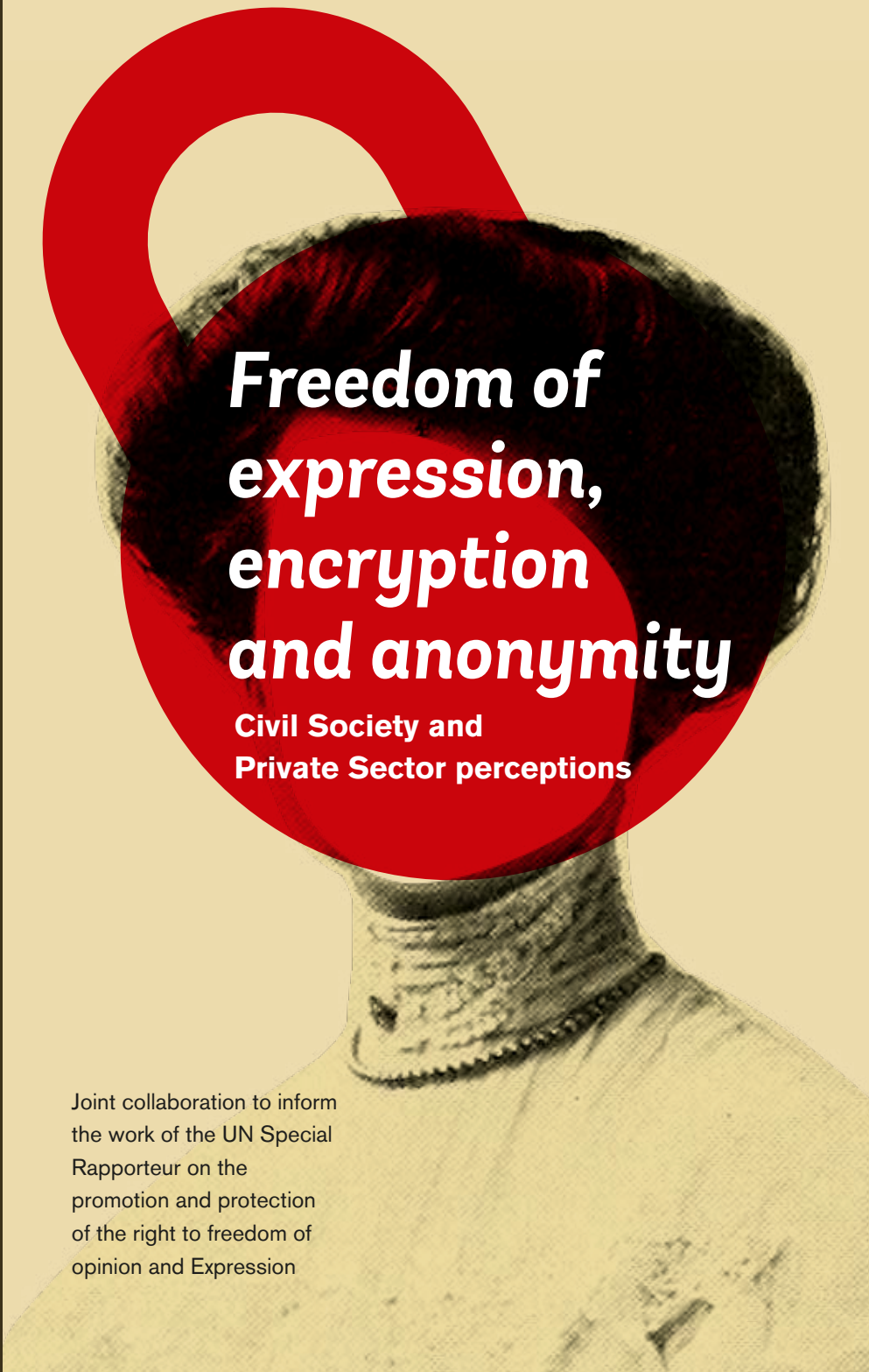

Freedom of expression, encryption and anonymity

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

Freedom of expression, encryption and anonymity

Civil Society and Private Sector perceptions

WORLD WIDE WEB FOUNDATION

CENTRE FOR INTERNET AND HUMAN RIGHTS
https://cihr.eu

OFICINA Antivigilância

DERECHOS DIGITALES América Latina

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

This research was funded by

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 quick and 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 other few countries from the Global South, while debating the relation within encryption, anonymity, and freedom of expression. The work was supported by Bertha Foundation.[5]

The core of the research was based on two different surveys focused on two different target groups. The first was a series of interviews among digital and human rights organizations, potential users of the technologies, to determine the level of awareness on both the anonymity and encryption technologies, to collect perceptions about the importance of these to protect freedom of expression and have a brief overview of the legal framework and corporate practices in their respective jurisdictions. That was conducted in over twenty countries from

1 http://webfoundation.org

2 https://antivigilancia.org

3 http://www.itsrio.org

4 https://www.derechosdigitales.org

5 http://www.berthafoundation.org

the Global South. The second part was an initial consultation with the private sector by conducting over a dozen interviews to document their attitude towards the topic.

Section I
Perceptions from Human Rights and Digital Rights Organizations on the use of encryption, anonymity and freedom of expression

The first section, and core 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 an online questionnaire with 15 questions (Annex III). 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 two weeks period.

It is important to note that, due to the size of the sample, this quick survey is absolutely not intended to be fully representative neither of the region of Latin America, nor of the other countries which submitted answers to the questionnaire. Nevertheless, the results were able to enlighten us with perceptions of several human rights advocates leading at the core front of the debates surrounding Internet freedoms.

I. 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, 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.[7] 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 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

6 This section is partially a contribution by The Center for Studies on Freedom of Expression and Access to Information (CELE).

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

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, though the Commission did lay out mandatory security protocol in Directive II/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 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

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 See [Spanish]: http://www.jus.gob.ar/media/33445/disp_2006_II.pdf

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. A range of other security entities, including immigration authorities, airport security, the 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 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 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 free-

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/

dom 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.

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 that messages could 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], holding 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 anonymity in Secret was not completely warranted because the server of the platform was storing the IP numbers of users, which, ultimately,

12 See [Portuguese]: 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/ (Accesed March 11th, 2015).

could 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 have 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, exceptionally authorities might ask intermediaries for user data to identify them. If that interpretation prevails in Courts, Brazilians will only enjoy some sort of pseudo-anonymity in the context of freedom of expression. Such approach raises particular concerns regarding how this interpretation can be extended

14 See: http://en.wikipedia.org/wiki/Brazilian_Civil_Rights_Framework_for_the_Internet

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).

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 watered down by with the mandatory data retention provision established in article 15 of Marco Civil, which asserts that "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 it 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 episodes in which detained protesters were forced to reveal their social network login and password details. Intelligence agencies and law enforcement authorities have also monitored social networks and Whatsapp, through programs such as Guardião and Mosaico, in addition to allegedly directly contacting intermediary providers of these services to gain access to user data and content of communications which, ultimately, weakens the power of digital tools like cryptography and encrypted standards.[17] That was the case of

16 See: https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf

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).

many people who were detained during protests surrounding the World Cup. Such requests are even made through private security companies[18], such as MODULO[19], which was in contracted to operate with the intelligence center of Rio de Janeiro, accountable 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 from the country, e.g. Sao Paulo[20], Rio de Janeiro[21] and Porto Alegre[22], new laws have been enacted to prohibit the use of masks, and sometimes even helmets and facial painting that could prevent identification of protests. 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

18 Veja. "Empresas de seguraça privada monitoram black blocs" [Portuguese]. March 24th, 2014. http://veja.abril.com.br/noticia/brasil/empresas-de-seguranca-privada-monitoram-black-blocs (Accessed March, IIst 2015).

19 See [Portuguese]: https://www.modulo.com.br/solucoes/gestao-de-eventos-e-incidentes

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

21 Lei 6528. See [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 IIth 2015).

positioned against it.[23] [24]Other organization concerned by civil liberties have also opposed to such measures.[25]

During the demonstrations of 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 telecommunication companies and Internet service providers would have to deliver user data to a broad range of authorities without judicial order[26] within 24hs. After concerns expressed by OAB and associations of telecommunication companies, the decree was modified and this particular provision was removed.[27]

23 Consultor Jurídico. "TJ-RJ considera constitucional proibição de máscaras em protestos" [Portuguese]. November IIth, 2014. http://www.conjur.com.br/2014-nov-11/tj-rj-considera-constitucional-proibicao-mascaras-protestos (Accessed: March IIth, 2015).

24 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 IIth, 2015).

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

26 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, IIth 2015)

27 Telesíntese. "Após polêmica, governo do rio anuncia que

Even though expedite procedure for access to user data was not approved, telecommunications companies are required to store more then connection logs of their user. Though there is no national legislation requiring the registering of SIM cards, there is a technical regulation from the National Telecommunications Agency – ANATEL[28] establishing that mobile service providers should keep the following data about their users: a) name; b) ID or tax number; c) address. The regulation also establishes that users have the duty to maintain their information up to date within the providers. Therefore, it is impossible to use a SIM card, even if pre-paid, without registering, once users who refuse to provide information may have the service suspended. On the other hand, as the country still don't have a legislation on data protection, it is unclear how this database is being protected and treated, another aspect that highlights the major importance for approving a strong bill on data protection.[29]

3. Chile

In Chile, there have been some drastic cases where privacy and (pseudo) anonymity on social media platforms have been

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 IIth, 2015)

28 Resolução ANATEL 477/2007. See [Portuguese]: http://legislacao.anatel.gov.br/resolucoes/22-2007/9-resolucao-477

29 See [Portuguese]: http://participacao.mj.gov.br/dadospessoais/

violated by law enforcement agencies[30] to threaten freedom of expression. Important part of those 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[31], there have been an interesting public debate about the right to be hooded in these instances[32], because of 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"[33] (known as the Hinzpeter's bill) which was especially hard on masked protesters[34], increasing the penalties for offenses of public

30 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).

31 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).

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

33 See [Spanish]: http://congresoabierto.cl/proyectos/7975-25

34 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).

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 caused a huge controversy in the public opinion[35] as it is effectively criminalizing the right to protest[36], but, even though it has little chance of approval, it has not been formally withdrawn.

Even though the national controversy on the Hinzpeter's bill, in 2014, members from within the country's largest opposition party submitted a bill[37] proposing greater punishment for those who cause destruction during public protests and to give law enforcement wider powers in dealing with offenders. María José Hoffman, one of the representatives who submitted the bill, said[38]: "This new attempt to eradicate violence during

35 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).

36 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).

37 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).

38 Publimetro. "Diputados UDI ingresan nuevo proyecto en contra de encapuchados" [Spanish]. July 16th, 2014. http://

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[39] in order to identify other protesters. In May of 2014, the Justice Department dismissed an investigation[40] of a young man accused of assaulting a police officer after a protest for the International Workers' Day, resulting from the presented evidence being based on facial recognition from Facebook photos and therefore inconclusive. In fact, the Judge "called [for] the prosecutor to be more serious in carrying out the investigations". In June 2014, the Cybercrime Brigade explained[41] to a local newspaper that they make a "digital registration" in social media in order

www.publimetro.cl/nota/politico/diputados-udi-ingresan-nuevo-proyecto-en-contra-de-encapuchados/xlQngq!COSsdL97Qe4E6/(Accessed March IIth, 2015).

39 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/ (Accesed March IIth, 2015).

40 Derechos Digitales. "La fiscalía está revisando tu Facebook" [Spanish]. May 29th, 2014. https://www.derechosdigitales.org/7418/la-fiscalia-esta-revisando-tu-facebook/ (Accesed March IIth, 2015).

41 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/ (Accesed March IIth, 2015).

to help their investigations, without specifying what it is and 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[42] 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 erroneous and unfounded report wrongly linking Ferrari with all three accounts.[43]

The Twitter account @losluksic was created with the express 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 two other accounts put Ferrari in trouble. For months he was under pressure to reach an agreement or conditional suspension; he was eventually acquitted of the charges, but was never compensated for the dismissal of due process and privacy.[44]

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

43 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/ (Accesed March 11th, 2015).

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

SIM Card registration is still not mandatory in Chile, however a draft bill[45] 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" should 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[46] 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 will 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. [47]

45 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).

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 3, 2015. http://congresoabierto.cl/proyectos/9894-15 (Accessed March 12th, 2015).

47 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 3, 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 biggest 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 the protest by the police.[48]

Since 2011 there is a mandatory requirement[49] 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, as, according to a resolution[50] issued by Ministry of Defense and Direction of Criminal Investigation of the National Police, 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; h) Acti-

48 Decree N° 2254 of 2013, Alcaldía de Medellín. Gaceta 4203. See [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

49 Decree 1630 of 2011. See [Spanish]: http://www.mintic.gov.co/portal/604/articles-3558_documento.pdf

50 Resolution 912 of 2008. See [Spanish]: https://www.redjurista.com/documents/r_mdef_0912_2008.aspx

vation date. In case of changes, telecommunications service providers must send updates to DIJIN every month.

Colombia has a long and running history of illegal interception of communications that affected opposition leaders, high court judges, journalists and human rights activists. For these actions, the ex-director of "Departamento Administrativo de Seguridad" - DAS (Colombian security agency, now disbanded) and ex-secretary of Government were found guilty[51] 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 2013 Intelligence and Counterintelligence Act intended to prevent cases such as these, a year later a new case of illegal communications surveillance was discovered. In February 2014, Semana revealed[52] that an undercover military intelligence unit not only executed an illegal operation, but also served as a center for the interception of electronic communications targeted at government and Fuerzas Armadas Revolucionarias de Columbia (FARC) representatives in the Peace Talks taking place in Havana, Cuba.

51 Semana. "Chuzadas del DAS: crimen y castigo" [Spanish]. February 2nd, 2015. http://www.semana.com/nacion/articulo/chuzadas-del-das-crimen-castigo/419365-3 (Accesed March 11th, 2015).

52 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 (Accesed March 11th, 2015).

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[53] 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 competent authority.

5. Cuba

Cuba regulates de use of cryptographic technologies. Citizens need a permit from the Ministry of interior in order to protect their communications using cryptography. The Ministry of Interior can only authorize the distribution, promotion, research, training and exchange of encryption technologies. This applies for foreign and local individuals and entities. Cuban authorities also regulate the use of cryptographic algorithms. It is forbidden to use unauthorized cryptographic algorithms. Only

53 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).

algorithms developed by the Ministry of Interior can be used.[54]

6. Ecuador

The persecution of anonymity on the Internet is not something new in Ecuador. The new Communications Law, enacted in 2013[55], holds publishers liable for their comment sections, users have to register under a real name policy, and therefore its ability to remain anonymous cannot be exercised when commenting[56]. 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 regulation of social media in cases of hate speech[57], instead of regulating it, the administration has opted for a public campaign using state media to criticise anonymity. During the Presidential weekly

54 Cuban regulation on encrypted communications. See: http://www.di.sld.cu/documentos/resol/DL_199.pdf

55 See [Spanish]: http://www.derecho-ambiental.org/Derecho/Legislacion/Ley_Organica_Comunicacion_Ecuador_2013.html

56 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/(Accesed March 11th, 2015).

57 Periodismo Ecuador. "Alexis Mera propone regular Redes Sociales en casos de calumnias" [Spanish]. August 18th, 2013. http://periodismoecuador.com/2013/08/28/alexis-mera-propone-regular-redes-sociales-en-casos-de-calumnias/ (Accesed March 11th, 2015).

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.[58]

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 by those who want to discredit him, but the satirical work of this anonymous user has been strongly supported by citizens, which has made of this incident a national controversy.[59]

After the incident, and as Global Voices reported[60], Crudo Ecuador's Twitter account was temporarily suspended on January 28 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 Crudo Ecuador said the account had been closed by "government trolls." Fearing for his life, the administrator of the site has

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

59 BBC News. "Ecuador President Rafael Correa's troll warfare". January 30th, 2015. http://www.bbc.com/news/blogs-trending-31057933 (Accesed March 11th, 2015).

60 Global Voices. "Ecuadorian President Threatens Internet Satirists". February 17th, 2015. http://globalvoicesonline.org/2015/02/17/ecuadorian-president-threatens-internet-satirists/ (Accesed March 11th, 2015).

recently announced[61] that he is shutting down the website and 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[62] 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"[63] 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. One of the most serious and organized efforts in this direction is "Crypto Party"[64] events.

61 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/ (Accesed March 11th, 2015).

62 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).

63 See: http://somosmas.ec/

64 See: http://cryptoparty.ec/

Besides the attack 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 mandatory registration of cellphones under penalty of suspension.[65] Users must provide full name, address, ID number and for validation purposes, the year of issue of the document. 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 "Servicio Móvil Avanzado."[66] Data can be requested by competent authorities in accordance with the requirements and procedures of the law.[67]

65 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).

66 ARCOTEL. "Servicio Móvil Avanzado" [Spanish]. http://www.arcotel.gob.ec/servicio-movil-avanzado/ (Accessed March 12th, 2015).

67 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). Addtional information in "Resolución Tel-535-16-CONTEL.2012". See [Spanish]: http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/0535_tel_18_conatel_2012.pdf

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.[68]

7. Guatemala

In Guatemala and for a period of two years, a broader group of civil society organizations advocated for the compulsory registry of SIM Cards and equipment launching a multimedia campaign.[69] The increased of armed theft and phone calls threatening citizens with extortion[70] 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 pads. The law was approved[71] with little opposition from citizens and extended

68 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).

69 "Ley de Celulares". See [Spanish]:https://web.archive.org/web/20130921164526/http://www.leycelulares.com/index.php/comparacion

70 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).

71 "Ley de Equipos Terminales Móviles". See [Spanish]: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs

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 approved yet a data protection law. While apps are not regulated, the social application SECRET sparkled controversy during 2014, when the Vice President threatened to regulate social networks, in order to protect the morality of women and children.[72]

8. Mexico

In Mexico, we can observe 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 illegal organized criminal activity. In the border state of Tamaulipas alone, from the period between 2010 and October 2014, 27 bloggers have reportedly been killed.[73]

Anonymity, or pseudo-anonymity, has been a partial solution to enable citizens to keep channelling denouncements. For instance, the website Valor por Tamaulipas[74] was founded by an anonymous user with the goal of sharing information regarding

leyes/2013/pdfs/decretos/D08-2013.pdf

72 Digital Rights LAC. "Secret shakes Guatemalan society". October 29th, 2014. http://www.digitalrightslac.net/en/secret-sacude-a-sociedad-guatemalteca/ (Accessed March 11th, 2015).

73 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).

74 See: http://www.valorportamaulipas.info/

drug-related violence within the State through social media. With 556K Facebook "likes"[75] and 122K followers on Twitter[76], the initiative survives mostly due to anonymity. However, it is not immune to threats and sad histories. In 2013, a drug cartel offered rewards 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[77] by the cartel, who later hacked into Fuentes Rubio's account and posted threats to other citizen journalists using social networks.

Another alarming example is of 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 and made several denouncements, including that of the purchase of an online surveillance tool[78] called "Black Eyed Hosting" by the Public Attorney (Procuradora General de Justicia de Estado-PGJE). The Mexican blog Información

75 See: http://facebook.com/ValorPorTamaulipas

76 See: http://twitter.com/valortamaulipas

77 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 (Accesed March 11th, 2015).

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

de lo nuevo[79] suggested that law enforcement officials had been monitoring Maldonado's activities using this tool[80] and charged him under minor drug-related offenses[81]. Maldonado's arrest took place 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[82] at

79 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 (Accesed March 11th, 2015).

80 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/ (Accesed March 11th, 2015).

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

82 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/ (Accesed March 11th, 2015).

least until September 2013. The Reforma newspaper found[83] 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 in disregard of anonymity also goes from online to offline environment. 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; others authorities have declared the necessity to increase the penalties for those who commit crimes with their faces covered. Indeed, though 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[84], 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 geo-location data from mobile phone companies. While privacy

83 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 (Accesed March 11th, 2015).

84 See [Spanish]: http://mexicosos.org/descargas/dossier/legislacion/ley_geolocalizacion.pdf

activists were against the law[85], other civil society groups advocating for citizen security were supportive of the law, which reflects the tensions between the two groups in the region.

9. Peru

Even though that the right of freedom of movement and the right of assembly don't require prior identification in Peru, in the last months of 2014 there were public declarations[86] from Daniel Urresti, Interior Ministry who has in charge the Peruvian police, in order to impose "de facto" restrictions on anonymity in rallies. For a protest in last December, he stated[87] that hooded protesters wouldn't be allowed to participate in the manifestation; and announced that police would ask for the national identification card to the attendees.[88] These kind

85 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/ (Accesed March IIth, 2015).

86 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 IIth, 2015).

87 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 IIth, 2015).

88 El Comercio. "Urresti puso reglas para protesta de hoy contra régimen juvenil" [Spanish]. December 22nd,

of proposals have been quickly condemned by civil society,[89] gremial associations[90] and even by other session of the government,[91] pointing out that these measures are criminalizing the social protest.

Nevertheless, other form of mandatory identification have also been implemented by law. Since 2010, all SIM cards are associated with the National ID Card.[92] People have to 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

2014. http://elcomercio.pe/lima/ciudad/daniel-urresti-ley-pulpin-reglas-protesta-hoy-contra-regimen-laboral-juvenil-noticia-1780080 (Accessed March 11th, 2015).

89 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).

90 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).

91 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).

92 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).

are kept by the company for billing purposes and marketing and is shared with State authorities. Next step will be that by mid-2015 users' identity will be verified by biometric fingerprints,[93] measures, that, ultimately, do not prevent that people use other peoples phone to commit ilegal acts, while it does represent a bigger risk for citizens privacy, due to unecessary collection and storage of sensitive user data.

10. Venezuela

According to Venezuelan Constitution, anonymity is prohibited in the context of freedom of expression[94] and covering faces during a manifestation 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 telecommunication companies register the IMEI number of mobile devices to their users ID. The argument for imposing such requirement has been to reduce mobile robbery, but, according to interviews, there is not evidence or 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 have been considered

93 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 (Accesed March 11th, 2015).

94 See [Spanish]: http://www.enoriente.com/constitucion/articulo57.htm

illegal in some cases, leading to prosecution. havista deputy Robert Serra[95] was murdered in Venezuela, at least 8 Twitter users, some operating under pseudonymous, were detained by Venezuelan authorities[96] for making political comments against Serra or about his death which allegedly tied them to the murder, according to Police (to date, only two detainees have been released).[97] All eight were transferred to a branch of the Venezuelan intelligence service, the Servicio Bolivariano de Inteligencia Nacional (SEBIN).[98] The news portal, Infobae, was blocked for posting content about the arrest.

The ruling party parliamentarian, Christian Zerpa, has confirmed that these detentions occurred because detainees "made fun" of the assassinated politician.[99] In many of these cases, the legal defense of these Twitter users has alleged

95 See: http://en.wikipedia.org/wiki/Robert_Serra

96 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/ (Accesed March 11th, 2015).

97 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/ (Accesed March 11th, 2015).

98 See [Spanish]: http://www.intelpage.info/servicio-bolivariano-de-inteligencia-nacional-sebin.html

99 IFEX. "The various paths of Internet censorship in Latin America". November 12nd, 2014. https://www.ifex.org/americas/2014/11/12/censura_en_internet/ (Accesed March 11th, 2015).

that the detentions were without a warrant. In the case of Inés Margarita González Árraga (@inesitaterrible), her legal defense reported[100] that she voluntarily handed over her personal computer to SEBIN, though this has not been declared by the prosecutors in the judicial file.

While there is not a 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[101] for conspiracy, incitement to hate, assault, hacking, and unauthorized access, while his lawyer stresses that he has been detained for merely having more than 100K followers and has issued opinions against the government in the exercise of his right to freedom of expression.

100 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/ (Accesed March 11th, 2015).

101 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/ (Accesed March 11th, 2015).

Section 2
Private sector perceptions on the use of encryption, anonymity and freedom of expression

Over the last two weeks, the Centre for Internet & Human Rights and the Web Foundation reached out via phone and email to private sector organisations from over 100 organisations across the world. The survey itself was conducted through an online survey platform where respondents and asked whether they wished to respond anonymously or not. As the vast majority of respondents' preferred anonymous responses we have not provided any additional information about the respondents in this analysis. Despite the relatively short 12-day response time, we have received a total of 14 full responses from Europe, North America and Africa. These responses stem mainly from large international companies, mainly from the technology sector.

Analysis

Given a non-representative survey design it is very difficult to draw broad conclusions for industry from this. 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 diverse 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[102] and other export

102 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/

control regimes are not mentioned by respondents, nor are existing controls on the usage of encryption in many countries across the world. Particularly after repeated victories in the crypto-wars[103] it seems that the full extent of global regulation of cryptography at both a national and international level remains little 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 some even as core to 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.

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. Also it should 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

policydocs/Uncontrolled_Surveillance_March_2014.pdf

103 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.

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 from a general ban on encryption either moderately or severely. This is a clear indication of potential harm created by 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 as well as additional potential regulation of encryption and what effects such regulation could have.

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

At the same time other respondents are more cautious and argue 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 them selves" in this important matter." Another respondent argues "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 believe 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. It also intended to identify emerging trends in State practice and regulations around anonymity and encryption in contexts were the discourse about 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:

Knowledge Gap at all levels

The first is that there is very little knowledge among both business and civil society communities about restrictions to encryption. Moreover what knowledge there 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 non existence 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 not using it. Furthermore, they seem to know very little about current or upcoming regulation that might hinder their right to communicate in private and there are only few advocacy efforts around the issue. Those usually, as in the case of Guatemala and Mexico, are not supported by broader Civil Society groups 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 both regulations and 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 as Standard "Global South" practice, weak data protection norms

As the recently published "Affordability Report" indicates, Latin America[104] is increasing not only the access but the affordability for users to connect to the Internet. The more connected, the more relevant online expression becomes, both politically and socially. According to the Web Index, the proportion of countries whose legal safeguards for privacy vary from weak to non-existent is 83%[105] and it is confirmed by the 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 in countries without national and regional legal frames to protect the data of users. 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 protest.
The International community is vastly cooperating with the

104 See: http://a4ai.org/affordability-report/

105 The Web Index (2014). See: http://thewebindex.org/report/ - 6.1_privacy_and_surveillance

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 were dissident voices or even just informative outlets are threatened, with widespread self censorship, independent, 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 alias to report. However, the problem they face is again related to a knowledge gap: few are aware that, even if they do not use their real name to publish online and in social media platform, the technologies leave them exposed, from IP identification to real time tracking using GPS, those 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 the full enjoyment of rights, further education and awareness on how new information and telecommunication technologies work is needed as a precondition of 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. However, all of them have expressed their frustration as there is no legal remedy to protect them against massive surveillance from their governments and from foreign governments. While encryption could be a technical solution to stop their rights being violated, it is another burden limiting their free exercise of their profession and the right to justice and due process of 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 Special Rapporteur UN special rapporteur on right to freedom of peaceful assembly is recommended.
4. It is important to address the right to anonymity and the impact of banning it for communities at risk, such as citizen reporters at risk, whistle-blowers and dissidents.
5. Furthermore, it is important to protect the ability to encrypt for those who have a duty of custody of sensitive information, from medical records to legal communications, regardless the legal safeguards, encryption is the only available tool to truly keep it 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.

Annex I - Collaborators respondents of the survey in Latin America

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

Argentina

- Asuntos del Sur - asuntosdelsur.org
- Anonymous contributors

Brasil

- Artigo I9 Brasil - http://artigoI9.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