The right to freedom of expression and the use of encryption and anonymity in digital communications

Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association for Progressive Communication (APC)

Association for Progressive Communications (APC)
February 2015

Table of contents

1. Introduction

APC welcomes the focus on anonymity and encryption as a priority for the Special Rapporteur on the Protection of the Right to Freedom of Opinion and Expression. APC is an international network and non-profit organisation that believes the internet is essential for our daily information and communication needs. We advocate for everyone to have affordable access to a free and open internet to improve our lives and create a more just world. We encourage strategies that empower people to use technologies to realise the full range of their human rights, to combat discrimination and protect themselves from violence, and to take part in framing policies that govern use of such technologies, including internet governance discussions, legislation, policy and regulatory proposals.

APC's expertise in encryption and anonymity-enabling tools comes in part from our practice. Tools that ensure confidential and private communications are critical for our work and the work of our members and partners. Our submission focuses on the relationships between privacy, confidentiality and human rights in the age of the internet, with highlights such as circumventing censorship, state repression of online political speech, hate speech and online violence. While presenting a case for how encryption and anonymity empower groups at risk – specifically, targets of online violence and sexual and gender rights activists – we also expose cases in which freedom of expression has been violated that involve encryption and anonymity. We end with specific recommendations.

2. Anonymity and human rights

2.1 Relationship between anonymity and freedom of expression

Anonymity is fundamental for the full exercise of the right to freedom of expression, as enshrined in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. As former UN Special Rapporteur on Freedom of Expression Frank La Rue notes, "throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."[1] Historically, leaflets or pseudonyms in the press enabled anonymous speech. Anonymity is especially critical in repressive environments in which certain types of protected expression are outlawed, and lack of anonymity could lead to criminal charges or other consequences.

The spread of the internet and new technologies has created new possibilities for communication and free expression and opinion, including enabling anonymity. As La Rue states, "Anonymity of communications is one of the most important advances enabled by the internet, and allows individuals to express themselves freely without fear of retribution or condemnation."[2] The former Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights

[1] La Rue, F. (2011, 16 May). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/17/27. www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[2] La Rue, F. (2013, 17 April). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

(IACHR) Catalina Botero recognises that a safe environment for the exercise of freedom of expression is deeply rooted in the preservation of anonymous platforms and the use of proportionate authentication services.[3] Technological innovation has concurrently increased opportunities for threats to freedom of expression and other rights (see section 2.2 below).

2.2 Relationship between anonymity and other rights

Anonymity is also inextricably linked to the right to privacy. An individual cannot have a reasonable expectation that his or her privacy is being protected without the ability to control what information is shared about them and how that information is used. Lack of privacy, or even perceived lack of privacy, is understood to have a chilling effect on freedom of expression, leading to self-censorship.

However, encryption protocols and standards should be constructed with privacy in mind, and designed so that they cannot be used to deduce or construct the identity of an anonymous individual either by linking properties of anonymous traffic on a computer network (linkability), or by comparing the properties of anonymous traffic to externally available data (fingerprintability).

Additionally, anonymity is an important enabler of the right to freedom of association and assembly online and the right to be free from discrimination. The relative anonymity that the internet offers enables individuals and minority groups, among others, to associate on sensitive matters such as sexual orientation or religion.[4] Anonymity provides an enabling environment for people to form relationships and seek support for problems that have a social stigma like drug addiction, illnesses such as HIV/AIDS, or sexual abuse.[5] It also allows people to engage in online association based on identities or beliefs that are illegal in some countries, like LGBT groups, political opposition, or religious minorities, for example (see section 4). In Ecuador, for instance, President Rafael Correa and "several government officials have issued statements against online anonymity and deemed satire on social networks to be conspiratorial and criminal in character."[6] The government has disseminated personal data belonging to anonymous users creating a situation that "threatens personal dignity, promotes self-censorship, and affects the legitimate control that society must exert over their elected representatives."[7]

---

[3] Catalina Botero defines proportionate authentication in paragraph 136 of the report: "Online identification and authentication requirements need to be used exclusively in sensitive and risky transactions and interactions, and not broadly for all services and applications. Authentication requirements must follow the principle of proportionality, which in this case indicate that if the risk is high, the collection of additional information from the user is justified. However, if the risk is low, there is no reason to do so. Among other things, this balance encourages anonymous platforms and services on the internet, which enable freedom of expression in contexts of repression or self-censorship. Also, the principle of diversity indicates that multiple identification schemes must be encouraged for online users, in order to avoid single or concentrated identifiers that can lead to security abuses and privacy intrusions."

[4] Almstrom, H., & Liddicoat, J. (2012). The Rights to Freedom of Peaceful Assembly and Association and the Internet: Submission to the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association. January 2012. www.apc.org/es/system/files/APC_Submission_FoA_Online.pdf

[5] Cominos, A. (2012) *APC Issue Paper: Freedom of Peaceful Assembly and Freedom of Association and the Internet*. https://www.apc.org/en/system/files/cyr%20english%20alex%20comninos%20pdf.pdf

[6] https://www.accessnow.org/pages/ecuador-free-expression-letter

[7] Ibid.

3. The right to use encryption and to be anonymous online

Encryption is required to preserve confidentiality in online communications. APC's Internet Rights Charter established in 2001 the right to use encryption: "People communicating on the internet must have the right to use tools which encode messages to ensure secure, private and anonymous communication."[8] Tools that anonymise user identity are required to preserve privacy in online communications. The Internet Rights and Principles Charter, developed by an open multistakeholder network of individuals and organisations committed to making the internet work for human rights, also reinforces the right to online anonymity,[9] as do the Necessary and Proportionate Principles[10] and the African Declaration on Internet Rights and Freedoms.[11]

The advent of ICTs has enabled the use of applied cryptography in many aspects of online communication, including and beyond anonymity and encryption. While encryption by itself can guarantee the confidentiality of a message, other cryptographic techniques can be applied to ensure the integrity of a message from deliberate or accidental modification, and the authenticity of a digital message or document.

To be able to verify integrity and authenticity is important in digital communication, due to technical limitations, as well as interference by adversarial state and non-state actors. Therefore, given that states as rights bearers have an obligation to positively ensure that people have a right to free expression, they need to ensure that applied cryptographic solutions are widely available.

3.1 Circumvention and censorship

Anonymity and encryption are both critical for circumventing censorship. In the first place, circumventing a content block or filter requires a user to hide the fact that they are trying to access the forbidden content with a virtual private network (VPN), proxy or onion router.[12] Sometimes it is required, and always an advisable measure, for the user to obfuscate their identity as well, in case the content is blocked at the content server level (such as when a website complies with requests from a government to remove certain types of content for certain users). Finally, as the content requested makes its way back to the user, it should be confidential and encrypted, to ensure that deep packet inspection[13] and other measures are not being used to prevent content from reaching the user.

---

[8] APC. (2001). Section 5.3: Right to encryption. *Internet Rights Charter*. https://www.apc.org/node/5677#5

[9] Internet Rights and Principles Dynamic Coalition. (2014). The Charter of Human Rights and Principles for the Internet. internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet-English_4thedition.pdf

[10] Principle 11:
Integrity of Communications and Systems in International Principles on the Application of Human Rights to Communications Surveillance. 10 July 2013.
https://en.necessaryandproportionate.org/LegalAnalysis/principle-11-integrity-communications-systems

[11] African Declaration on Internet Rights and Freedoms. 2013. africaninternetrights.org/declaration-container/declaration

[12] Onion routing is a technique for anonymous communication over a computer network.

[13] Deep packet inspection is a form of computer network packet filtering that inspects the content of the network packet.

3.2 The right to whisper

Not only is it a universal right to be able to impart one's ideas and information openly and without threat of persecution; it is also a right to be able to limit to whom one imparts one's ideas. The ability to share information confidentially with various people – for example, one's doctor, lawyer or intimate partner – on one's own terms is essential.

The LEAP Encryption Access Project coined the phrase "right to whisper". They say, "like free speech, the right to whisper is a necessary precondition for a free society. Without it, civil society languishes and political freedoms are curtailed. As the importance of digital communication for civic participation increases, so too does the importance of the ability to digitally whisper."[14]

4. Anonymity and encryption as tools to empower groups at risk

Due to the internet's ability to provide relative anonymity and control over interactions, communities who are socially and politically excluded, and face discrimination or violence, often turn to the internet as a "safer" space.

4.1 Anonymity and encryption as tools to combat hate speech and online violence

APC, through our EROTICS project, conducted exploratory research on sex, rights and the internet, examining how the internet facilitates the exercise of sexual rights and the expression of sexualities, particularly of women living in different sociopolitical, economic and cultural contexts, and how emerging regulation online affects this ability.[15] The research encompassed a survey and research in five countries – Brazil, India, Lebanon, South Africa and the United States – between June 2008 and June 2011.[16] Our research found: "Due to the interactivity and anonymity facilitated by internet technology, the targets of hate speech and online harassment may engage in direct verbal interaction with their aggressors. Rather than acting as passive victims, the former have the opportunity to exercise effective responses."[17] In Lebanon and South Africa, in particular, our research found that "the ability for internet users to feel safe in their online interaction through the anonymity and social codes provided is a significant factor that contributes to its meaningful use."[18]

As documented in case studies developed from APC's research mapping women's experiences of technology-related violence against women (tech-related VAW), survivors strategise against VAW by using the same technology that the perpetrators did. The research, which was conducted in Bosnia and Herzegovina, Colombia, the Democratic Republic of Congo (DRC), Kenya, Mexico, Pakistan and the Philippines, found that a contributing factor was their inability to access justice either through domestic legal remedy or corporate grievance mechanisms; this is frequently the

[14] LEAP. (n/d). The Right to Whisper. https://leap.se/en/about-us/vision

[15] EROTICS: An exploratory research project into sexuality and the internet. www.apc.org/en/projects/erotics-exploratory-research-project-sexuality-and-0

[16] APC. (2011). *Sex, rights and the internet: An exploratory research study*. www.genderit.org/sites/default/upload/erotics_finalresearch_apcwnsp.pdf#synthesis

[17] Ibid.

[18] Ibid.

case, since legal remedies often fail to recognise tech-related VAW, or incidents are not taken seriously by police, courts and other administrative systems.[19]

For example, Berenice, a woman from Mexico, had her private photos and videos non-consensually uploaded on pornography websites. She had no idea who the culprit was, but suspected that someone had hacked her email. Afraid that people might say demeaning things about her, Berenice contacted the cyber crime police through Facebook. However, when she did not get a favourable response, she took the matter into her own hands. She capitalised on the anonymity offered by the internet as a means to safely and publicly denounce the situation. She also researched to find out how such a violation could have taken place, and what she could do to protect herself. She related, "Once I found out about the video, I changed my passwords and I changed the names of my accounts. I don't use last names any more either." She also learned how to do reverse-image searches and tried to monitor where her pictures and the video were being uploaded, and then ask for them to be taken down."[20]

Meanwhile, between 2009 and 2012, Antonia and other employees of the Colombian feminist organisation Mujeres Insumisas experienced a series of both online and offline threats as a direct result of the work they do: defending the human rights of women. Alongside threats via mobile phones and electronic pamphlets, the NGO received 12 threatening emails from paramilitary groups in Colombia, admonishing them to stop working for women's rights. Following an increasing number of threats – both physical and via email – and the difficulties of fighting for legal justice, the organisation designed and implemented self-protection measures, including recommendations for database handling, movement to and from the office, permanent location information for the team, and maintaining confidentiality on social networks.[21]

In Pakistan, Bayhaya, a woman human rights defender, developed a campaign in response to certain right-wing narratives. The campaign was disseminated widely across the media. Not long into the campaign being launched, she started to receive abusive comments and threats. Once Bayhaya learned of the abuse, she immediately deactivated her Facebook and Twitter accounts; however, large amounts of her personal data, including her photographs, had already been stolen and republished. Her face was used for posters in which arrows pointed at her, calling on people to identify "the woman who has insulted the Quran and the Prophet Mohammed". In other words, Bayhaya's campaign was implicitly accused of blasphemy, and related hate speech called on people "to hang this woman in a public square." The risks associated with the accusation of blasphemy – from violence to murder – led to Bayhaya removing all traces of her campaign from social media. This proved to be the most effective strategy in curbing the extent of the threats, although at the same time it limited her own freedom of expression.[22]

Just as online anonymity can empower survivors of tech-related VAW, it can be used to shield perpetrators of online violence. However, APC's experience is that laws that place limitations on

[19] APC. (2015). Case studies on women's experiences of technology-related VAW and their access to justice. www.apc.org/en/pubs/cases-women%E2%80%99s-experiences-technology-related-vaw-a

[20] www.genderit.org/sites/default/upload/case_studies_mex3_0.pdf

[21] www.genderit.org/sites/default/upload/case_studies_col1_1.pdf

[22] www.genderit.org/sites/default/upload/case_studies_pak1_0.pdf

anonymity with the stated goal of protecting victims of violence, may not actually protect survivors or serve their needs. For example, recent geotracking legislation and provisions of the new telecommunications law in Mexico represent a serious infringement on the right to privacy and do not meaningfully protect the personal safety of at-risk groups. Furthermore, as La Rue points out, "Restrictions of anonymity in communication … have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization."[23]

4.2 Anonymity and encryption as tools to empower the expression and realisation of sexual rights

Some countries criminalise certain types of sexuality, and people with sexualities deviating from the "norm" may be subject to violence and abuse. Some lesbian, gay, bisexual, transgender and intersex (LGBTI) people face the risk of violence or punitive measures including imprisonment or execution. Online anonymity is an important tool for LGBTI communities to associate safely.[24]

A global study conducted as part of APC's EROTICS project revealed that 98% of sexual rights activists, women's rights activists, safe abortion activists, LGBTQ activists, sex education activists, and others responded that the internet is "absolutely crucial for sexual rights."[25] Only 10% of gender and sexual rights activists said that "they could perform [their] advocacy work without the internet."[26] A significant 37% of this sample of gender and sexuality activists and intellectuals declared that the internet allows groups to network in safer conditions than face-to-face, and 26% thought that it allows dialogue between people with diverse opinions. Anonymity is critical for all of these actions.

Informed by this research, anonymity is included as a key concept in the newly launched Feminist Principles for the Internet. Principle 12 establishes that it is an inalienable right to choose, express and experiment with our diverse sexualities on the internet.[27]

Anonymity can function as both a pathway of resistance and a pathway of restriction. The case of Lebanese feminist lesbians engaging anonymously online shows how women can invent safe spaces online which can lead to mobilisation and reform. As we noted in our submission[28] to the UN Working Group on Discrimination Against Women in Law and Public Life meeting in 2013, the queer movement in Lebanon would not exist if it was not for the ability to network online. The movement traces its roots to the ability to access online spaces where lesbians could meet anonymously and safely, to discuss issues from dating to rights. Several issues have come up during the decade since the queer movement first emerged. One has been the importance of anonymity.

[23] La Rue, F. (2013). Op. cit.

[24] Comninos, A. (2013). Op. cit.

[25] Rafia, S. (2014, 15 September). How crucial is anonymity for sexual exploration and promoting sexual rights activism? *GenderIT*. www.genderit.org/feminist-talk/how-crucial-anonymity-sexual-exploration-and-promoting-sexual-rights-activism

[26] APC. (2013). Survey on sexual activism, morality and the internet: Preliminary analysis of survey results. erotics.apc.org/research/survey-sexual-activism-morality-and-internet

[27] In April 2014, APC convened a global meeting of 50 activists, academics and technical experts from around the world during which the drafting of the Feminist Principles for the Internet was initiated. See: www.genderit.org/articles/feminist-principles-internet

[28] APC. (2013). *The impact of ICTs on women's public and political life*. https://www.apc.org/en/system/files/WG%20final%20paper_word.pdf

As the findings of the EROTICS research make clear, anonymity has been key to the success of lesbian organising in Lebanon. The decision to leave "coming out" off the agenda has been a key one, and has been a result of the importance of anonymity online in terms of building trust and protecting the community, not just from possible legal action but also from the reaction of friends and family. However, the research also acknowledges the possibility for abuse of anonymity, as brought dramatically to light by the Scottish man who masqueraded as "Gay Girl in Damascus", whose charade endangered concerned activists and reporters. The researchers did not have any answers on how to address the problems that anonymity brings, but they are clear that state intervention merely makes vulnerable populations more vulnerable. This fear is grounded upon the state's attempts to take action against queer activists, for example, in the first ever prosecution relating to online activity in Lebanon, albeit against individuals who appear to have nothing to do with the site.

As the case study illustrates, the ability to interact anonymously was key not only to the movement, but also came to be seen as a defining aspect of the Lebanese experience of being a lesbian, as opposed to the emphasis on "coming out" in many Western LGBT campaigns. A blanket ban on anonymity, or the use of technology to prevent anonymity, risks exposing women to harm, decreases their ability to create and use public spaces and can serve to remove important issues (such as LGBT rights in Lebanon) from the public realm.

Technology also enables new forms of repression against at-risk groups, like gender and sexuality activists, presenting serious challenges to their work and personal safety. "Central to the value of online spaces in this regard is their ability to create a communicative and interactive environment that is relatively safe and secure. Privacy and anonymity are important components to this."[29]

5. Cases of violations of freedom expression and other rights relating to encryption and anonymity

As La Rue noted, "restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas. They can also result in individuals' de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities."[30] Violations of freedom of expression and other rights in relation to encryption and anonymity can take a number of forms.

5.1 Bans on use of encryption

Banning the use of encryption presents severe security and privacy implications for human rights defenders, journalists, and other at-risk groups. A number of countries have in place legal bans on the use of encryption of communications, in the name of security and law enforcement. For example, the Pakistan Telecommunications Authority (PTA) directive issued on 21 July 2011 orders ISPs and mobile phone companies to implement the Monitoring and Reconciliation of International Telephone Traffic Regulations 2010, by prohibiting and reporting all users sending encrypted

[29] APC. (2013). Op. cit.

[30] La Rue, F. (2013). Op. cit.

information over the internet.[31] In Egypt, the use of encryption by communication companies, which need it for services such as HTTPS, is illegal.[32]

In Brazil, anonymity is prohibited by Article 5 of the Federal Constitution, which states that "free expression of thought is assured, prohibiting anonymity," without specifying in which situations this should apply. Although this restriction was designed to prevent individuals from offending and causing damage to the honour and image of third parties, without leaving any trace for identification, it has been generating confusion and is being used to limit the right to privacy and freedom of expression online and offline.

For example, the software application Secret, a social network to share secrets anonymously, was banned in Brazil as a result of an August 2014 court decision. The decision resulted in the removal of the app from online stores on the grounds that it violated Article 5 of the Federal Constitution. This decision was also applied for Cryptic, which ran the Secret app in the Windows Phone platform. Moreover, it said that Apple, Google and Microsoft would have to remotely wipe the applications from the phones of users who had already installed them. Despite controversy in Brazil surrounding applications like "Secret" over ethics and responsibility for content, this banning of the application represents a limitation on freedom of expression.

The government of Brazil also limited anonymity both online and offline in response to protest around the 2014 World Cup.[33] Various governmental agencies – local police, the intelligence agency (ABIN - Brazilian Agency of Intelligence) and the army – carried out monitoring and surveillance of social networks and implemented wiretaps during protests. Because many protesters were using online platforms they could be identified and considered suspect of participating in social movements.

For example, local police in the cities of Rio de Janeiro and Goiania[34] used software to monitor some key words like demonstration, protest and meeting. Anyone who entered these terms was subjected to a police investigation, even if he or she had not taken part in protests. It is believed that the purpose of such monitoring was to create databases on the protesters, including personal information found on networks such as in which protests they participated, groups and pages they visited, as well as their political positions and comments posted on websites. These actions represent serious violations of the rights to freedom of expression, peaceful assembly and association, and privacy, enabled by digital communications.

---

[31] Bukovska, B. (2011, 2 September). Pakistan: Ban on internet encryption a violation of freedom of expression. *Article 19*. www.article19.org/resources.php/resource/2719/en/pakistan:-ban-on-internet-encryption-a-violation-of-freedom-of-expression

[32] Koops, B. (2013). Crypto law survey: Overview per country. www.cryptolaw.org/cls2.htm#eg

[33] Folha de Sao Paulo. (2013, 12 May). Polícia de São Paulo indiciou 1/3 dos detidos durante protestos. *Folha de Sao Paulo*. www1.folha.uol.com.br/cotidiano/2013/12/1381005-policia-de-sao-paulo-indiciou-13-dos-detidos-durante-protestos.shtml; Rizzo, A., & Monteiro, T. (2013, 19 June). Abin monta rede para monitorar internet. *Estadao*. sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500; Neto, J. F. (2013, 4 September). No Rio de Janeiro, rosto coberto é crime inafiançável. *Brasil De Fato*. www.brasildefato.com.br/node/25773

[34] Rizzo, A., & Monteiro, T. (2013, 19 June). Op cit.

5.2 Built-in backdoors

Backdoors, or trapdoors, are secret vulnerabilities that can be included into encryption standards. They can exist due to a flaw in the implementation of an encryption standard or built intentionally by software makers or standard authors, or inserted by authorities in order to enable wiretapping and surveillance.

In 2013, the *Guardian* revealed that US and British intelligence agencies have established covert partnerships with technology companies and internet service providers with the purpose of inserting backdoors into encryption software. In one case, it was revealed that the US National Security Agency (NSA) paid a company USD 10 million in order to introduce such a weakness into its project. This was part of a wider strategy by the intelligence agencies to undermine encryption and encryption standards relied on by developers in order to develop secure software.[35]

It was also revealed that in the early 2000s, the NSA had extensively lobbied the National Institute of Standards and Technology (NIST) to include an encryption algorithm that could theoretically contain a backdoor. The algorithm, known as Dual_EC_DRBG, was included in the standard, and remained even as the theoretical weakness became well known to the public.

Recently, in the wake of the Charlie Hebdo attacks, British Prime Minister David Cameron announced that he intends to ban encryption in the UK and introduce backdoors. This echoed similar remarks made a year before by FBI Director James Comey, stating that strong encryption can hinder law enforcement, and that backdoors are necessary. However, they fail to provide cases were strong encryption has hindered or prevented law enforcers from doing their work.[36]In fact, the Internet Engineering Task Force, while choosing not to take a political stance on wiretapping, has made the following security considerations:

- The system is less secure than it could be had this function not been present.
- The system is more complex than it could be had this function not been present.
- Being more complex, the risk of unintended security flaws in the system is larger.

Wiretapping, even when it is not being exercised, therefore lowers the security of the system.[37]

5.3 Surveillance

The knowledge, or even the perception, of being surveilled can lead to self-censorship. And while innovation has enabled new opportunities for expression and anonymity online, it has also enabled governments and private actors to monitor and collect information about individuals' communications and activities. Online surveillance has been a central issue for human rights

[35] Ball, J. et al. (2013, 6 September). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[36] Froomkin, D. et al. (2014, 17 October). The FBI Director's Evidence Against Encryption Is Pathetic. *The Intercept*. https://firstlook.org/theintercept/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb; Cohn, C. (2014, 17 October). EFF Response to FBI Director Comey's Speech on Encryption. *EFF*. https://www.eff.org/deeplinks/2014/10/eff-response-fbi-director-comeys-speech-encryption

[37] IETF Network Working Group. (2000). IETF Policy on Wiretapping. May 2000. https://www.rfc-editor.org/rfc/rfc2804.txt

activists for years – but with the recent revelations by former NSA contractor Edward Snowden, mass surveillance has become a pressing global issue.

5.4 Real-name registration

The introduction of a real-name identification system – meaning users must provide their real names before they can post comments or upload content online – can compromise users' ability to express themselves anonymously, particularly in countries where human rights are frequently violated.

In Ecuador, Article 20 of the "Ley Orgánica de Comunicaciones" establishes that comments and other content published on web pages are an individual's responsibility and intermediaries must generate mechanisms to record personal data to allow identification, such as name, email address, and any other sort of identifier of the person who published the content. Platforms are also required to design and implement regulatory mechanisms to prevent the publication and allow the denunciation and removal of content that adversely affects the rights protected by the Ecuadorian Constitution and national law. This means that communication media can only reproduce or publish messages on social networks when the author of the message is identified. If the intermediaries do not comply with this provision in the law, they are considered liable for the infringing content.

In June 2007, websites in South Korea were forced to implement a verification system that would verify individuals' identities, requiring a "real name system" when posting articles or comments, affecting almost all users on all major websites, regardless of the content. It required web operators to collect all the users' identity verification information and to store it for long periods, and many prospective posters, not completely sure of what a prohibited post is, became hesitant to post at all, in fear of disciplinary measures or outright prosecution.[38]

The Korean Progressive Network Centre Jinbonet and PSPD Public Interest Law Centre filed constitutional challenges against the "internet verification rule", part of the Information Network Act,[39] in June 2010. A decision came two years later when it was overruled by the Constitutional Court in 2012, arguing that it was unconstitutional to require people to authenticate their identity in order to post or comment on websites.

6. Limitations on encryption and anonymity

Information exchange on the internet happens on at least two discrete levels. First, there is the content. Second, there is the routing information and other data that is produced simply to get the content from one place to another. This second kind of information is called metadata. Metadata is not primary information; rather it is personal data about communications. It is nonetheless critical and anything but benign. Communications data is storable, accessible and searchable, and access to and analysis of the data can be hugely revelatory and highly invasive.[40] It can be used to draw

[38] Lavin, A. (2012, 7 September). Victory for freedom of expression in South Korea. *APCNews*. http://www.apc.org/en/node/15124

[39] Park, K. S. (2012, 25 August). Korean internet identity verification rule struck down unconstitutional: 13 highlights of the judgment. *Unbeaten Path*. blog.naver.com/kyungsinpark/110145810944

[40]Joint submission from Privacy International, Access, Electronic Frontier Foundation, Article 19, Association for Progressive Communications, Human Rights Watch and World Wide Web Foundation to the OHCHR consultation on "The right to privacy in the digital age". 1 April 2014.

social networks, to infer the content of the information exchange (if it is not already known) and to map patterns of a variety of user behaviour. In her recent report, the former UN High Commissioner for Human Rights stated that from the perspective of the right to privacy, this distinction between metadata and content data is not persuasive.[41]

While it is possible to ensure that content is confidential with the use of encryption, metadata is completely transparent to the network, or anyone or anything monitoring the internet either passively or actively – that is, unless there are proactive technical solutions to obfuscate metadata in a way that user privacy, or user anonymity, is protected. Software and protocol developers have a role to play in addressing the technical limitations of metadata in order to provide true anonymity for users who want to communicate confidentially as well as privately.

In addition to technical limitations, legal limitations are increasingly being introduced in the name of national security and law enforcement, setting hurdles to users who want to exercise their rights to freedom of expression, privacy and association, with the use of encryption. As La Rue highlights in the context of such legal limitations, restrictions on encryption often drive users to self-censorship and result in the de facto exclusion of individuals from vital social spaces, and exacerbate social inequality. Furthermore, restrictions on anonymity online allow the private sector to collect and compile vast amounts of personal data, and create risks of massive privacy violations.[42]

7. Recommendations

APC supports the recommendations made by Frank La Rue in 2011 and 2013, specifically his call upon states "to ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems,"[43] and his affirmation that "Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys."[44]

Furthermore we make the following recommendations:

- States should not undermine the integrity of open cryptographic protocols by building in backdoors.
- States should remove all restrictions on the import, export, development and use of encryption.
- Governments should not require individuals to provide their encryption keys in response to a judicial order of limited scope.
- Governments should not require internet intermediaries to provide personal data of users without a judicial order.
- Internet intermediaries should contribute to reinforcing anonymity by not disclosing personal data of their users without a judicial order.

http://www.ohchr.org/Documents/Issues/Privacy/PrivacyInternational.pdf

[41] http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

[42] La Rue, F. (2013). Op. cit.

[43] La Rue, F. (2011). Op. cit.

[44] La Rue, F. (2013). Op. cit.

- Intermediaries should not prevent users from accessing their services while using circumvention and anonymity tools.
- Developers should construct and design encryption protocols and standards to increase encryption online with privacy in mind, so that they cannot be used to deduce or construct the identity of an anonymous individual either by linking properties of anonymous traffic on a computer network (linkability), or by comparing the properties of anonymous traffic to externally available data (fingerprintability).
- States should put in place effective mechanisms for remedy that protect individuals whose rights have been violated due to limitations on anonymity, particularly for individuals from groups at risk.