Freedom of Expression and the Private Sector in the Digital Age

Latin America Report for the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression.

January, 2016.

Introduction

This report presents a summary of some examples where the private sector in Latin America has had an important role protecting or undermining the right of freedom of expression of users. These next pages not intended to be an exact portrait of the Latin American situation, but is an effort to understand the kind of responsibility that the private sector have with human rights in developing countries.

Brief regional context on private sector in the digital age

The privatization processes in Latin America began in the mid-seventies in Chile, followed by other countries in the region in the late 80s: "Latin America is the region that most state enterprises were sold worldwide since the former prime minister Margaret Thatcher began with privatization in Britain in the mid of the last decade. Latin America surpasses Europe and Asia in terms of number of companies that were sold with more than a third of the privatization processes that have been made in the world in the last twelve years".[1] The first two waves of popular privatizations in the region are, first, the industrial sector, and then the ones related to infrastructure such as telecommunications, electricity and roads services.

In fact, Latin American countries privatized and restructured their telecommunications industries to a more radical degree than any other region during the 80s-90s:[2] Telecommunications increased in importance around the same time that most Latin America political leaders were abandoning nationalist ideas about the role of the state in the economy in favor of liberal economic reform.[3] However, the preoccupation has arisen regarding the concentration of the market because only two transnational companies took over the telecommunication market: Telefónica España and Grupo Carso Global Telecom (Telmex and América Móvil's owners).[4]

In this context, as Consumers International has stated[5], the highest percentage of consumer complaints in the region are regarding mobile phones, and in few countries is behind claims against banks and financial institutions. This is especially significant when, according to the GSMA analysis from 2015,[6] within five years Latin America will occupy the second place worldwide in terms of the installed base of smartphones. In fact, the region has the fastest growing internet population in the world, surpassing Asia with a 50 % penetration;[7] moreover, regarding time on social networks, people

[1] Rafael Pampillón (1998). Los Procesos de Privatización en América Latina (de la sustitución de importaciones a la eficiencia productiva), unofficial translation. http://dspace.ceu.es/handle/10637/575
[2] Luis Gutiérrez y Sanford Berg (1998). Telecommunications Liberalization and Regularuty Governance: Lessons from Latin America.
[3] Sybil Rhodes (2006). Social Movements and Free-Market Capitalism in Latin America: Telecommunications Privatization and the rise of Consumer Protest. State University of New York Press.
[4] ECLAC (2005). Organización industrial y competencia en las telecomunicaciones en América Latina: estrategias empresariales. http://archivo.cepal.org/pdfs/2005/S05930.pdf
[5] Consumers International (2014). Telefonía móvil en América Latina: Hablan los consumidores. http://es.consumersinternational.org/media/1465668/publicaci%C3%B3n-dmdc-2014-%C3%BAltima-versi%C3%B3n-carta-p.pdf
[6] El País (2015). El milagro móvil en América Latina. http://economia.elpais.com/economia/2015/08/27/actualidad/1440698867_622525.html
[7] The Park Group (2015). Social Media in Latin America 2015 http://www.thesparkgroup.com/social-media-latin-america-2015/

in the region spend ten hours on average, five hours more than the rest of the world. Also they are 20 % of Facebook users worldwide and nearly 40 % of WhatsApp.[8] In this context, social networks and other digital tools have been fundamental for social movements.[9]

Despite these numbers, Latin America's role in the global software and services industry is not yet compatible with its economic importance, but gradually expands due to its growing domestic market and export opportunities arising with outsourcing trend: Uruguay, Brazil and Chile are the most prominent countries in this industry.[10]

[8] Alan Lazalde (2015). Internet en América Latina. http://blogs.cccb.org/lab/es/article_internet-a-lamerica-llatina/

[9] Emiliano Treré & Claudia Magallanes-Blanco (2015). Battlefields, Experiences, Debates: Latin American Struggles and Digital Media Resistance. http://ijoc.org/index.php/ijoc/article/download/3407/1509

[10] Paulo Bastos Tigre & Felipe Silveira Marques (2009) Desafíos y oportunidades de la industria del software en América Latina.
http://repositorio.cepal.org/bitstream/handle/11362/1989/S33826D4412009_es.pdf?sequence=1

Surveillance firms

The business of surveillance and its impact on human rights

Description:

In recent years, different news, reports and leaked documents have confirmed the presence of international surveillance firms selling malware to local governments in Latin America. Even though governments believe that this kind of technology can be used for the legitimate purpose of criminal investigations and intelligence gathering, with no proper oversight these tools can be used to compromise journalists, human rights defenders and political opponents.

Some of the surveillance firms which are known to operate in Latin America are:

1) **Gamma International:** At the beginning of 2014, an initial report from Citizen Lab detected the presence of FinFisher, a surveillance malware sold exclusively to governments, in countries as Mexico and Panama. A recent report from 2015 confirmed the malware's presence in Mexico, Venezuela and Paraguay.[11]
2) **Hacking Team:** The massive emails' leak from the Italian company Hacking Team, shed a light on the sales made by this surveillance firm in countries as Brazil, Chile, Colombia, Ecuador, Honduras, Mexico and Panama. "Remote Control System", Hacking Team's key product, is a malicious software presented to the user as a genuine and harmless software but when executed gives the attacker remote access to the infected device for both computers or smartphones.
3) **M.L.M. Protection**: Israeli surveillance firm who sold long-range interception technology in 2010 to Panama Government, enabling it to tap into computers and cellphones from a distance and record almost any content, including text messages and communications sent via applications such as WhatsApp and Blackberry Messenger.

Their sales are problematic for several reasons, but especially because these technologies have been used against journalists, human rights defenders and political opponents. Two examples:

1) **Panama**: During the presidency of Ricardo Martinelli in Panama (2009-2014) approximately 150 people had been spied upon by the government, including politicians, journalists, trade unionists, businessmen, and civil society leaders. The current government began an administrative investigation last year into the illegal interception of telephone and internet communications during the Martinelli era. For Catalina Botero, former Special Rapporteur on freedom of expression for the Inter-American Commission on Human Rights (IACH), "this type of espionage has a dramatic effect on human rights. [...] First, there is an affectation of the right to

[11] Citizen Lab (2015). Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

privacy. If that expectation is lost, it damages many of the rights that must be defended in a democracy".[12]

2) **Mexico**: This country is by far the biggest paying client of Hacking Team: at least 14 states and government agencies have hired the company's services since 2010. A day after the leaked documents began circulating, Mexico's minister of the interior, Miguel Angel Osorio Chong, acknowledged the government had hired Hacking Team's services, but that it occurred during the administration of the previous president, Felipe Calderon. However, leaked documents tell a different story, with CISEN, Mexico's civil national-security intelligence service, listed as one of Hacking Team's active clients.[13] Even though hacking software like FinFisher has helped the government's drug war efforts, activists are worried of the potential use for domestic spying and for the lack of debate about how and when these tools should be used.[14] Later reports found that in the state of Puebla, the government employed the Hacking Team's tool to spy on political opponents and journalists: first, to monitor the campaign headquarters of an opposition politician called Ernesto Cordero and then several journalists.[15]

All these companies are from overseas and sell targeted surveillance services. However, there are public reports regarding the selling of mass surveillance software to local governments as Brazil and Uruguay.

1) **Digitro Tecnología Ltda.:** This Brazilian company sold a mass surveillance software named El Guardián (The Guardian) to the Uruguayan Government. The cost of the software licence was USD 2 million and there is a yearly service fee of USD 200,000. The Guardian is a system designed to monitor several networks, allowing up to 30 people to work simultaneously on mobile phones, landlines and emails.[16] Digitro also provides services in Brazil: The Brazilian Federal Police has admitted that they use the software to monitor social media.[17]

This kind of mass surveillance has been under the radar for local activists in Brazil and Uruguay. Its consequences in the freedom of expression is one of their main concerns.

1) **Uruguay**: Local authorities have reassured the media that the surveillance software will be used within the traditional legal framework, which implies that the judiciary would need to authorise surveillance activities.[18] However, local activists remain

[12] La Prensa (2015). Phonetapping Scandal Brings Down Martinelli Officials https://panampost.com/elisa-vasquez/2015/01/14/phonetapping-scandal-brings-down-martinelli-officials/
[13] Vice News (2015). Mexico Is Hacking Team's Biggest Paying Client — By Far. https://news.vice.com/article/mexico-is-hacking-teams-biggest-paying-client-by-far
[14] Fusion (2015). The Hacking Team leak shows Mexico was its top client, but why? http://fusion.net/story/163872/the-hacking-team-leak-shows-mexico-was-the-top-client-but-why/
[15] Animal Político (2015). El gobierno de Puebla usó el software de Hacking Team para espionaje político http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/
[16] Global Information Society Watch (2014). Penumbra: Surveillance, security and public information in Uruguay. https://www.giswatch.org/en/country-report/communications-surveillance/uruguay#_ftn11
[17] Convergencia Digital (2013). Exército usou software Guardião para monitorar redes sociais. http://wap.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34302&sid=11#.U5ZMmS9htb0
[18] 180 (2013). Gobierno: guardián centraliza vigilancia electrónica pero mantiene garantías. http://www.180.com.uy/articulo/34766_Gobierno-guardian-centraliza-vigilancia-electronica-pero-mantiene-garantias

sceptical. They are worried about who is going to use this program, on what terms, under what procedures, how will be implement it with telephone companies and how judges are being prepared to use these tools.[19]

2) **Brazil:** As the researcher Fabrizio Scrollini stated "several accountability agencies are worried about the extent to which the software is being used on its civilian population and how exactly several state units at the national and state level are using it. For instance, there were concerns that it was used in the context of the last Confederations Cup football tournament in Brazil, and the social unrest that erupted in several cities".[20]

Key legal policy issues:

- **Purchase's legality:**

The Mexican Constitution states that only the federal authorities with statutory powers may ask the judge for the intervention of communications. Thus, for instance, Hacking Team's software purchased by the states of Jalisco, Queretaro, Puebla, Campeche and Yucatan is illegal because they are not federal authorities and have no legal authority to engage in espionage or even ask the judge to intercept communications.

As an Italian company, Hacking Team's technologies are now subject to European Union export restrictions. The EU developments are grounded in agreements made in December 2013 that subjected intrusion software to the Wassenaar Arrangement, an export-control regime for dual-use technologies involving forty-one countries. As Privacy Internacional asserts, in its branding and communications materials, Hacking Team claims to have understanding of the "potential for abuse of the surveillance technologies" and asserts its complying with international standards including the Wassenaar Arrangement protocols.[21]

However, the Mexican example shows how easily this kind of companies use measures to circumvent the legal framework. In order to sell surveillance software, Hacking Team's option is to use the intervention of third parties in the purchase: companies as SYM Servicios Integrales or TEVA (Queretaro) allow Hacking Team to sell software to intermediaries and not directly to public authorities. The consequences in a country with a human rights crisis as Mexico[22] can be severe.

As James Mamford said: "The privatization of mass surveillance is the result of weak export controls and voluntary international agreements regarding invasive spyware. The only mechanism for regulating spying systems is the Wassenaar Arrangement, which allows for countries to regularly exchange information on transfers of conventional weapons and dual-use

[19] Declaración conjunta sociedad civil uruguaya (2014). Vigilancia, seguridad y privacidad: llamamiento para que Uruguay adopte estándares de derechos humanos. http://www.mjackson.uy/wp-content/uploads/2014/12/Declaraci%C3%B3n-10-de-diciembre-2014_Vigilancia-Seguridad-Privacidad.pdf
[20] Global Information Society Watch (2014). Penumbra: Surveillance, security and public information in Uruguay. https://www.giswatch.org/en/country-report/communications-surveillance/uruguay#_ftn11
[21] Privacy International (2015). Briefing for the Italian Government on Hacking Team https://privacyinternational.atavist.com/hackingteamsurveillanceexports
[22] IACHR (2015). Preliminary Observations on the IACHR Visit to Mexico http://www.oas.org/en/iachr/media_center/PReleases/2015/112A.asp

goods and technologies. But it is nonbinding on its 41 signatories, including the United States, and Israel has never formally agreed to its terms".[23]

- **Legality of the use**:

As has been stated previously in this report with the examples of Mexico and Panama, this kind of surveillance technologies have been used to spy on activists, journalists and political dissidents. While monitoring can legitimately being exercise with clear objectives, it is necessary to delimit concepts of "national security" and "public order" to prevent illegitimate purposes in the context of espionage activities. Its application should be allowed only where there is some risk with respect to the protected interest and where that harm is greater than the general interest of society in terms of upholding the right to privacy, freedom of expression and free flow of information.

Not just surveillance purposes should be monitored, but also the means by which this activity is carried out. For some Mexican activists, in theory there have been over 50,000 interventions that did not have a court warrant in the case of surveillance with FinFisher malware.[24] Also, people are not notified after the government snoops on them, nor can they find out, making it almost impossible to bring a case to court.[25] Meanwhile in Chile the Hacking Team leaked emails showed the intentions of local authorities to use the software without warrants.[26] For local activists the data get from Hacking Team's software could not be used as evidence if they have been achieved without meeting the strict standards set in criminal proceedings.[27]

Decisions to conduct surveillance that can encroach privacy of individuals must be authorized by impartial and independent judicial authorities, with independence from those responsible for monitoring communications. Judges must follow the criteria of due process and the principles of necessity, appropriateness and proportionality.

- **Transparency and accountability:**

In democratic states additional explanations for a better understanding of the public spending in technologies highly abusive on people's rights must be done. Thus, the intervention from the State must be justified and just for exceptional cases, following due process, and with mechanisms for transparency and accountability that can allow external control over the State's surveillance capacities. States should disseminate, at least, information on the regulatory framework of the monitoring programs; the parties responsible for implementing and monitoring these programs, procedures for authorization,

[23] Foreign Policy (2016). U.S. firms are making billions selling spyware to dictators. https://foreignpolicy.com/2016/01/22/the-espionage-economy/
[24] El Economista (2015). Vulneración a Hacking Team confirma abuso de espionaje en México. http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico
[25] Reuters (2015). Mexico ramps up surveillance to fight crime, but controls lax. http://www.reuters.com/article/us-mexico-surveillance-idUSKCN0S61WY20151012
[26] CIPER (2015). Los correos que alertaron sobre la compra del poderoso programa espía de la PDI http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi/
[27] Derechos Digitales (2015). Hacking Team: La era dorada de la vigilancia. https://www.derechosdigitales.org/9292/la-era-dorada-de-la-vigilancia/

data management, as well as information on the use of these techniques, including aggregate data on its scope.[28]

As Citizen Lab has asserted referring to FinFisher, "the market for intrusion software is challenging to track because the key players, from government customers to software developers, have a strong interest in keeping transactions private".[29] Despite of this, governments and surveillance companies must to engage in a culture of transparency and respect for human rights.[30]

[28] Declaración conjunta sociedad civil uruguaya (2014). Vigilancia, seguridad y privacidad: llamamiento para que Uruguay adopte estándares de derechos humanos. http://www.mjackson.uy/wp-content/uploads/2014/12/Declaraci%C3%B3n-10-de-diciembre-2014_Vigilancia-Seguridad-Privacidad.pdf

[29] Citizen Lab (2015). Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

[30] Privacy International (2012). Surveillance companies: real responsibility goes beyond the letter of the law. https://www.privacyinternational.org/node/330

Internet Service Providers

ISPs' role in surveillance activities

Description:

As mentioned above (Surveillance Firms section), Uruguayan and Brazilian governments use a mass surveillance software named The Guardian. Authorities in Uruguay have explained the procedure behind its use, saying that first the police makes a request, then the prosecutor reviews it, and finally the judge is who authorizes it. After this, telephone and internet providers start the interception of up to hundreds of devices.

Key legal policy issues:

- **Transparency in the role of ISPs in surveillance:**

For the local authorities, this fact is presented as a guarantee of transparency because the police does not perform the surveillance operation.[31] On the contrary, for local activists there is no clarity in the role of telephone and internet service providers; this lack of transparency can be a problem to oversight not just State's activities in the private communications of users but also the ones that implies ISPs.

Data retention

Description:

According to different reports made by EFF and local organizations,[32] Latin American countries have been importing the EU data retention regime, compelling ISPs and telecommunication companies to store data of who communicates with whom and from where, while most of the time those countries either do not have a data protection regime or a clear regulation about how this data is being accessed by public authorities. For example,[33] Mexican companies currently retain the data of all domestic telecommunications users for two years, Brazil's Marco Civil da Internet requires telecommunication companies to retain connection logs for one year, meanwhile in Chile there is a bill aimed to increase data retention from one to 15 years.[34]

Key legal policy issues:

[31] El País (2015). "El Guardián": gobierno pone en marcha súper espía informático. http://www.elpais.com.uy/informacion/guardian-gobierno-pone-marcha-super.html
[32] Boing Boing (2015). Which Colombian ISPs keep your data private? http://boingboing.net/2015/05/22/which-colombian-isps-keep-your.html
[33] Americas Quarterly (2015). Privacy Is a Human Right: Data Retention Violates That Right. http://americasquarterly.org/content/privacy-human-right-data-retention-violates-right
[34] Derechos Digitales (2015). Proyecto de ley de ciberdelito:Otra mala pasada del Congreso chileno. https://www.derechosdigitales.org/9545/el-proyecto-de-ley-de-ciberdelitos-en-chile-otra-mala-pasada-del-congreso/

- Handing over users' personal data

Agreements with ISPs and public authorities, enabling non-transparent access to users data are also common. For example, in Chile there is evidence from a very well known local investigation where the telecom company handed over personal data to the police without a court order;[35] in Mexico there isn't a clear compromise from these companies to protect users' personal metadata when is required without a warrant.[36] Telecommunications companies should oppose, in any case, to deliver their customers' personal information, without a prior and specific court order. Otherwise, they should face penalties or fines and, eventually, respond for the harm that they may cause.

- Strong personal data protection by internal policies.

The protection of users' personal data is fundamental for the respect of freedom of expression. Thus, to protect human rights, companies need to advance in internal personal data protection policies, known and understandable for every user, in order to respond with clear procedures when personal data are required by the State. Likewise, when there is no legal obligation for mandatory data retention, companies should advance in having data retention just the minimum period of time, just enough for administrative internal procedures.

- Compulsory registry of SIM cards for commercial purposes

In countries as Guatemala and Peru, there is a compulsory registry of SIM cards and mobile phones, demanded by local laws with the excuse of security.[37] The amount of data required can vary, from the ID card or even the use of biometric data sets. What is also worrying is the use of these practices for the commercial purposes of the companies: not just because the State can demand that data, but also because those kind of practices can facilitate the profiling of users, especially in countries with a weak or non existent data protection laws.

ISP's role in net neutrality

Given the possibility that ISPs can limit information, contents, social networks and communication tools on internet using commercial and/or political criteria, net neutrality has been considered as an enabler of human rights as freedom of expression. In fact, in 2013 IACHR asserted that net neutrality "is a necessary condition for exercising freedom of expression on the Internet pursuant to the terms of Article 13 of the American Convention".[38]

[35] Digital Rights LAC (2013). On the parody on Twitter: lessons to learn. http://www.digitalrightslac.net/en/sobre-la-parodia-en-twitter-lecciones-que-aprender/

[36] EFF (2015). Informe "¿Quién Defiende Tus Datos?" Muestra Mucho por Hacer Para Defender la Privacidad de Usuarios de Internet en México. https://www.eff.org/es/deeplinks/2015/06/informe-quien-defiende-tus-datos-muestra-mucho-por-hacer-para-defender-la

[37] Renata Ávila, Ben Wagner, Thomas Behrndt, Joana Varon, Lucas teixeira, Paz Peña & Juan Carlos Lara (2014). Freedom of expression, encryption, and anonymity. https://www.derechosdigitales.org/wp-content/uploads/freedom-of-expression-encryption-and-anonymity1.pdf

[38] IACHR (2013). Annual Report of The Inter-American Commission on Human Rights.

Besides the recognition of the importance of the State in guaranteeing net neutrality, IACHR add: "By the same token, steps should be taken to prevent the establishment of private sector controls from resulting in a violation of freedom of expression".[39] In this context, for the IACHR should be no discrimination in the treatment of internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application.

A lot of countries from Latin America have some levels of protection over net neutrality, but the lack of enforcement of those protections is a major problem, for example:

1) **Chile**: In 2010, Chile became the first country in Latin America to adopt a law on the issue. Civil society groups have noted that the government has not properly enforced the laws and regulations: for example, zero-rating services[40] or traffic management are often offered by telecommunication companies.[41] This is not a new complaint with activists in other countries in the region.
2) **Paraguay**: The national telecoms authority, Comisión Nacional de Telecomunicaciones (CONATEL), issued a regulation in 2009 that protects Net Neutrality.[42] CONATEL posted a public letter of reprimand to an ISP for blocking the use of calls in WhatsApp but did not issue a fine or sanctions.[43]

Key legal policy issues:

- Lack of enforcement of net neutrality rules

Regarding traffic management by network operators and ISPs, evidence from countries as Chile,[44] Mexico[45] and Paraguay[46] shows how countries with some level of regulation on net neutrality don't have enough enforcement and therefore violations are constant. The problem is the same with zero-rating services. For example, the Chilean telecommunications regulator (Subtel) has banned mobile operators from offering zero-rating social media because such practices are illegal under Chilean net neutrality law.[47] Nevertheless, mobile operators are still offering these services because the legal framework on net neutrality is failing to apply fines in a meaningful manner.

---

http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf
[39] Ibid.
[40] Subtel (2014). Ley de Neutralidad y Redes Sociales Gratis. http://www.subtel.gob.cl/ley-de-neutralidad-y-redes-sociales-gratis/
[41] ONG Cívico (2013). Se confirma: en 4 años, SUBTEL no ha fiscalizado la calidad de la banda ancha en Chile https://ongcivico.org/neutralidad-en-la-red/se-confirma-en-4-anos-subtel-no-ha-fiscalizado-la-calidad-de-la-banda-ancha-en-chile/
[42] thisisnetneutrality.org
[43] ABC Color (2015) Advierten a operadoras por caso de WhatsApp http://www.abc.com.py/nacionales/conatel-advierte-a-operadoras-sobre-llamadas-por-whatsapp-1351966.html
[44] ONG Cívico (2013). Se confirma: en 4 años, SUBTEL no ha fiscalizado la calidad de la banda ancha en Chile https://ongcivico.org/neutralidad-en-la-red/se-confirma-en-4-anos-subtel-no-ha-fiscalizado-la-calidad-de-la-banda-ancha-en-chile/
[45] Proceso (2015). Empresas de telecom violan neutralidad de la red en México: ONG. http://www.proceso.com.mx/?p=412308
[46] Tedic (2015). Las contínuas violaciones a la neutralidad de la red en Paraguay. http://www.tedic.org/las-continuas-violaciones-a-la-neutralidad-de-la-red-en-paraguay/
[47] Gigaom (2014). In Chile, mobile carriers can no longer offer free Twitter, Facebook or WhatsApp https://gigaom.com/2014/05/28/in-chile-mobile-carriers-can-no-longer-offer-free-twitter-facebook-and-whatsapp/

- Censorship.

ABColor.me was a parody website where anyone can create false reports, which were published in almost identical way to the digital version of traditional Paraguayan newspaper "ABC Color". The newspaper sued ABColor.me and local activists detected that two ISPs (Personal and Tigo) blocked for hours ABColor.me website without a judicial order.[48] This is one clear example of the use of the technical capabilities of ISPs to prevent certain content from reaching its potential audience, under arbitrary criteria. The fact a website was blocked without a court order or without consideration about its nature as a parody, shows both the power of ISPs and their willingness to use it for censorship. Strong net neutrality rules would outlaw this kind of behavior.

[48] Pillku (2014) Golpe a la neutralidad de la red en Paraguay http://pillku.com/article/proveedores-de-internet-bloquean-sin-autorizacion-/

Social Media

Description:

Latin American internet users spend an average of 10 hours on social media a month, five more hours than the world average; Facebook dominates as the top social site with over 200 million users across the region; significant portions of the population in Latin America are using new technology and surpassing expectations, showing self-organization and empowerment.[49]

Key legal policy issues:

- Equal treatment for protection of users

In 2014, a powerful Chilean industrialist sued a Twitter user for identity theft. Months later, after extensive public controversy, the case was definitely dismissed; for the judge, the content of the Twitter account was clearly about satire and irony, a bedrock for the freedom of expression. The investigation of the case showed how Twitter handed over the personal information of this user to the Chilean police, through diplomatic channels but without a prior and specific court order. Would Twitter act in the same way with a similar case in United States? Twitter and other social media companies should apply the same strong standards used for the protection of the rights of their users located in the United States and other developed countries, to those living in developing countries or, straight out, in the third world.[50]

- Improvement of mechanisms to deal with online harassment

"Freedom of expression means little as our underlying philosophy if we allow voices to be silenced because they are afraid to speak up" said a Twitter spokesperson in 2015,[51] explaining how Twitter's approach has changed regarding freedom of expression, harassment and hate speech in its platform. In Latin America, online harassment -especially against women- has been a recurrent behavior, particularly in countries with high rates of violence against women. Like Twitter, other big internet companies have started to take measures to protect users and avoid behaviors that imperil freedom of expression, but the underlying questions is if those good practices are equally efficient in the developed world and the global south. For example, testimonies in Mexico have shown the difficulties for local women to get efficient answers from social media companies in general.[52]

- Commitment with the fight against emerging ways of censorship

[49] The Park Group (2015). Social Media in Latin America 2015 http://www.thesparkgroup.com/social-media-latin-america-2015/

[50] Digital Rights LAC (2014). On the parody on Twitter: lessons to learn http://www.digitalrightslac.net/en/sobre-la-parodia-en-twitter-lecciones-que-aprender/

[51] Motherboard (2016) The History of Twitter's Rules http://motherboard.vice.com/read/the-history-of-twitters-rules

[52] Cimac Noticias (2015) Se minimiza violencia de género en redes sociales http://www.cimacnoticias.com.mx/node/70359

Twitter bots are automated scripts that generate content through social media platforms and then interact with people. Andres Monroy, a social-computing researcher at Microsoft Research, has observed similar behaviors in Mexico and other countries such as Venezuela: the bots are run by traditional spammers targetting popular hashtags; its impact on trending topics is hard to quantify, as the popularity of a hashtag does not mean it is "trending". Politically motivated spambots exist and pose real problems for activists, particularly when they flood hashtags with useless content making it more difficult for information to reach the public.[53] What is Twitter doing to fight this trend? According a 2015 report from Wired, Twitter gave a canned response: "We review all reported content against our rules, which prohibit unlawful use, targeted abuse, and threats of violence".[54]

- Foreign monopolies power versus local laws enforcement

A judge in Sao Bernardo do Campo, Brazil, ordered the suspension of WhatsApp's services, after the California-based company, despite a fine, failed to comply with two judicial rulings to share information in a criminal case. The criminal case involves a drug trafficker linked to one of Sao Paulo's most dangerous criminal gangs, the PCC, or First Command of the Capital. The trafficker allegedly used WhatsApp services while committing crimes, and the court wants access to his communications with others. WhatsApp said it was unable, not unwilling, to comply.

Even though the measure was strongly criticized because its disproportionality affected the human rights of millions of Brazilian users, local voices have also warned how the US company put in danger the freedom of expression of Brazilians when simply ignored the local law and the decision of a judge.[55] Likewise, the incident highlighted growing international tensions between technology companies' privacy concerns and national authorities' efforts to use social media to recover information on possible criminal activities.[56]

[53] Wired (2015). Pro-Government Twitter Bots Try To Hush Mexican Activists http://www.wired.com/2015/08/pro-government-twitter-bots-try-hush-mexican-activists/
[54] Ibid.
[55] Blog do Gindre (2015). Impressões finais sobre a suspensão temporária do WhatsApp. http://gindre.com.br/impressoes-finais-sobre-a-suspensao-temporaria-do-whatsapp/
[56] Reuters (2015). Brazil court lifts suspension of Facebook's WhatsApp service. http://www.reuters.com/article/us-brazil-whatsapp-ban-idUSKBN0U000G20151217

Search engines and data processors

Right to be forgotten

Description:

In Argentina, the Supreme Court refused to recognize the "right to be forgotten" in a case involving the model María Belén Rodríguez, who had sued Google and Yahoo for unauthorized commercial use of her image through their search results. It was determined that companies cannot be sued for actions where they were not at fault, but that they can be punished in cases of negligence where they are aware of illegal content available via their search engines but do nothing to remove that content.[57]

Key legal policy issues:

- Litigation on freedom of expression

Even though powerful commercial reasons can be behind the decision, companies as Google have successfully litigated against the "right to be forgotten" arguing the importance of immunity from liability of intermediaries for the freedom of expression. This is an important sign for the Latin American context, but also an important precedent for further discussion regarding this issue in the region.

Censorship

Description:

1DMX.ORG is a website dedicated to reporting and documenting abuses against the opponents of the current Mexican president. Although the site's content was legal and indeed protected speech under both Mexican and U.S. law, it was suspended for three months by its host GoDaddy at the behest of the Department of Homeland Security of the U.S. (DHS). At first, GoDaddy sent an email saying the group had violated the terms of service, but didn't say how. When the site's owners pushed for more information, GoDaddy told them they were part a criminal investigation triggered by the Department of Homeland Security's Mexico City branch. Somewhere, someone had tagged them as a threat to national security, and taken down 1dmx.org in the process.[58]

Key legal policy issues:

- Equal treatment for protection of users

[57] Derechos Digitales (2015). What are the implications of the right to be forgotten in the Americas? https://www.ifex.org/americas/2015/09/22/derecho_olvido/

[58] The Verge (2014). Did GoDaddy and Homeland Security shut down a Mexican protest site? http://www.theverge.com/2014/5/24/5746232/did-godaddy-and-homeland-security-shut-down-a-mexican-protest-site

How different would have been the case 1DMX.ORG if managers have had the opportunity for the legitimate defense of their rights before the suspension of the site? To deny complete information on its customers and not defend their freedom of expression, as it happened with GoDaddy, means violating the fundamental rights of its users.

New Media

Right to be forgotten

Description:

The Chilean Supreme Court recently ruled in favor of a constitutional suit and ordered to remove from the internal index of the digital version of El Mercurio (the most influential newspaper in the country) a news article, published more than 10 years ago, about the investigation of a retired policeman for sexual abuse of minors. Even though in Chile there is not a "right to be forgotten" in statute, the rule referred to the famous European Court decision, and justified its position in the need of the protection of honour and reputation if the victim.[59]

Key legal policy issues:

- Enforcement against human rights

Despite the Supreme Court rule just to retire the registry of the news article, and from the internal search engine of this specific website, El Mercurio deleted the whole article. This disproportionate measure will affect directly the freedom of expression and is a dangerous procedure to enforce the Court's ruling.

[59] El Mercurio (2016). Corte Suprema aplica "derecho al olvido" y ordena eliminar noticia de hace una década. http://www.elmercurio.com/Legal/Noticias/Noticias-y-reportajes/2016/01/22/Corte-Suprema-aplica-derecho-al-olvido-y-ordena-eliminar-noticia-de-motores-de-busqueda.aspx

Other actors: copyright industries

Description:

Ares Rights is a Spanish law firm that "has been sending Digital Millennium Copyright Act (DMCA) takedown notices on behalf of several Ecuadorian state officials, targeting documentaries, tweets, and search results that include images of those officials, alleging copyright infringement".[60] According to Techdirt, they have also work in the same way for Argentine authorities.[61] Ecuadorian authorities have denied relation to this company. Anyhow, even if Ares Rights is sending DMCA notices independently (but in the government's name) or if it is colluded with local authorities, its actions are at least problematic for freedom of expression on internet.

Key legal policy issues:

- Censorship as a business model

The controversial DMCA (Digital Millennium Copyright Act) from the U.S. has been widely criticized because it can be used to silence any speech with copyright violation as an excuse. The reason is because rightsholders have an easy way to take down online material they dislike sending a takedown notice to a website or an ISP. "The target of the letter has the right to object by filing a counter-notice, but even if that happens, the targeted material must remain offline for 10 to 14 days before being reposted. If this restriction isn't followed, the ISP or website in question could lose its 'safe harbor' from lawsuits".[62] As big companies on internet are in USA, any business that allows the uploading of content -as Youtube, for example- needs to have DMCA compliance language in its Terms of Use or Privacy Policy. Therefore, any person can use the DMCA no matter where he or she is in the world. In this sense, the DMCA has been exported to the globe for this mechanism but also throughout Free Trade Agreements.[63]

[60] EFF (2014). State Censorship by Copyright? Spanish Firm Abuses DMCA to Silence Critics of Ecuador's Government https://www.eff.org/es/deeplinks/2014/05/state-censorship-copyright-spanish-firm-abuses-DMCA

[61] Techdirt (2013). Spanish Anti-piracy Firm Ares Rights History Of Censorship By Copyright For Ecuador & Argentina https://www.techdirt.com/articles/20130628/17335823665/spanish-anti-piracy-firm-ares-rights-appears-to-specialize-censorship-copyright-latin-american-countries-like-ecuador.shtml

[62] ArsTecnica (2010). DMCA takedowns: trampling on free speech rights? http://arstechnica.com/tech-policy/2010/04/dmca-takedowns-a-free-speech-killer/

[63] "Especially in Latin America, the so-called Free Trade Agreements became a new way in which international rules, led in this case by the United States, sought to influence local regulations, this time with the aid of potential trade sanctions in the event of noncompliance. [...] Such free trade treaties contain full chapters dedicated to the enforcement of copyright and related rights, and set out not only police and judicial procedures but also other aspects concerning technological protection measures (TPM) and the limitation of liability of Internet service providers, discussed further below, based on the criteria established by the Digital Millennium Copyright Act (DMCA) of 1998". (Lara & Ruiz (2012). Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf)