.globo.com/rio/tribunal-de-justica-julga-constitucional-lei-que-proibe-uso-de-mascaras-em-protestos-no-rio-14523863 Accessed March 11th 2015.

24 Connectas. "Atropelando Direitos" [Portuguese] August 29th, 2014. http://www.conectas.org/pt/acoes/justica/noticia/25324-atropelando-direitos Accessed: March 11th 2015

25 Telesíntese. "Teles e provedores deverão entregar dados de 'vândalos' em 24hs" [Portuguese] July 23th 2013 http://www.telesintese.com.br/teles-e-provedores-deverao-entregar-dados-de-vandalos-em-24hs-para-governo-do-rj/ Accessed March 11th 2015

26 Telesíntese. "Após polêmica, governo do rio anuncia que mudará decreto que quebra sigilo de dados de vândalos" [Portuguese] July 24th 2013 http://www.telesintese.com.br/apos-polemica-governo-do-rio-anuncia-que-mudara-decreto-que-quebra-sigilo-de-dados-de-vandalos/ Accessed March 11th 2015

27 Resolução ANATEL 477/2007: http://legislacao.anatel.gov.br/resolucoes/22-2007/9-resolucao-477

28 http://participacao.mj.gov.br/dadospessoais/

3. Chile

In Chile, there have been some drastic cases where privacy and (pseudo) anonymity on social media platforms have been violated by law enforcement agencies[29] to threaten freedom of expression. A significant number of these violations has been committed in the context of social protests.

Anonymity in the context of protest is not a crime in Chile. However, since the beginning of the students protests in 2011[30], there has been an interesting public debate about the right to be hooded in these instances[31] due to the violence of some hooded protesters and there have been attempts to criminalize those who demonstrate covering their faces.

As a consequence, in late 2011, Rodrigo Hinzpeter, then the Interior Minister of President Sebastián Piñera, presented the "Bill to Fortify the Protection of Public Order"[32] (known as the Hinzpeter's Bill) which was especially hard on masked protesters[33], increasing the penalties for offenses of public disorder "when acting hooded (wearing a mask, covering the face) or with anything else that would prevent, hinder or delay the identification of the perpetrator."

The bill has sparked huge public controversy in the public opinion[34] as it is effectively criminalizing the right to protest[35], but, even though it has little chance of approval, it has not been formally withdrawn.

Despite the national controversy over Hinzpeter's Bill in 2014, members from within the country's

[29] Digital Rights LAC. "Right to protest and policing in social networks". June 30th 2014. http://www.digitalrightslac.net/en/derecho-a-protesta-y-vigilancia-policial-en-redes-sociales/ Accessed March 11th 2015.

[30] The Atlantic. "Student Protests in Chile". August 10th 2011. http://www.theatlantic.com/photo/2011/08/student-protests-in-chile/100125/ Accessed March 11th 2015.

[31] BBC News. "Unmasking Chile's hooded protest movement". May 22th 2013. http://www.bbc.com/news/world-latin-america-22565124 Accessed March 11th 2015.

[32] See the text of the bill [Spanish] http://congresoabierto.cl/proyectos/7975-25

[33] Benjamin Witte's Web Site. "Chile's Congress Bids Adieu To Controversial 'Hinzpeter Law'". June 5th 2014. https://benwitte.wordpress.com/2014/06/05/chiles-congress-bids-adieu-to-controversial-hinzpeter-law/ Accessed March 11th 2015.

[34] Reporters Without Borders. "Bill would criminalize protests, turn journalists into police informers". October 6th 2011. http://en.rsf.org/chile-bill-would-criminalize-protests-06-10-2011,41137.html Accessed March 11th 2015.

[35] Senador De Urresti. "Diputado De Urresti (PS): 'Solo se buscaba criminalizar la protesta social'" [Spanish]. December 17th 2013. http://deurresti.cl/2013/12/17/diputado-de-urresti-ps-solo-se-buscaba-criminalizar-la-protesta-social/ Accessed March 11th 2015.

largest opposition party submitted a bill[36] proposing greater punishment for those who cause destruction during public protests and granting law enforcement wider powers in dealing with offenders. María José Hoffman, one of the representatives who submitted the bill, said[37]: "This new attempt to eradicate violence during legitimate social protests sets a term of imprisonment for participants of disorder or violence during demonstrations if they are masked with the purpose of concealing their identity".

In January 2014, a student was arrested without a warrant after a student rally and, without a corresponding court order, he was forced to reveal his Facebook password[38] in order to identify other protesters. In May 2014, the Justice Department dismissed an investigation[39] of a young man accused of assaulting a police officer after a demonstration on International Workers' Day, based on facial recognition from Facebook photos. The presented evidence was deemed inconclusive, and in fact, the Judge "called [for] the prosecutor to be more serious in carrying out the investigations". In June 2014, the Cybercrime Brigade explained[40] to a local newspaper that they make a "digital registration" in social media in order to help their investigations, without specifying what the registration is or how privacy rights are respected.

Chilean Twitter user Rodrigo Ferrari, was facing prosecution for operating a Twitter account that parodied millionaire Andrónico Luksic. Under allegations of identity theft, the police approached Twitter without a court warrant[41] to access the user information of three Twitter accounts: @losluksic, @andronicoluksic, and @luksicandronico. In addition to illegally accessing this personal data, although information provided by Twitter only linked Ferrari to @losluksic, the Police Department issued an unfounded report erroneously linking Ferrari with all three accounts.[42]

---

[36] BioBio Chile. "Parlamentarios de la UDI presentan nuevo proyecto de ley que sanciona violencia de encapuchados" [Spanish]. July 17th 2014. http://www.biobiochile.cl/2014/07/17/parlamentarios-de-la-udi-presentan-nuevo-proyecto-de-ley-que-sanciona-a-encapuchados.shtml Accessed March 11th 2015.

[37] Publimetro. "Diputados UDI ingresan nuevo proyecto en contra de encapuchados" [Spanish]. July 16th 2014. http://www.publimetro.cl/nota/politico/diputados-udi-ingresan-nuevo-proyecto-en-contra-de-encapuchados/xIQngq!COSsdL97Qe4E6/ Accessed March 11th 2015.

[38] Derechos Digitales. "Integridad física y privacidad de tu información, dos caras de la misma moneda" [Spanish]. February 6th 2014. https://www.derechosdigitales.org/6927/los-derechos-digitales-tambien-son-derechos-humanos/ Accessed March 11th 2015.

[39] Derechos Digitales. "La fiscalía está revisando tu Facebook" [Spanish]. May 29th 2014. https://www.derechosdigitales.org/7418/la-fiscalia-esta-revisando-tu-facebook/ Accessed March 11th 2015.

[40] Derechos Digitales. "¿Por qué las redes sociales en Chile no son seguras para tus derechos?" [Spanish]. June 25th 2014. https://www.derechosdigitales.org/7576/porque-las-redes-sociales-en-chile-son-seguras-para-tus-derechos/ Accessed March 11th 2015.

[41] Derechos Digitales. "Fiscales, policías e infracciones al debido proceso en Chile" [Spanish]. February 21st 2013. https://www.derechosdigitales.org/3667/fiscales-debido-proceso/ Accessed March 11th 2015.

[42] Digital Rights LAC. "On the parody on Twitter: lessons to learn". July 17th 2013. http://www.digitalrightslac.net/en/sobre-la-parodia-en-twitter-lecciones-que-aprender/ Accessed March 11th 2015.

The Twitter account @losluksic was created with the expressed intention of parody, which was easily identified by the humorous and satirical tone of the messages, and by the profile image of dollars falling from the sky. But the unfounded connection with the other two accounts got Ferrari into trouble. For months he was under pressure to reach an agreement or conditional suspension. He was eventually acquitted of the charges, but he was never compensated for the dismissal of due process and privacy.[43]

SIM Card registration is still not mandatory in Chile, however a draft bill[44] alleged to prevent terrorist attacks and activities of criminal organizations has been proposed, seeking to compel users to register every SIM card under natural or legal entity identity card or tax number and nationality. The "Subsecretaría de Telecomunicaciones" would maintain these records, and data would be protected according to data protection law, which enables these kinds of data to be handed over to the police and the Public Prosecutor for research purposes without requiring a warrant. Another draft bill[45] alleged to prevent thefts and the coordination of illegal activities proposes that every service provider should maintain a register of those who purchase prepaid phones and those who already have one. (There would be one year to register all the prepaid phones in the country.) Data to be registered and associated would be name, address, ID number or passport number and SIM card number. In this case, data could be handed over only with court order or express legal provision. [46]

[43] Derechos Digitales. "Fiscales, policías e infracciones al debido proceso en Chile" [Spanish]. February 21st 2013. https://www.derechosdigitales.org/3667/fiscales-debido-proceso/ Accessed March 11th 2015.

44 Congreso Abierto. "Exige a los operadores de telefonía móvil registrar los datos personales de los clientes que adquieran una línea en la modalidad prepago" [Spanish]. December 9th 2014. http://congresoabierto.cl/proyectos/9767-15 Accessed March 12th 2015.

45 Congreso Abierto. "Modifica la ley general de telecomunicaciones, en materia de individualización y recolección de datos de usuarios de servicios telefónicos de prepago" [Spanish]. March 3rd 2015. http://congresoabierto.cl/proyectos/9894-15 Accessed March 12th 2015.

46 Congreso Abierto. "Modifica la ley general de telecomunicaciones, en materia de individualización y recolección de datos de usuarios de servicios telefónicos de prepago" [Spanish]. March 3rd 2015. http://congresoabierto.cl/proyectos/9894-15 Accessed March 12th 2015.

4. Colombia

There is no national legislation prohibiting anonymity in social protests in Colombia. However, the municipality of Medellín (the second largest city in Colombia) has banned the use of any element that may impose an obstacle to the identification of protesters under penalty of forced interruption of a protest by the police.[47]

Since 2011 there has been a mandatory requirement[48] for registering mobile devices in order to provide a white list of registered devices and a blacklist of stolen devices. Users must provide: name, address, contact number and ID number. This database is duplicated by the police since, according to a resolution[49] issued by Ministry of Defence and Direction of Criminal Investigation of the National Police (DIJIN), telecommunications service providers authorized to operate must "allow remote queries" to subscriber's data" (article 1) "via web through VPN" which must contain the following information: a) complete names or registered corporate or trade name; b) identification number and type or tax identification (for legal entities); c) address; d) telephone number; e) city of residence; f) mobile number or fixed line number; g) "ID and FLOTA number," if any; and h) Activation date. In case of changes, telecommunications service providers must send updates to DIJIN every month.

Colombia has a long-running history of illegal interception of communications that affected opposition leaders, high court judges, journalists and human rights activists. For these actions, the former director of the now-disbanded Colombian security agency Departamento Administrativo de Seguridad (DAS) and former secretary of the Colombian Government were found guilty[50] of illegal interception of communications, of judges, journalists, human rights defenders, and opposition leaders, among other groups, as they were considered potentially dangerous to the administration of former President Álvaro Uribe Vélez.

External interception laboratories and facilities were the most common form of intelligence equipment deployment reported in illegal surveillance cases. Despite the adoption of a new

---

47 See Decreto Nº 2254 de 2013. Alcaldía de Medellín. Gaceta 4203 [Spanish] http://www.medellin.gov.co/irj/go/km/docs/pccdesign/SubportaldelCiudadano_2/PlandeDesarrollo_0_15/Publicaciones/Shared%20Content/GACETA%20OFICIAL/2014/Gaceta%204203/DECRETO%202254%20DE%202013.pdf Accessed March 11th 2015.

48 Decree 1630 of 2011: http://www.mintic.gov.co/portal/604/articles-3558_documento.pdf [Spanish] Accessed March 11th,2015

49 Resolution 912 of 2008: https://www.redjurista.com/documents/r_mdef_0912_2008.aspx [Spanish], Accessed in March 11th 2015.

50 Semana. "Chuzadas" del DAS: crimen y castigo [Spanish] February, 2015. http://www.semana.com/nacion/articulo/chuzadas-del-das-crimen-castigo/419365-3

Intelligence and Counterintelligence Act in 2013 intended to prevent cases such as these, a year later a new case of illegal communications surveillance was discovered. In February 2014, *Semana* revealed[51] that an undercover military intelligence unit not only executed an illegal operation, but also served as a centre for the interception of electronic communications targeted at representatives from the government and from Fuerzas Armadas Revolucionarias de Columbia (FARC) in the Peace Talks taking place in Havana, Cuba.

According to information obtained by *Semana*, the intelligence operation was intercepting emails, and Blackberry and WhatsApp instant messages with the help of (young) civilians who had been contacted by military agents at technology conventions (i.e. Campus Parties). This operation is known as "Andromeda."

This scandal brought to light[52] that there are two branches of military intelligence: (1) one specialized in the interception of telephone communications, and (2) another devoted to the interception of digital communications. According to a *Semana* source, the branch dedicated to the interception of telephone communications operates within the Public Prosecutor's Office, which is subject to stricter controls. In contrast, due to the feeble legal framework on digital communications surveillance, the second branch is more prone to commit abuses. However, it was reported that 115 out of 440 intercepted telephone numbers did not have a warrant issued by the required authority.

5. Cuba

Cuba regulates the use of cryptographic technologies. Citizens need a permit from the Ministry of Interior in order to protect their communications using cryptography. Only the Ministry of Interior can authorize the distribution, promotion, research, training and exchange of encryption technologies. This restriction applies to both foreign and local individuals and entities. Cuban authorities also regulate the use of cryptographic algorithms. It is forbidden to use unauthorized cryptographic algorithms, and only algorithms developed by the Ministry of Interior can be used. [53]

[51] Semana. "¿Alguien espió a los negociadores de La Habana?" [Spanish] February 3th 2014. http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3 Accessed March 11th 2015.

[52] Semana. "Chuzadas: así fue la historia" [Spanish]. February 8th 2014. http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3 Accessed March 11th 2015.

[53] Cuban regulation on encrypted communications http://www.di.sld.cu/documentos/resol/DL_199.pdf

6. Ecuador

The persecution of anonymity on the Internet is not something new in Ecuador. The new Communications Law, enacted in 2013[54], says that publishers are liable for their comment sections, and users have to register under a real name policy, therefore losing the ability to remain anonymous when commenting[55]. These new conditions are detrimental to freedom of expression online.

Social media has become a new target for the executive power. Although the administration of President Rafael Correa has previously expressed its intentions of regulating of social media in cases of hate speech[56], instead of regulating it, the administration has opted for a public campaign using state media to criticise anonymity. During the Presidential weekly report broadcasted via radio and television, President Correa revealed important personal data (name, surname, and city) of three Twitter users who had severely insulted him, asserting that irony and sarcasm were different than slander, lies, and falsehoods.[57]

In this context, the government has been particularly critical with @CrudoEcuador, an anonymous Twitter and Facebook user who posts humorous memes about topics of Ecuadorian national interest, especially political figures like the President of Ecuador. Correa accused @CrudoEcuador of a "systematic campaign of defamation" paid for by those who want to discredit him. The satirical work of this anonymous user has been strongly supported by citizens, however, turning this incident into a national controversy.[58]

After the incident, and as Global Voices reported[59], *Crudo Ecuador's* Twitter account was temporarily suspended on January 28th for several hours due to complaints which claimed it violated the social network's terms of service. In an interview with newspaper *El Comercio*, the writers behind @CrudoEcuador said the account had been closed by "government trolls." Fearing

[54] See the text of the Law [Spanish] http://www.derecho-ambiental.org/Derecho/Legislacion/Ley_Organica_Comunicacion_Ecuador_2013.html Accessed March 11th 2015.

[55] Digital Rights LAC. "Ecuador's Communications Law: With a View Toward a More Democratic Law". July 17th 2013. http://www.digitalrightslac.net/en/ley-de-comunicacion-en-ecuador-de-cara-a-una-ley-mas-democratica/ Accessed March 11th 2015.

[56] Periodismo Ecuador. "Alexis Mera propone regular Redes Sociales en casos de calumnias" [Spanish]. Agugust 18th 2013. http://periodismoecuador.com/2013/08/28/alexis-mera-propone-regular-redes-sociales-en-casos-de-calumnias/ Accessed March 11th 2015.

[57] Diario de Cuba. "Rafael Correa busca presionar a detractores en redes sociales" [Spanish]. February 5th 2015. http://www.diariodecuba.com/internacional/1423094745_12710.html Accessed March 11th 2015.

[58] BBC News. "Ecuador President Rafael Correa's troll warfare". January 30th 2015. http://www.bbc.com/news/blogs-trending-31057933 Accessed March 11th 2015.

[59] Global Voices. "Ecuadorian President Threatens Internet Satirists". February 17th 2015. http://globalvoicesonline.org/2015/02/17/ecuadorian-president-threatens-internet-satirists/ Accessed March 11th 2015.

for his life, the administrator of the site has recently announced[60] that he is shutting down his website and the related social media accounts.

The office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) had recently expressed[61] concerns about the criticism made by high government officials towards the manager of *Crudo Ecuador*, and urged authorities to consider the consequences that such statements may have on his safety.

Because there is no legal mechanism against anonymity in Ecuador, the president announced the creation of "Somos Más Ecuador"[62] where supporters of Correa's government can respond to its critics via social media.

A great debate about anonymity has been present through civil society in the last several years, and many organizations are working towards the promotion of encryption and anonymity. Among the most serious and organized efforts in this direction are "Crypto Party"[63] events.

Besides the attacks on anonymity on the Internet, there are other practices and technologies used to curtail privacy with the excuse of security, such as mandatory registration for all mobile phone numbers (through the identity card), and the mandatory operation of CCTV cameras inside taxi cabs, addressing security concerns.

Since 2011, with the alleged aim of reducing robbery of mobile devices in the country, Ecuador has enforced mandatory registration of cellphones under penalty of suspension.[64] Users must provide full name, address, ID number and for validation purposes, the year the document was issued. This information is associated with the IMEI number or SIM CARD of the phone. All this information is recorded in a database and stored for at least five years by every provider of the

[60] Panam Post. "Correa's Nemesis Crudo Ecuador Shuts Down over Intimidation". February 20th 2015. http://panampost.com/rebeca-morla/2015/02/20/correas-nemesis-crudo-ecuador-shuts-down-over-intimidation/ Accessed March 11th 2015.

[61] Organization of American States. "The Office of the Special Rapporteur Urges Ecuador to Ensure the Safety of Citizen Behind "Crudo Ecuador" and Expresses Concern Regarding Comments Made by High Authorities". February 25th 2015. http://www.oas.org/en/iachr/media_center/PReleases/2015/R17.asp Accessed March 11th 2015.

[62] See somosmas.ec. Accessed March 11th 2015.

[63] See cryptoparty.ec Accessed March 11th 2015.

64 Explored. "Inicia registro obligatorio de celulares" [Spanish]. April 14th 2011. http://www.explored.com.ec/noticias-ecuador/inicia-registro-obligatorio-de-celulares-469601.html Accessed March 12th 2015.

"Servicio Móvil Avanzado."[65] Data can be requested by competent authorities in accordance with the requirements and procedures of the law.[66]

While implementing the new regulation, the Minister of Telecommunications declared that if people do not register, not only the lines, but also the devices can be blocked even outside the country, stressing that agreements for cooperation were under negotiation with Colombia and Peru.[67]

7. Guatemala

During a two-year period in Guatemala, a broad group of civil society organizations launched a multimedia campaign advocating for the compulsory registry of SIM Cards and equipment[68]. The increase of armed theft and phone calls threatening citizens with extortion[69] and anonymous calls was the justification to introduce and approve a law mandating the compulsory registry of SIM Cards and mobile devices, including mobile telephones, smartphones, and tablets. The law was approved[70] with little opposition from citizens, and extended the powers of police, without the approval of a judicial authority, to request information about mobile communications and collaborate with authorities. It is important to note that Guatemala has not yet approved a data protection law. While apps are not regulated, the social application *Secret* sparked controversy in 2014 when the Vice President threatened to regulate social networks in order to protect the morality of women and children[71].

65 ARCOTEL. "Servicio Móvil Avanzado" [Spanish]. http://www.arcotel.gob.ec/servicio-movil-avanzado/ Accessed March 12th 2015.
66 ARCOTEL. "Codificación de la norma que regula el procedimiento para el empadronamiento de abonados del servicio móvil avanzado (SMA) y registro de terminales perdidos robados o hurtados" [Spanish]. http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/codificacion_norma_empadronamiento.pdf Accessed March 12th 2015. Additional information in "Resolución Tel-535-16-CONTEL.2012" [Spanish] http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/0535_tel_18_conatel_2012.pdf Accessed March 12th 2015.
67 El Universo. "Usuarios de celulares ahora están obligados a registrarse contra robos" [Spanish]. July 8th 2011. http://www.eluniverso.com/2011/07/08/1/1356/usuarios-celulares-ahora-estan-obligados-registrarse-contra-robos.html Accessed March 12th 2015.
68 See the text of the Law "Ley de Celulares" [Spanish] https://web.archive.org/web/20130921164526/http://www.leycelulares.com/index.php/comparacion Accessed March 11th 2015.
69 InSight Crime. "700 Extortion-Related Murders in Guatemala through July 2014: NGO". August 15th 2014. http://www.insightcrime.org/news-briefs/guatemala-700-homicides-extortion-2014 Accessed March 11th 2015
70 See the text of the Law "Ley de Equipos Terminales Móviles" [Spanish] http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2013/pdfs/decretos/D08-2013.pdf Accessed March 11th 2015
71 Digital Rights LAC. "Secret shakes Guatemalan society". October 29th 2014. http://www.digitalrightslac.net/en/secret-sacude-a-sociedad-guatemalteca/ Accessed March 11th 2015.

8. Mexico

In Mexico, there has been a substantial increase in the persecution and murder of Internet activists and bloggers who report cases of corruption and abuse of power by the Government, or other organized criminal activity. In the border state of Tamaulipas alone, from the period between 2010 and October 2014, 27 bloggers have reportedly been killed.[72]

Anonymity, or pseudo-anonymity, has been a partial solution to enable citizens to keep channelling denouncements. For instance, the website *Valor por Tamaulipas*[73] was founded by an anonymous user with the goal of sharing information via social media regarding drug-related violence within the State. With 556,000 Facebook "likes"[74] and 122,000 followers on Twitter[75], the initiative survives mostly due to anonymity. However, it is not immune to threats and sad histories. In 2013, a drug cartel offered a reward of US$46,000 for information that would lead to the identity or location of the page administrator; sadly, in October 2014 María del Rosario Fuentes Rubio, who used a pseudonym but became a known collaborator of *Valor por Tamaulipas*, was brutally killed[76] by the cartel which also hacked into Fuentes Rubio's account and posted threats to other citizen journalists using social networks.

Another alarming example is the arrest of Twitter user and *Anonymous* member, Gustavo Maldonado. On his social media accounts, Maldonado was highly critical of Chiapas Governor Manuel Velasco Coello and the federal government. He made several denouncements, including that of the purchase of an online surveillance tool[77] called "Black Eyed Hosting" by the Public Attorney (Procuradora General de Justicia de Estado, PGJE). The Mexican blog *Información de lo nuevo*[78] suggested that law enforcement officials had been monitoring Maldonado's activities using this tool[79] and charged him under minor drug-related offenses[80]. Maldonado's arrest took place

[72] Revista Era. "Veintisiete tuiteros y bloggers han sido asesinados en #Tamaulipas" [Spanish]. October 16th 2014: http://revistaera.com/index.php/notas/11531-veintisiete-tuiteros-y-bloggers-han-sido-asesinados-en-tamaulipas Accessed March 11th 2015.

[73] See http://www.valorportamaulipas.info/ Accessed March 11th 2015

[74] See facebook.com/ValorPorTamaulipas Accessed March 11th 2015

[75] See twitter.com/valortamaulipas Accessed March 11th 2015

[76] Reporters Without Borders. "A Netizen Is Killed in Tamaulipas". October 23th 2014. http://en.rsf.org/mexique-a-netizen-is-killed-in-tamaulipas-23-10-2014,47144.html Accessed March 11th 2015.

[77] Proceso. "Acusan de narcomenudista a cibernauta crítico del gobierno chiapaneco" [Spanish]. August 10th 2013. http://www.proceso.com.mx/?p=349780 Accessed March 11th 2015

[78] Libertad de Expresión Yucatán. "Acusan de venta de drogas a Gustavo Maldonado López, crítico del gobierno de Chiapas" [Spanish] http://www.informaciondelonuevo.com/2013/08/acusan-de-venta-de-drogas-gustavo.html Accessed March 11th 2015

[79] Global Voices. "Government Critic Arrested on Drug Charges in Mexico". August 12 2013. http://advocacy.globalvoicesonline.org/2013/08/12/government-critic-arrested-on-drug-charges-in-mexico/ Accessed March 11th 2015

only hours after he shared a video on the *Anonymous Legion Chiapas* YouTube channel, exposing a corruption scandal related to local water supply services and other social problems.

Authorities in the State of Chiapas have a long history of corruption, abuse of power, and unregulated usage of surveillance technologies such as "Black Eyed Hosting" to threaten the freedom of expression of its citizens. However, that is not the only surveillance technology in Mexico. Citizen Lab denounced the presence of FinFisher spyware in Mexico[81] what was in use at least until September 2013. The *Reforma* newspaper found[82] that FinFisher was acquired by the Procuraduría General de la República during the administration of President Felipe Calderon. According to the Citizen Lab investigation, FinFisher was also present in Panama.

A push for the usage of surveillance technologies with disregard to anonymity also moves from online to offline environments. For instance, local representatives in the "Asamblea General del Distrito Federal" have stated the necessity to strengthen surveillance through video cameras in Mexico City, with the aim of improving intelligence work at the social protests. Other authorities have declared the necessity to increase the penalties for those who commit crimes with their faces covered. Indeed, although anonymity in social protests is not explicitly punished, there are multiple statements by public officials that have led to hostile attitudes against people who protect their identity in contexts of social protest. As such, people have been subjected to arbitrary arrests for wearing masks during protests.

Mexico also approved the Geolocalization Law in 2014[83], expanding police authority for the purposes of countering drug and gang related violence and weakened privacy safeguards. The reform gives unprecedented mandate to Mexican public authorities and law enforcement bodies to access real time geolocation data from mobile phone companies. While privacy activists were opposed to the law[84], other civil society groups advocating for citizen security were supportive of the law, which reflects the tensions between the two groups in the region.

---

[80] Jesus Robles Maloof. "Gustavo Maldonado, blogger and political prisoner in Chiapas. #FreeGumalo". August 16th 2013. https://roblesmaloof.wordpress.com/2013/08/16/gustavo-maldonado-bolgger-and-political-prisioner-in-chiapas-freegumalo/ Accessed March 11th 2015.

[81] Global Voices. "Mexico: Advocates Demand Investigation of FinFisher Spyware". June 21st 2013.. http://advocacy.globalvoicesonline.org/2013/06/21/mexico-advocates-demand-investigation-of-finfisher-spyware/ Accessed March 11th, 2015.

[82] Periódico AM. "Derrocha la PGR en equipo espía" [Spanish]. July 6th 2013. http://www.am.com.mx/leon/mexico/derrocha-la-pgr-en-equipo-espia-29702.html Accessed March 11th 2015.

[83] See text of the law http://mexicosos.org/descargas/dossier/legislacion/ley_geolocalizacion.pdf [Spanish]. Accessed March 11th 2015.

[84] Ars Technica. "Mexican 'Geolocalization Law' draws ire of privacy activists". April 24th 2012. http://arstechnica.com/tech-policy/2012/04/mexican-geolocalization-law-draws-ire-of-privacy-activists/ Accessed March 11th 2015.

9. Peru

Even though the right to freedom of movement and the right of assembly didn't previous require identification in Peru, in the final months of 2014 there were public declarations[85] from Daniel Urresti, former Minister of the Interior who was in charge of the Peruvian police, in order to impose *de facto* restrictions on anonymity in rallies. For a protest in December 2014, Urresti stated[86] that hooded protesters wouldn't be allowed to participate in the demonstration and announced that police would ask for the national identification card to the attendees[87]. These kinds of proposals have been quickly condemned by civil society[88], trades unions[89] and even other sectors of the government[90], pointing out that such measures are criminalizing public protest.

Nevertheless, other forms of mandatory identification have also been implemented by law. Since 2010, all SIM cards are associated with the national ID card[91]. People must submit their original document and the telecommunications provider must record the full name (or company name) and the number and type of legal identification of the subscriber. These data are kept by the company for billing purposes and marketing, and are also shared with State authorities. The next step will be in mid-2015 when users' identity will be verified by biometric fingerprints[92]. These measures do not prevent people use other peoples' phones to commit illegal acts, while it does represent a bigger risk for citizens' privacy, due to unnecessary collection and storage of sensitive user data.

---

[85] El Comercio. "Urresti puso reglas para protesta de hoy contra régimen juvenil" [Spanish]. December 22th 2014. http://elcomercio.pe/lima/ciudad/daniel-urresti-ley-pulpin-reglas-protesta-hoy-contra-regimen-laboral-juvenil-noticia-1780080 Accessed March 11th 2015.

[86] Diario Correo. "Daniel Urresti sobre marcha contra Ley Pulpín: 'la policía no va a reprimir va a acompañarlos'" [Spanish]. December 22nd 2014. http://diariocorreo.pe/ciudad/daniel-urresti-sobre-marcha-contra-ley-pulpin-la-policia-no-va-a-reprimir-va-a-acompanarlos-552619/ Accessed March 11th 2015.

[87] El Comercio. "Urresti puso reglas para protesta de hoy contra régimen juvenil" [Spanish]. December 22nd 2014. http://elcomercio.pe/lima/ciudad/daniel-urresti-ley-pulpin-reglas-protesta-hoy-contra-regimen-laboral-juvenil-noticia-1780080?ref=nota_lima&ft=contenido Accessed March 11th 2015.

[88] Espacio 360. "Hay mas del ministro del interior Daniel Urresti que tal vez no sepas" [Spanish]. July 2nd 2014. http://espacio360.pe/noticia/actualidad/hay-mas-del-ministro-del-interior-daniel-urresti-que-tal-vez-no-sepas-1971 Accessed March 11th 2015.

[89] El Comercio. "CTP marchará para pedir renuncia del ministro Daniel Urresti" [Spanish]. February 7th 2015. http://elcomercio.pe/lima/sucesos/ctp-marchara-pedir-renuncia-ministro-daniel-urresti-noticia-1790017 Accessed March 11th 2015.

[90] RPP Noticias. "Ana Jara: Para ejercer derecho a la protesta no se requiere llevar DNI" [Spanish]. December 22nd 2014. http://www.rpp.com.pe/2014-12-22-ana-jara-para-ejercer-derecho-a-la-protesta-no-se-requiere-llevar-dni-noticia_753205.html Accessed March 11th 2015.

91 Perú 21. "Los celulares de prepago en la mira" [Spanish]. May 27th 2010. http://peru21.pe/noticia/486144/celulares-prepago-mira Accessed March 12th 2015.

92 RPP Noticias. "Operadoras de móviles identificarán a clientes con huellas dactilares" [Spanish]. December 7th 2014. http://www.rpp.com.pe/2014-12-07-operadoras-de-moviles-identificaran-a-clientes-con-huellas-dactilares-noticia_748869.html

10. Venezuela

According to the Venezuelan Constitution, anonymity is prohibited in the context of freedom of expression[93] and covering faces during a demonstration is seen as a non-peaceful form of protest, what usually leads to arrests and assaults by the police. In a similar concept, all mobile lines (prepaid or monthly plans) are associated either with citizens ID cards or tax payer number as a requirement for acquiring a number. The National Commission of Telecommunications also requires that telecommunications companies register the IMEI number of each mobile devices to the user's ID. The argument for imposing such requirements has been to reduce theft, but according to interviews, there is no evidence of reduction in these numbers.

In the online environment, due to Ley Resorte, anonymous content is also prohibited and shall be removed or blocked by ISPs. Even the use of pseudonymous has been considered illegal in some cases, leading to prosecution. When Chavista deputy Robert Serra[94] was murdered in Venezuela, at least eight Twitter users, some operating under pseudonymous, were detained by Venezuelan authorities[95] for making political comments against Serra or tweeting about his death which, according to police, allegedly tied them to the murder. (To date, only two detainees have been released.[96]) All eight were transferred to a branch of the Venezuelan intelligence service, the Servicio Bolivariano de Inteligencia Nacional (SEBIN).[97] The news portal, *Infobae*, was blocked for posting content about the arrests.

The ruling party parliamentarian, Christian Zerpa, has confirmed that these detentions occurred because detainees "made fun" of the assassinated politician[98]. In many of these cases, the legal defence of these Twitter users has alleged that the detentions were without a warrant. In the case of Inés Margarita González Árraga (@inesitaterrible), her legal defence reported[99] that she voluntarily handed over her personal computer to SEBIN, though this has not been declared by the prosecutors in the judicial file.

---

93 Artículo 57 de la Constituición de la Republica Bolivariana de Venezuela: http://www.enoriente.com/constitucion/articulo57.htm

94 http://en.wikipedia.org/wiki/Robert_Serra

95 Global Voices. "Venezuela: Twitter Users Detained After Socialist Party Deputy is Slain". October 22nd 2014. http://globalvoicesonline.org/2014/10/22/venezuela-twitter-users-detained-after-socialist-party-deputy-is-slain/ Accessed March 11th 2015.

96 El Venezolano. "Al menos seis tuiteros venezolanos permanecen presos desde el 2014" [Spanish]. February 15th 2015. http://elvenezolanonews.com/seis-tuiteros-venezolanos-permanecen-presos-desde-el-2014/ Accessed March 11th 2015.

97 Servicio Bolivariano de Inteligencia Nacional (SEBIN) [Spanish] http://www.intelpage.info/servicio-bolivariano-de-inteligencia-nacional-sebin.html Accessed March 11th 2015.

98 Derechos Digitales. "The various paths of Internet censorship in Latin America". November 12nd 2014. https://www.ifex.org/americas/2014/11/12/censura_en_internet/ Accessed March 11th 2015.

99 IPYS Venezuela. "Venezuela: 7 twitteros fueron detenidos por agentes de seguridad del Estado" [Spanish]. October 28th 2014. http://ipys.org.ve/alerta/venezuela-7-twitteros-fueron-detenidos-por-agentes-de-seguridad-del-estado/ Accessed March 11th 2015.

While there is no legal provision in the Venezuelan Penal Code for incarceration for expressing political opinions via social networks, other Twitter users have also been arrested. The person behind the Twitter handle @AnonymusWar has been detained[100] for conspiracy, incitement to hate, assault, hacking, and unauthorized access. His lawyer, however, stresses that his client has been detained simply for having more than 100,000 followers and for expressing opinions against the government in the exercise of his right to freedom of expression.

100 Noticiero Digital. "El Nacional: Seis tuiteros continúan detenidos en el Sebin por sus mensajes" [Spanish]. February 15th 2015. http://www.noticierodigital.com/2015/02/el-nacional-seis-tuiteros-continuan-detenidos-en-el-sebin-por-sus-mensajes/ Accessed March 11th 2015.

Section 2

Private Sector Perceptions on the Use of Encryption, Anonymity and Freedom of Expression

During an intensive timeframe of two weeks in early 2015, the Centre for Internet & Human Rights and the World Wide Web Foundation reached out via phone and email to private sector organisations from over 100 organisations around the world. The survey itself was conducted through an online survey platform in which respondents were asked whether they wished to respond anonymously or not. Given that the vast majority of respondents chose to answer anonymously, we have not provided any additional information about the respondents in this analysis. Despite the relatively short 12-day response time, we received a total of 14 full responses from Europe, North America, and Africa. These responses stem mainly from large international companies, and mainly from the technology sector.

Analysis

Given a non-representative survey design, it is very difficult to draw broad conclusions. What can be suggested, however, is that within this sample of responses, almost all respondents tend to support and value the use of encryption as a technology. However, the perceptions of appropriate ways forward are varied and here the surveys relatively general questions are not well-equipped to elicit a response.

In particular, restrictions on encryption through trade regulation such as the Wassenaar Arrangement[101] and other export control regimes are not mentioned by respondents, nor are existing controls on the usage of encryption in many countries across the globe. Especially after repeated victories in the Crypto Wars,[102] it seems that the full extent of global regulation of cryptography at both a national and international level is not well understood.

It is also notable that most of the private sector organisations that responded do not have a general position on the restriction of cryptography. While most respondents do see the technology positively and for some it is even a core part of their business, the responses of different corporate actors are mixed. As these positions are interesting in and of themselves, we have included some of them here verbatim without attribution to reflect the diversity of opinions and positions.

---

[101] See Maurer, Tim, Edin Omanovic, and Ben Wagner. 2014. *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*. Washington D.C. The paper can be downloaded here: http://newamerica.net/sites/newamerica.net/files/policydocs/Uncontrolled_Surveillance_March_2014.pdf

[102] See Mathieson, SA. 2005. "UK Crypto Regulation Option Dies." *Network Security* 2005(6): 2 and Landau, Susan Eva. 2010. *Surveillance Or Security?: The Risks Posed by New Wiretapping Technologies*. MIT Press.

More than half of the companies providing responses also suggested that restrictions on encryption would negatively affect their relationship with the customers moderately or severely. It should also be noted that two organisations that responded have experienced government attempts at weakening cryptography within their own products or those of their competitors.

In particular, there are questions about what influence lawful interception should have on encryption technologies and whether public controls on some forms of encryption technologies are appropriate. While some respondents believe this is definitely appropriate, other are opposed to regulating encryption in any way. While this likely is a result of different business models, it also reflects diversity of opinion in the business community.

Lastly, it is perhaps most important to remember that among the respondents the majority of the companies (86%) believe they would suffer—either moderately or severely—from a general ban on encryption. This is a clear indication of potential harm from too much regulation of encryption that cannot be ignored by policy makers. Moreover, as such bans already exist in many parts of the world, it is important to also consider existing and future regulation of encryption and what effects such regulation would have.

Notable Company Statements on Restriction Cryptography

The group essentially splits into two groups: the actors who are favourable to some restriction of cryptography in some form or another, and the actors who oppose restrictions. Those responses in opposition to a restriction of cryptography are quite strong, articulating that the organisation is "opposed to restriction on cryptography," or that encryption should "not be restricted in any way."

At the same time, other respondents were more cautious and argued that they "support government control over encryption." Further they "believe in lawful intercept for government use [as they] don't believe in 'every one by themselves' in this important matter." Another respondent argued that "having warranted access to encrypted communications is not the same thing as 'weakening' encryption," while noting that the "interesting questions are around what encryption does to mass surveillance capability, and whether any mass surveillance can be justified as proportionate."

What comes through in all responses is the perceived importance of cryptography as a technology in general and ensuring that it can be used effectively. Cryptography is "essential to the preservation of business secrets and personal privacy" and "a key technical component to realizing […] individuals' security and privacy on the Internet."

Lastly, one private sector organisation responded with a strong statement on this topic outside of the survey:

> "Nokia strongly believes that government surveillance reform is needed to calm international concerns and to reduce the likelihood of individual countries reacting by enacting

requirements leading to fragmentation of the Internet. All governments should immediately put an end to the alleged practice of deliberately weakening Internet security by compromising encryption and other similar means. All countries should stop the bulk collection of private data for government surveillance purposes. Government surveillance must pass the test of necessity, proportionality and legitimacy; and must contain measures for effective, independent and impartial oversight as well as remedial measures. Companies should be allowed to publish the number and nature of government demands, such as lawful interception requests and other similar requests."

General Conclusions

The purpose of our report was to rapidly diagnose the current perceptions and knowledge of key communities about encryption and anonymity. We also intended to identify emerging trends in State practices and regulations around anonymity and encryption in contexts where urban violence and gangs is the narrative used to promote public and political support of surveillance technologies. It was revealing to see the uniformity of global trends against anonymity and the strong support from civil society in certain countries. The report also did a preliminary exploration with the private sector. Although the sample and research time were limited, there are several general trends that emerge from this report:

- **There are knowledge gaps at all levels.**

There is very little knowledge among both business and civil society communities about restrictions to encryption. Moreover, that knowledge is typically incomplete, suggesting that much of the regulation of encryption is barely known, even to relevant organisations.

The knowledge gap is present at all levels. From human rights lawyers to the business sector, there is little to no knowledge on how policies such as SIM registration harm privacy and pose a threat to freedom of expression. While affected communities, such as public interest lawyers litigating cases against the State and corporations, are aware of the importance of anonymity and how useful encryption is to preserve it, they are, in practice, not using it themselves. Furthermore, they seem to know very little about current or upcoming regulation that might hinder their right to communicate in private and there are very few advocacy efforts around the issue. As in the cases of Guatemala and Mexico, advocacy efforts are not supported by broader civil society groups that are advocating for citizen security. At the same time, the academic and policy research in this area is limited and highly centred on Europe and North America. There is little systematic research on either regulations or restrictions to encryption in Latin America, the Middle East, Asia, and Africa. Despite (or perhaps because of) this lack of research, the regimes outside of Europe and North America are typically more restrictive.

- **SIM Card Registration is standard practice in "Global South", and data protection norms are weak.**

As the recently published "Affordability Report" indicates, Latin America[103] is improving not only access but also affordability for users to connect to the Internet. The more connected people are, the more relevant online expression becomes, both politically and socially. According to the Web

[103] See Affordability Report http://a4ai.org/affordability-report/

Index, the proportion of countries whose legal safeguards for privacy are weak or non-existent is 83%[104] which is confirmed by the "Affordability Report." All country cases show a pattern towards restriction of anonymity and weaker safeguards for the right to communicate in private, especially for mobile users. Furthermore, the telephone databases are shared across borders and data localization is becoming a widely used tool to persecute transnational crime.

Data retention is also widespread and there is increasingly alarming administrative procedures for data retention and obligations for Internet service providers to collaborate with authorities. All of this is happening in countries without national or regional legal framework to protect user data. Real-name registration to acquire mobile devices and services is becoming the standardized practice and the criminalization of anonymity is rapidly spreading, especially in the context of protests. The international community is cooperating extensively with the Global South, providing sophisticated surveillance technologies to tackle crime at the expense of citizens' privacy. Most of the surveillance equipment in the region and the training on how to use it are results of cooperation agreements between police bodies across borders.

- **For communities at risk, anonymity and encryption are the only ways to safely communicate and express opinions.**

In contexts in which dissident voices or even just informative outlets are threatened, with widespread self-censorship, independent and anonymous voices are the only ones reporting about sensitive issues. For them, the ability to communicate their ideas anonymously is a matter of life or death. The most visible case of this is Mexico but there are other communities denouncing corruption and exposing both corporate and governmental corrupt practices also using aliases to report. However, the problem they face is again related to a knowledge gap: few are aware that, even if they do not publish their real name online, the technologies leave them exposed. From IP identification to real-time tracking using GPS, people who think they are anonymous ignore that the sensors embedded in new technologies make them more vulnerable and identifiable. The research confirmed that States in the Global South already have sophisticated technologies to track and monitor dissident voices and that they are willing to use it during critical times, when big events or demonstrations are taking place, or when a political crisis unfolds. For people's full enjoyment of their right to privacy, further education and awareness on how new information and telecommunication technologies work is needed for advancing broader encryption adoption.

- **For lawyers, privacy is vital to protect attorney-client information, but encryption is hard to adopt.**

Most of the interviewed lawyers are aware of and worried about the confidentiality of their communications, both ethically and legally. Furthermore, all of them have expressed their frustration as there is no legal remedy to protect themselves and their clients against massive

[104] See The Web Index (2014) thewebindex.org/report/#6.1_privacy_and_surveillance

surveillance from their own governments and from foreign governments. While encryption could be a technical solution to stop their rights from being violated, it is another burden that potentially limits their free exercise of their profession and the right to justice and due process for their clients.

Recommendations

1. It is important to issue recommendations addressing the importance of anonymity and encryption for mobile users.
2. Broader research and better policy for the Global South should be recommended to the academic community.
3. Further coordination with other special rapporteurs, such as the UN Special Rapporteur on right to freedom of peaceful assembly and of association is recommended.
4. It is important to address the right to anonymity and the impact of banning it on communities at risk, such as citizen reporters, whistle-blowers and dissidents.
5. It is important to protect the ability to encrypt for those who have custody of sensitive information, from medical records to legal communications. Regardless the legal safeguards, encryption is the only available tool to keep information truly private.
6. International organizations and international cooperation agencies should address the challenges of urban and citizen security with solutions that don't limit or harm citizens' rights.

I. Annex I - Collaborators Respondents of the Survey in Latin America

The research wouldn't be possible without the collaboration of the Bertha Foundation Be Just Network (http://www.berthafoundation.org/justnet.html) and the following organizations:

Argentina

- Asuntos del Sur - asuntosdelsur.org
- Anonymous contributors

Brasil

- Artigo 19 Brasil - http://artigo19.org/
- Conectas Direitos Humanos - http://www.conectas.org/
- Cultura Digital e Democracia - https://thecdd.wordpress.com/
- InternetLab - http://www.internetlab.org.br
- Intervozes - Coletivo Brasil de Comunicação Social - http://intervozes.org.br/
- Oficina Antivigilância - https://antivigilancia.org
- Open Knowledge Brazil - http://br.okfn.org/
- Representative from Comissão de Direitos Humanos da OABRJ and Coletivo de Advogados
- Anonymous contributors

Chile

- Colectivo de comunicación Mapuche Mapuexpress - mapuexpress.org
- Derechos Digitales - derechosdigitales.org

Colombia

- Fundación Karisma - karisma.org.co
- Fundación para la Libertad de Prensa - flip.org.co
- Anonymous contributors

Ecuador

- Asociación de Software Libre de Ecuador - ASLE - asle.ec
- Asociación para el Progreso de las Comunicaciones (APC) - apc.org
- Colectivo Internet Libre
- Usuarios Digitales - facebook.com/InternetEcuador
- Anonymous contributors

Guatemala

- Nómada - nomada.gt
- Anonymous contributors

México

- ContingenteMX - contingentemx.net
- R3D - r3d.mx
- Anonymous contributors

Perú

- Hiperderecho - hiperderecho.org

Venezuela

- Acceso Libre - accesolibre.red
- Anonymous contributors

II. Annex II – Questionnaires

Questions

1. Do you use encryption when conducting your business transactions with customers, the government or other businesses?
Choose one of the following answers

- ○ **Always**
- ○ **Sometimes**
- ○ **Never**
- ◉ **No answer**

2. If sometimes, in which specific cases do you use encryption and why?

Answer

3. Do you offer encryption technologies as part of your products or services?

- ○ **Yes**
- ○ **No**
- ◉ **No answer**

4. Could your products be developed without encryption to the same quality standard?

- ○ **Yes**
- ○ **No**
- ◉ **No answer**

5. Would your business suffer from a general ban on encryption?
Choose one of the following answers

- ○ **severely**
- ○ **moderately**
- ○ **It will not affect my business model at all**

- ◉ **No answer**

6. Would your business benefit from a general ban on encryption?
Choose one of the following answers

- ○ **Highly**
- ○ **moderately**
- ○ **It will not affect my business model at all**
- ◉ **No answer**

7. Will new restrictions on encryption affect the relations with your customers?
Choose one of the following answers

- ○ **severely**
- ○ **moderately**
- ○ **It will not affect my business model at all**
- ◉ **No answer**

8. Have you experienced governments trying to weaken cryptography in your products or those of your competitors?

- ○ **Yes**
- ○ **No**
- ◉ **No answer**

9. Does your organisation have a general position on the restriction of cryptography?

Answer

10. Which organisation do you represent?

Answer

11. Would you be willing to have your responses attributed to your organisation?

- ○ **Yes**

- ○ **No**
- ◉ **No answer**

Survey to inform the UN Human Rights Council on the use of encryption and anonymity in digital communications (H1)

The United Nations Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression David Kaye, is currently preparing a report on the legal framework governing the relationship between freedom of expression and the use of encryption and anonymous communication.

The report will be presented in June to the Human Rights Council and we are asking for your help, as legal expert, to provide information that allows us to better understand the current situation related to the privacy of communications and the use of encryption and anonymity online in your country. As part of this process the World Wide Web Foundation and the Centre for Internet & Human Rights, in partnership with Oficina Antivigilância, are conducting this survey. We will to compile and analyse the responses and submit them to the Rapporteur by the end of February, 2015.

In many countries in the world, human rights organizations, journalists and political dissidents are targets of surveillance by government intelligence and law enforcement agencies and other non-governmental groups. We hope to gain a better understanding of how human rights groups use encryption and which challenges they face in doing so.

What is encryption?
Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption has the power to authenticate the identity of authors against impersonation and ensure that the messages are not altered in transmission. Encryption is a method to secure communication, it is a crucial enabler of the right to privacy and the right to free expression as set forth in Article 19 of the International Covenant on Civil and Political Rights, ratified by 168 countries in the world.

1. Which organisation do you represent?

2. Do you know what encryption is?

- Yes
- No
- No answer

3. Do you use encrypted communications with your clients?

- ○ Yes
- ○ No
- ◉ No answer

* This can include encrypted emails, websites (HTTPS) or hardware devices which encrypt your communications.

4. How important is encryption for your day-to-day work?

Answer

5. Are any controls maintained by the governments on which organisations or individuals are allowed to use of encryption?

- ○ Yes
- ○ No
- ◉ No answer

6. Are there any controls maintained by your customs on the import of encryption?

- ○ Yes
- ○ No
- ◉ No answer

7. Are there any controls on the export of encryption?

- ○ Yes
- ○ No
- ◉ No answer

* For example software or equipment which include encryption are often controlled.

8. Could you identify the government departments responsible for setting policy on the use, import, or export of encryption?

Answer

9. Are police or other investigative authorities authorized to compel you reveal your private communications by disclosing your passwords or keys?

- ○ Yes
- ○ No
- ◉ No answer

10. Has your government attempted to weaken cryptography or cryptographic standards?

- ○ Yes
- ○ No
- ◉ No answer

11. Does your country attempt to restrict anonymous communications?

- ○ Yes
- ○ No
- ◉ No answer

12. Have you heard about stories, events or investigations related to the usage of encryption or anonymity in the last 5 years in your country?

Answer

13. Would you be willing to have your responses attributed to your organisation?

- ○ Yes
- ○ No
- ◉ No answer

* It would be very helpful for us to be able attach your name to your responses, but we understand if you prefer not to be named.

Annex III
Separate submission by CELE – Argentina

Encryption and anonymity in the digital environment – Argentina

The Center for Studies on Freedom of Expression and Access to Information (CELE) welcomes the opportunity to submit information on the legal guidelines and policies that govern the use of emerging digital technologies in Argentina for the Special Rapporteur's upcoming report.

CELE was created in response to a need to construct spaces for debate and study on the importance of and limits to freedom of expression and access to public information in Latin America. The Center works to protect freedom of expression and access to information as fundamental rights in democratic societies, ones that permit the open debate of ideas and facilitate citizens' full participation in their countries' political and social development. CELE's rigorous investigations and research projects aim to support the work of civil society, journalists, government institutions, and the academic community in promoting the full exercise of these rights.

Recent advancements in encryption technologies have proven pivotal for protecting freedom of expression and anonymity in the digital environment. Efforts to ensure users' capacity to communicate and undertake online transactions securely involve a concurrent commitment to upholding users' right to privacy. In Argentina, however, government institutions have made improper use of the technological developments that are rapidly changing digital information management, leaving users vulnerable to personal data breaches.

Personal data is protected under Law No. 25.326, which was passed in 2000 and restated in Regulatory Decree No. 1558/2001.[105] The Personal Data Protection Law exists to guarantee "comprehensive protection of personal information recorded in files, records, databases, databanks or other technical means of data treatment, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honor and privacy, as well as the access to information" and is overseen by the National Commission for the Protection of Personal

[105] Available at: http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Data. The law defines personal data as any information relating to ascertained or ascertainable individuals or legal entities. However, it does not cover data from opinion polls, statistical research under Law 17.622 (governing the National Institute of Statistics and Censuses), market research, and medical or scientific investigations, so long as the information cannot be linked to an identifiable individual or legal entity.[106]

The law itself does not specify the type of security measures in place for the safeguarding of personal data, though the Commission did lay out mandatory security protocol in Directive 11/2006, which requires that data protection breaches be recorded and classified based on three security levels: basic, medium, and critical.[107]

In spite of Argentina's data protection law that ostensibly aims to preserve the integrity of personal data, government practices at the national level have demonstrated an alarming disregard for individual privacy. Mass surveillance was institutionalized at the national level through a 2011 executive decree that ordered the creation of the Federal System of Biometric Identification (SIBIOS), a centralized, nation-wide ID service that enables law enforcement to "cross-reference" information with biometric and other data that was originally collected for the national ID registry.

The SIBIOS initiative gives the Argentine Federal Police access to the National Registry of Persons (RENAPER) database, making available approximately 14 million digitized fingerprints, with the goal of having all 40 million Argentine citizens registered in the SIBIOS in 2015. Provincial officials have reported increasing progress in the implementation of the SIBIOS initiative and security forces are continually trained to make broad use of the system and its accompanying technologies. The SIBIOS integrates existing identification databases, collecting the digital images, civil status, blood type, and extensive additional background information of citizens. This information may be consulted by a range of other security entities, including immigration authorities, airport security, the National Gendarmerie, and with authorization, provincial security elements. These integrated databases make use of a wide array of new technologies, such as facial recognition identification and mobile fingerprinting devices.[108]

In July 2014, it was reported that Argentines would have to renew their national identity card (DNI) for the third time in five years. Authorities indicated at the time that the new electronic ID card would feature a chip that stores citizens' medical and public transportation history, along with social security information. The upgrade raises significant concerns about privacy

[106] For additional information on the content and scope of the Personal Data Protection Law No. 25.326, see: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf
[107] Available at: http://www.jus.gob.ar/media/33445/disp_2006_11.pdf
[108] See: https://www.eff.org/deeplinks/2012/01/biometrics-argentina-mass-surveillance-state-policy

encroachments, with some technology and civil liberties experts asserting that the new ID card qualifies as one of the world's most invasive surveillance systems, enabling surveillance at a massive scale in real time.[109]

While Argentine authorities have boasted that the new systems leverage emerging digital technologies to improve national security and streamline data collection, CELE contends that these developments jeopardize individual rights to free expression and privacy, as well as the ability to transact anonymously. The collection of sensitive personal information and widespread tracking at the national level could critically undermine citizens' willingness to exercise their right to freedom of expression. Though civil society groups have voiced their opposition to the State's encroachments, there has been minimal public awareness of the increased surveillance. There must be a sustained, coordinated response from stakeholders to encourage government authorities to consider the implications of identification and other new technologies on freedom of expression, data protection, privacy, and anonymity in the digital era.

[109] See: http://panampost.com/belen-marty/2014/07/01/argentinas-national-id-cards-to-store-sensitive-data/