White Paper in Response to Call for Submission of Information

Submitted to:

United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Submitted by:

Human Rights Foundation
&
Wickr Inc.

February 13, 2015
New York

Table of Contents

A. Call for submission of information

On January 7, 2015, the United Nations Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, called on all member States to submit information about relevant national laws, regulations, policies or practices that permit or limit, directly or indirectly, the use of encryption technologies and services or the ability of individuals to communicate anonymously online.[1]

The Special Rapporteur also called on all interested non-governmental stakeholders—including civil society, corporate actors, international and regional organizations, and national human rights institutions—to provide their views on the appropriate scope of the right to freedom of expression as applied to encryption and anonymity.

B. Standing of the Human Rights Foundation and Wickr to submit information

Pursuant to the Special Rapporteur's call for submission of information, the Human Rights Foundation (HRF), a nongovernmental human rights organization, and Wickr Inc., a corporate actor, hereby submit a joint white paper with their views and information regarding the use of encryption and anonymity in digital communications.[2]

The following subtitles of this white paper will, (1) present the universal standard on the rights to privacy and freedom of expression, including the state of recommendations on anonymity and encryption, (2) list several cases where pro-democracy movements have massively benefited from digital communications, and will consider encryption and anonymity issues faced in this context, (3) present Wickr's World Encryption Map project, and (4) provide preliminary conclusions and recommendations based on the previous three parts.

C. International human rights law

a. Standard of protection for the right to privacy

---

[1] *See* http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[2] *See* Manual of Operations of the Special Procedures of the Human Rights Council. August 2008. ¶¶ 23 and 133, *available at* http://www.ohchr.org/Documents/HRBodies/SP/Manual_Operations2008.pdf.
Mandate-holders are called upon to take account of all available sources of information that they consider to be credible and relevant. This includes information emanating from Governments, inter-governmental organizations, international and national non-governmental organizations, national human rights institutions, academic community, the victims of alleged human rights abuses, relatives of victims, and witnesses. Wherever feasible and appropriate mandate-holders should endeavour to consult and meet with such sources, and they should seek to cross-check information received to the best extent possible.
Civil society in general, and international, regional and national NGOs in particular, provide invaluable support to the Special Procedures system. They provide information and analysis, help to disseminate the findings of the Special Procedures, and assist in follow-up activities, and thus help also formulate and implement relevant national policies and programmes for human rights education to improve situations of the issues under the Special Procedures. Meetings with their representatives are appropriate in all aspects of the work of the Special Procedures including in their activities in Geneva and New York, on field missions, and more generally. It is thus appropriate for mandate-holders to give careful and timely consideration to invitations from NGOs and academic institutions to participate in activities such as conferences, debates, seminars and regional consultations. The OHCHR should generally be kept informed of the relevant activities of mandate-holders as they relate to civil society.
See also Working with the United Nations Humans Rights Programme: A Handbook for Civil Society (Handbook for Civil Society). 2008, *available at* http://www.ohchr.org/EN/AboutUs/CivilSociety/Documents/Handbook_en.pdf

According to Article 12 of the Universal Declaration of Human Rights (hereinafter, UDHR): "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . Everyone has the right to the protection of the law against such interference or attacks."[3]

Almost replicating the language used on the UDHR, Article 17 of the International Covenant on Civil and Political Rights (hereinafter, ICCPR) provides: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . Everyone has the right to the protection of the law against such interference or attacks."[4]

In its General Comment No. 16, the United Nations Human Rights Committee (hereinafter, HRC) stated:[5]

> In the view of the Committee this right [to privacy] is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons.
> . . .
>
> The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.
>
> In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.
> . . .
>
> [T]he competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant.
>
> Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.
>
> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.
> . . .
>
> States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.
>
> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most

[3] Universal Declaration of Human Rights, G.A. Res. 217A, at 71, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948).
[4] International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171, *available at* http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[5] U.N. Human Rights Committee, General Comment No. 16, ¶¶ 1, 3, 4, 7-10, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).

> effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

In its General Comment No. 27, the HRC stated:[6]

> To be permissible, restrictions [to Article 12] must be provided by law, must be necessary in a democratic society for the protection of these purposes and must be consistent with all other rights recognized in the Covenant.
>
> The law itself has to establish the conditions under which the rights may be limited . . . In adopting laws providing for restrictions permitted by article 12, paragraph 3, States should always be guided by the principle that the restrictions must not impair the essence of the right; the relation between right and restriction, between norm and exception, must not be reversed. The laws authorizing the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution.
>
> Article 12, paragraph 3, clearly indicates that it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them. Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected.
>
> The principle of proportionality has to be respected not only in the law that frames the restrictions, but also by the administrative and judicial authorities in applying the law. States should ensure that any proceedings relating to the exercise or restriction of these rights are expeditious and that reasons for the application of restrictive measures are provided . . . The application of restrictions in any individual case must be based on clear legal grounds and meet the test of necessity and the requirements of proportionality.

In its General Comment No. 31, on the nature of the general legal obligation on States parties to the ICCPR, the HRC stated:[7]

> States Parties must refrain from violation of the rights recognized by the Covenant, and any restrictions on any of those rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.

i. The right to privacy in the digital age

In resolution 68/167, the United Nations General Assembly stated: "[T]he same rights that people have offline must also be protected online, including the right to privacy."[8]

In this regard, the Office of the United Nations High Commissioner for Human Rights has stated:[9]

---

[6] U.N. Human Rights Committee, General Comment No. 27, ¶¶ 11-16, U.N. Doc CCPR/C/21/Rev.1/Add.9 (1999).
[7] U.N. Human Rights Committee, General Comment No. 31, ¶ 6, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004).
[8] The Right to Privacy in the Digital Age, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Jan.21, 2014).

> Digital communications technologies, such as the Internet, mobile smartphones and WiFi-enabled devices, have become part of everyday life. By dramatically improving access to information and real-time communication, innovations in communications technology have boosted freedom of expression, facilitated global debate and fostered democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights.
> . . .
>
> Governments frequently justify digital communications surveillance programmes on the grounds of national security, including the risks posed by terrorism . . . Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.
> . . .
>
> Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.

ii. Interrelation between the right to privacy and the right to freedom of opinion and expression

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated:[10]

> Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[11] The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used.
> . . .
>
> The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas . . . In this regard, article 17 of ICCPR refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communication, both online and offline.[12] As the Special Rapporteur noted in a previous report,[13] the right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online

---

[9] High Commissioner for Human Rights, The Right to Privacy in the Digital Age, ¶¶ 1, 24 and 25, delivered to the U.N. Human Rights Council, U.N. Doc. A/HRC/27/37 (June 30, 2014).
[10] Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶¶ 22 and 24, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013). (Footnotes 11-14 belong to the quoted text).
[11] Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, Butterworth, 2004, para. 4.82.
[12] ICCPR commentary, p.401.
[13] A/HRC/17/23.

> communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties.[14]

In resolution 12/16, the United Nations Human Rights Council stated that restrictions inconsistent with the right to freedom of expression include:[15]

> (i) Discussion of government policies and political debate; reporting on human rights, government activities and corruption in government; engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups.
>
> (ii) The free flow of information and ideas, including practices such as the banning or closing of publications or other media and the abuse of administrative measures and censorship.
>
> (iii) Access to or use of information and communication technologies, including radio, television and the Internet.

In its 2011 report, the Special Rapporteur on the situation of human rights defenders stated:[16]

> The right to freedom of opinion and expression is of crucial importance to the work of human rights defenders. Without this right defenders would not be able to perform their monitoring and advocacy work to promote and protect human rights. This right applies to both men and women promoting and protecting human rights, providing they accept and apply the principles of universality and non-violence. In the case of women human rights defenders, States need to ensure that tradition, history, culture and religious attitudes are not used to justify violations of women's right to equality before the law and to the equal enjoyment of all rights.

iii. Anonymity in communications

In different reports, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated: [17]

> [W]hile users can enjoy relative anonymity on the Internet, States and private actors have access to technology to monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of Internet users' right to privacy, and undermine people's confidence and security on the Internet, thus impeding the free flow of information and ideas online.
> . . .
>
> In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. 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.

---

[14] A/HRC/17/23.
[15] U.N. Human Rights Council, Res. 12/16, 4-5, U.N. Doc. A/HRC/RES/12/16 (Oct. 12, 2009).
[16] Margaret Sekaggya, Special Rapporteur on the situation of human rights defenders, ¶ 43, U.N. Doc. A/66/203 (July 28, 2011).
[17] Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 82, U.N. Doc. A/HRC/17/27 (May 16, 2011). *See also supra* note 10 at ¶¶ 23, 24, 47-49, 52, 79 and 88.

> . . .
>
> Restrictions of anonymity in communication, for example, 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.
> . . .
>
> One of the most important advances facilitated by the advent of the Internet was the ability to anonymously access and impart information, and to communicate securely without having to be identified . . . However, in the name of security and law enforcement, gradually States have been eradicating the opportunities for anonymous communication.
> . . .
>
> Restrictions on anonymity facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of State surveillance.
>
> In this sense, 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 . . . Furthermore, restrictions on anonymity allow for the collection and compilation of large amounts of data by the private sector, placing a significant burden and responsibility on corporate actors to protect the privacy and security of such data
> . . .
>
> Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.
> . . .
>
> In order to receive and pursue information from confidential sources, including whistleblowers, journalists must be able to rely on the privacy, security and anonymity of their communications. An environment where surveillance is widespread, and unlimited by due process or judicial oversight, cannot sustain the presumption of protection of sources. Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.
> . . .
>
> States should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés or mobile telephony.

iv. Encryption in communications

In this regard, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stated:[18]

> Through communications, the most personal and intimate information, including about an individual's or group's past or future actions, can be revealed. Communications represent a valuable source of evidence upon which the State can draw to prevent or prosecute serious crimes or forestall potential national security emergencies.
> . . .

[18] *See id*. at ¶¶ 12, 71, 89 and 95-96.

The security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption.

. . .

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.

. . .

States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection. States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

D. Cases where pro-democracy activists under authoritarian regimes have benefited from Digital Communications: the issues of encryption and anonymity[19]

N°	STATE	TYPE OF MOVEMENT AND/OR DENOMINATION	SOCIAL NETWORKING WEBSITES AND/ OR APP	STATE'S REACTION	ENCRYPTION	ANONYMITY	SOURCES
1	Republic of Moldova	2009: Civil society movement also known as the Grape Revolution and the Twitter Revolution.	1. Twitter 2. Facebook	The government shut down internet service during the protests. It also blocked several social-networking websites because protestors were using them to communicate amid a media blackout. State authorities interfered with mobile connections in an attempt to silence protestors.	We have not been able to determine whether and to what extent encryption technologies were used during the demonstrations. The personal use of encryption technologies is restricted by regulation. A license from Moldova's Ministry of National Security is required.	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. After protests were over, it has been reported that in the separatist Transnistria region, residents increasingly use social-networking websites to anonymously discuss politically sensitive issues with their counterparts in the rest of Moldova.	Freedom House OpenNet Initiative The New York Times Spiegel The Telegraph
2	Islamic Republic of Iran	2009/2011-2012: Iranian Green Movement, Green Revolution, the Green Wave, the Sea of Green, or the Persian Awakening.	1. Twitter 2. YouTube 3. Facebook 4. Gmail 5. Flickr	Government filtered content, including the words "violence," "unrest," and "democracy." Other sophisticated censorship methods included: tampering with internet access, mobile-telephone service, and satellite broadcasting; hacking opposition and other critical websites; monitoring dissenters online and using the information obtained to intimidate and arrest them; ordering blogging service providers inside Iran to remove "offensive" posts or blogs; and trying to fill the information vacuum created by these measures with propaganda and	We have not been able to determine whether and to what extent encryption technologies were used during the demonstrations. In Iran, the personal use of encryption technologies is restricted by regulation. During the 2009 crackdown on dissent, many arrested activists reported that interrogators had confronted them with copies of their e-mails. Authorities claimed that they had access to all the e-mail and text messages exchanged in Iran. In addition, internet service providers have been accused of forging SSL certificates to eavesdrop on emails sent through secure channels (https), making protected communication increasingly	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. However, following the 2009 protests, the government has increased technical measures to curb anonymous communications. Intercepted communication has been repeatedly used to identify, target, and prosecute activists, journalists, and human rights advocates no matter what platforms they used to express their views and organize protests. In a move that also affected internet users outside of Iran, two international companies responsible for issuing digital certificates for popular online services like Gmail, Yahoo,	Freedom House OpenNet Initiative CNN I CNN II The Economist The Wall Street Journal Daily Mail BBC Time CNET

[19] The main sources in the preparation of this database are Freedom House's Freedom on the Net and Freedom of the Press indexes.

				misinformation. The internet censorship system in Iran is said to be one of the most comprehensive and sophisticated in the world.	difficult for those without more sophisticated skills. On several occasions, around politically sensitive dates, internet service providers have blocked the SSL protocol, preventing millions of Iranians from having secure access to their email addresses.	Hotmail and Skype were hacked during 2011. The forged certificates could have been used to potentially spy on some 300,000 users in Iran. The Computer Crime Law obliges internet service providers to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to monitor all this data. Bill 106 issued by the Communications Regulatory Authority in March 2012 requires the registration of all of the IP addresses in use inside Iran, in order to organize and systematize them beyond the data already collected. Implementing such registration will allow the authorities to more to track users' online activities even more thoroughly. When purchasing a mobile phone subscription or prepaid SIM card, users must present identification, facilitating the authorities' ability to track down the authors and recipients of specific messages. On March 2012, regulations came into effect making it a requirement for customers of cybercafes to provide personal information (such as their name, father's name, national identification number, and telephone number) before using a computer. Cafe owners are required to keep such information, as well as customers' browsing history, for six months. They are also required to install closed-	

						circuit surveillance cameras and retain the video recordings for six months.	
3	Tunisian Republic	2010-2011: Tunisian Revolution, Jasmine Revolution.	1. Twitter 2. Facebook 3. YouTube 4. Dailymotion 5. Flickr 6. Wat TV	Government blocked websites, harvested passwords and usernames of bloggers, reporters, political activists, and protestors to delete what they deemed as offending material. Social media sites played an important role in providing independent information and analysis, spreading the protestors' demands, and showing videos of demonstrations in cities across the country. As a result, the government increased its efforts to dismantle networks of online activists, hack into their social networking and blogging accounts, conduct extensive online surveillance, and disable activists' online profiles and blogs. Tunisia's multilayered internet censorship apparatus was one of the world's most repressive. It is said to have largely dissipated with President Ben Ali's fall on January 14, 2011.	We have not been able to determine whether and to what extent encryption technologies were used during the demonstrations. A number of laws from the Ben Ali era remain, including provisions that ban the personal use of encryption technologies. For example, article 11 of the Telecommunications Decree prohibits internet service providers from transmitting encrypted information without prior approval from the Minister of Communications. By the beginning of the protests in late 2010, e-mail hacking in Tunisia was already common, accounts that had no secured access were monitored, and important information could suddenly disappear. In 2010, many cases of phishing targeting users of Google's Gmail service were reported. In the absence of easily accessible encryption instruments, government forces were able to easily intercept internet traffic to impede citizens' ability to express their views and organize. Moreover, lack of encryption available to consumers resulted in increased internet censorship performed by the government during the protests.	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. However, it should be noted that anonymity and the right to privacy was said to be already nonexistent in Tunisia by the time of the demonstrations. During the protests, digital activists and online users reported widespread government hacking into their digital media accounts, sometimes deleting their profiles and blog entries. While the government did not expressly forbid anonymity and users could post anonymous comments on websites, the government had access to user information through internet service providers and could trace a comment to its author. The private internet connections of some journalists, activists, and political bloggers was often cut, ostensibly due to "technical problems," or the speed was reduced to hamper their ability to view sites and post information. Text messaging was monitored for taboo topics (including expressions of political opposition to the government, discussions of human rights issues) in much the same way as the internet. Another legislation from the Ben Ali era that remains in force and concerns anonymity is the Internet	Freedom House OpenNet Initiative WIRED Foreign Policy The New York Times

						Regulations. Article 8 of the said regulations requires internet service providers to submit a list of all subscribers to the Tunisian Internet Agency. During the protest in 2010-2011, the Electronic Frontier Foundation called on Facebook to consider allowing anonymous accounts for Tunisian users: "Consider allowing pseudonymous accounts for users in authoritarian regimes, where political speech under your real name is dangerous and potentially deadly. Many Tunisian activists are unable to reinstate Facebook accounts that have been erased by the Tunisian government because they were not using their real names."	
4	Arab Republic of Egypt	2011/2012-2013: Civil society movement.	1. Facebook 2. Twitter 3. YouTube 4. Google 5. Hotmail 6. Flickr 7. BlackBerry Messenger 8. Bambuser	During the January 2011 revolution, social-networking websites helped spread ideas of discontent among Egyptians by calling them to join in protest and put pressure on the Egyptian government. The revolution that ultimately led to President Mubarak's ousting had to deal with large-scale government tactics aimed at suppressing the uprising's roots online, including: shutting down internet connectivity, cutting off mobile communications, imprisoning dissenters, blocking media websites, confiscating newspapers, and disrupting satellite signals in a desperate measure to limit media	We have not been able to determine whether and to what extent encryption technologies were used during the demonstrations. However, encrypted instant messaging services like BlackBerry were available in the country at the time of the protests. Personal use of encryption is not banned in Egypt, domestic laws and regulations require communication service operators to apply for permission with the authorities. Under Article 64 of the 2003 Telecommunications Law, the use of encryption devices is prohibited without the written consent of the National Telecommunication	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. However, even before the revolution, restrictions on anonymity made it easier for activists to be monitored and singled out by the authorities. The international condemnation of the government's tactics to crush dissent after the January 2011 unrest led the authorities to restore internet connectivity. However, authorities decided to unblock internet access on February 2, 2011, likely because it was harder for Egyptian security forces to control online communications and	Freedom House OpenNet Initiative BBC CBS The Guardian The Independent The New York Times WIRED The Telegraph PCMag

				coverage. Government control over online access made it easy to block internet traffic in less than an hour on January 27, 2011 following the revolutionary demonstrations. The government shut down almost all of its Border Gateway Protocol routes, which disconnected the country from the global network. During the 2012-2013 unrest, it has been reported that authorities repeatedly throttled mobile internet service in the areas around political protests, preventing activists from communicating through social networks and voice over internet protocol applications.	Regulatory Authority, the military, and national security authorities. In addition, import of cryptographic technologies has to be registered with the Ministry of Economy and International Trade. According to media reports, the 2011 attempt by the Egyptian government to shut down all online communication was unprecedented. This temporary measure completely blocked the whole country from accessing any internet resources, as well as any encryption or anonymity-enabling instruments like Tor network, an anti-censorship that activists were using to circumvent the Facebook and Twitter blocks.	monitor protestors' plans while Egypt was offline. In 2011, the government enforced an article from the 2003 Telecommunication Act (Law #65) that obliges internet service providers and mobile operators to allow government access to customer databases. The Telecommunications Law allows the offices of the Presidency, Security, Intelligence, and the Administrative Control Authority to obtain citizens' online information without prior consent for cases that concern national security. Several reports highlighted instances of members of the national security forces using internet service providers' databases to obtain information about the activities of specific customers. Mobile operators and internet service providers are required to collaborate with the Homeland Security Agency and the military police when asked to release information or provide records of subscribers. In addition, internet cafe customers need to provide their names, email addresses, and mobile numbers to receive a personal identification number (PIN) to access the internet. The country's three mobile operators are also required to register their subscribers as well as keep records of their online activities, and an out-going phone call can be traced by a half-dozen government entities.	

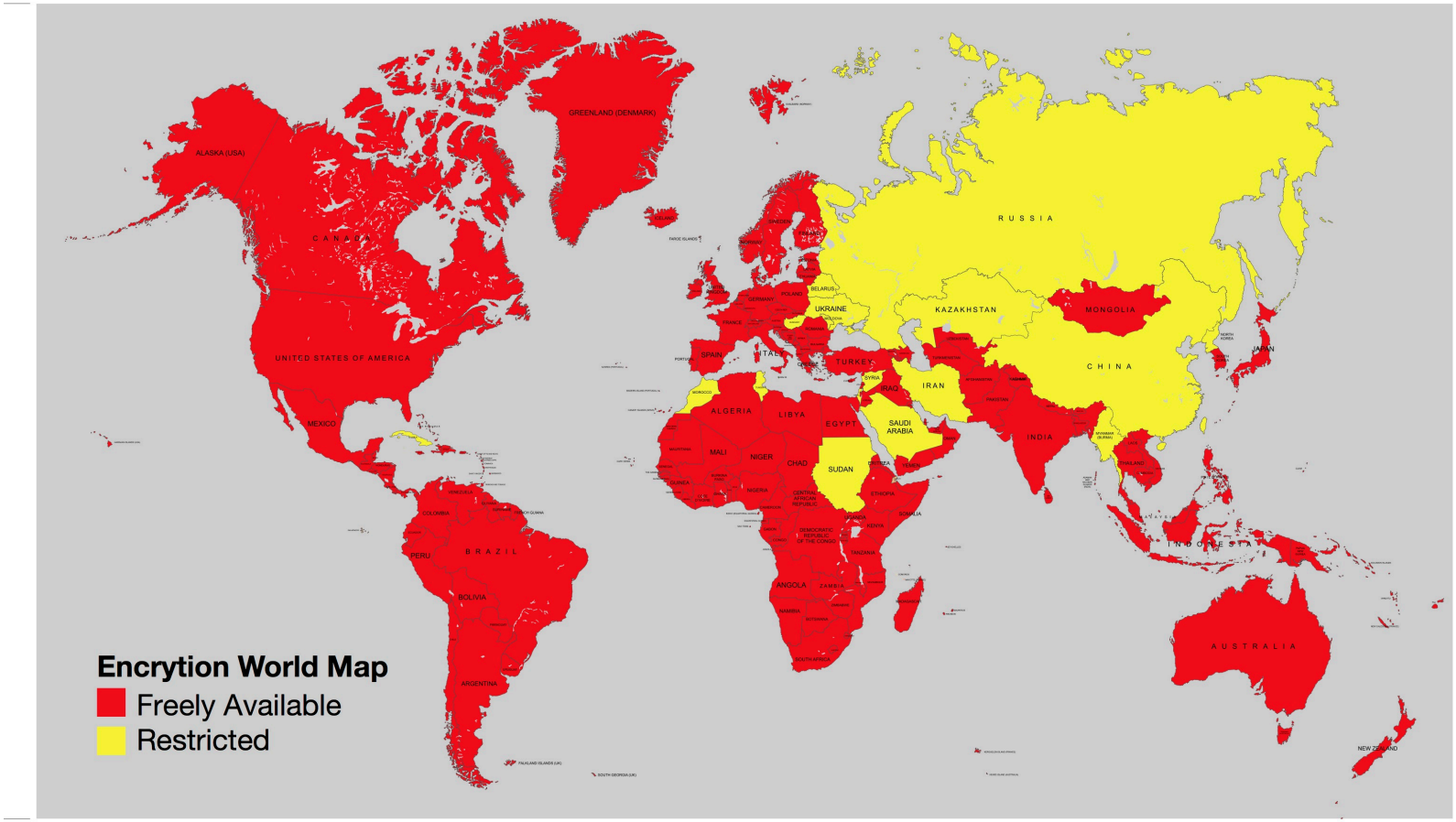
5	Ukraine	2013-2014: #EuroMaidan	1. Twitter 2. Facebook 3. YouTube 4. Zello	During the protests, the ousted government of President Yanukovych used jamming and blocking techniques that seemed to be limited to and aimed at obstructing the work of independent media. The Euromaidan protests did not cause the government to block or filter websites, but short-lived anti-protest laws, which included measures limiting internet freedom, and extra-legal pressure on media and citizens created an atmosphere of fear, leading to self-censorship in state-controlled media. Users also reported that certain independent media sites were blocked at their companies or offices. YouTube, Facebook, Twitter, and blog-hosting services such as Wordpress and LiveJournal, freely available, gained significantly more users during the Euromaidan protests.	We have not been able to determine whether and to what extent encryption technologies were used during the demonstrations. The personal use of encryption technologies is restricted by regulation. Although use of encryption is highly regulated according to Ukraine's law, it did not appear that the government engaged in enforcing these restrictions during the protests.	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. According to media reports, during the initial days of the uprising, the application Zello was widely used by protesters to communicate. As the protests escalated into violence, organizers switched to real life walkie-talkies for most communications. It should be noted that currently there is no obligatory registration for either internet users or mobile phone subscribers, although the anti-protest legislation that was briefly introduced by parliament in January 2014 included a bill that would require buyers to present a passport before purchasing prepaid mobile services. It should also be noted that the pervasiveness of extralegal surveillance of Ukrainian users' activities is unclear.	Freedom House OpenNet Initiative International Business Times Motherboard The Washington Post I The Washington Post II CNN Huffington Post I Huffington Post II
6	Republic of Turkey	2013-2014: Civil society movement	1. Twitter 2. YouTube 3. WordPress 4. Dailymotion 5. Soundcloud 6. Vimeo	During the protests, the government blocked thousands of websites. Authorities increased arrests and legal prosecutions for online activities, including tweets and Facebook comments critical of the government. It should be noted that the blocking and removal of online content is permitted and regulated in Turkey under the Regulation of Publications on the	We have not been able to determine whether and to what extent encryption technologies were used during the demonstrations. The personal use of encryption technologies is not restricted by regulation. However, since 2011, suppliers of encryption hardware and software are required to provide encryption keys to state authorities before they can offer their products or	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. However, according to various media reports, during the protests, activists employed Virtual Private Networks (VPNs) to communicate with one another. One of the VPN providers reported a sharp increase in its usage in Turkey at that time. Generally, VPN is used to	Freedom House OpenNet Initiative The Telegraph BBC CNN The Wall Street Journal I The Wall Street Journal II Al Jazeera

				Internet and Suppression of Crimes Committed by means of Such Publication. (Law No. 5651.)	services to individuals or companies within Turkey. Failure to comply can result in administrative fines and, in cases related to national security, prison sentences.	protect users' location and allow them to use the internet undetected. While internet service providers are not required to monitor the information that goes through their networks, nor do they have a general obligation to seek out illegal activity, they're required to log data on their users and abide blocking orders. Data must be made available to the regulatory authority upon request and without the need for a court order. It should be noted that the constitution states that "secrecy of communication is fundamental," and users are allowed to post anonymously online. The anonymous purchase of mobile phones is not allowed and buyers need to provide official identification.	The Guardian
7	Bolivarian Republic of Venezuela	2014: Civil society movement	1. Twitter 2. Zello 3. Tunnel Bear 4. Blackberry Messenger 5. WhatsApp	The government cut off the internet and blocked numerous websites, including those belonging to independent media. Rumors of throttling—the intentional slowing down of service to effectively cripple online activity—were also common during the protests. The hacking of political websites and the usurpation of the Twitter profiles of political activists, critical journalists, and dissident voices, a trend that began in 2012, also continued during the protests.	According to media reports, demonstrators purportedly used encryption technologies like the Blackberry messaging service for communication purposes. There are no restrictions on personal use of encryption in Venezuela. However, similarly to the Egyptian case, government of Venezuela attempted to suppress the civil society movement by blocking access to the internet entirely, as well as individual social networks and websites. Social networks and messaging services available to activists appeared to play a role in mobilizing the	According to media reports, anonymity was a concern for protestors during demonstrations. Applications like Zello were particularly popular during the early phases of the protests. Once the situation intensified, protestors begun using encrypted chat applications and social media sites with privacy options that allow for greater protection against surveillance from the authorities. According to the news reports, Venezuelan protesters actively employed anonymous bulletin boards to share information and self-organize. The government forces then	Freedom House OpenNet Initiative International Business Times Huffington Post The Wall Street Journal Bloomberg CNN

					protests in Venezuela in 2014. Venezuelans that wanted to access the blocked resources had to use proxy services to circumvent government censorship.	moved to block these platforms. Another concern regarding anonymity is the tracking of mobile phone users. Since 2005, mobile phone operators are required to collect copies of subscribers' identity documents, addresses, fingerprints, and signatures. According to the Computer Crimes Act, this information must be delivered to state security agencies upon presentation of a judicial warrant. Service providers are also obligated to keep detailed logs of all calls, including the phone number and location of both the caller and the recipient.	
8	Peoples Democratic Republic of China (Hong Kong)	2014: Occupy Central	1. Instagram 2. Weibo 3. Weixin 4. FireChat 5. Facebook 6. Wickr	Protestors feared an internet and telecommunication networks shutdown that ultimately didn't take place. These rumors prompted them to download applications like FireChat, a tool that establishes a mesh network between smartphones, allowing them to communicate within a given range without a cellular or internet signal. However, it was in mainland China where authorities blocked social networking resources, including Facebook and Instagram, as well as media websites, in order to prevent the dissemination of information about the protests taking place in Hong Kong. The Weibo and Weixin accounts of some Hong Kong protestors were cancelled.	Peer-to-peer encryption communication service Wickr has seen a rapid increase in its user numbers during the 2014 protests in Hong Kong. In China, the personal use of encryption is restricted by regulation. During the 2014 Hong Kong protests, activists took advantage of encryption technology to circumvent government censorship. They also were largely prepared for cellular network shut down by employing the peer-to-peer networked applications. (Bluetooth-enabled.)	We have not been able to determine to what extent anonymity of communications was a concern for demonstrators. China's online population is among the most avid users of proxy servers and VPN services that enable them to access the internet anonymously and beyond The Great Firewall. Using such technology and peer-to-peer encryption communication services allowed for a higher level of protection and anonymity in sharing information and organizing the protests.	Freedom House OpenNet Initiative CNN Slate Foreign Policy BBC

				But what authorities really sought was to shut off interaction with the mainland. To this end, the government also disrupted mainland access to chat applications like KakaoTalk and LINE, used by protestors in Hong Kong to mobilize, and censored vocabulary specific to political developments.			

E. World Encryption Map[20]



[20] This World Encryption Map is an ongoing project recently developed by Wickr Inc. aimed at researching and assessing restrictions under cryptography laws and regulations worldwide as applied to personal use of encryption technology. Countries where individuals are allowed without any additional steps to use encryption for personal purposes are color-coded as red ("freely available"). Countries, in which restrictions or reporting requirements are imposed on individual citizens employing encryption for personal purposes are color-coded as yellow ("restricted"). Traditionally, encryption regulations have the following applications: (1) personal use; (2) domestic controls; and (3) export and import. For the purposes of this paper, we only consider restrictions imposed directly on individual persons and their use of encryption technology. Wickr intends to continue researching and assessing the World Encryption Map to keep it up-to-date.

F. Conclusions and recommendations

a. Conclusions

i. On the state of international law regarding privacy and freedom of expression, including the issues of encryption and anonymity

International human rights law, as interpreted by the UN General Assembly, the UN Human Rights Council, the UN High Commissioner on Human Rights and, in particular, the UN Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, establishes that:

> (1) No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. The same rights that people have offline must also be protected online, including the right to privacy. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself;
>
> (2) The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. In this regard, the ICCPR refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communication, both online and offline;
>
> (3) Restrictions on anonymity facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of State surveillance. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny;
>
> (4) The security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption. 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. States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

ii. On how digital communications have been used by pro-democracy activists under authoritarian regimes, and the roles actually played by anonymity and encryption

Based on a quick overview of recent cases where pro-democracy activists under authoritarian regimes have benefited from digital communications, HRF and Wickr provisionally conclude:

> (1) Digital communications played a significant role in rallying pro-democracy demonstrations against authoritarian regimes.
>
> (2) In most cases, we were not able to determine whether and to what extent encryption technologies were used during the demonstrations.

(3) In most cases, we were not able to determine to what extent anonymity of communications was a concern for demonstrators.

(4) The absence of easily available encryption technology tends to facilitate government surveillance of digital communications.

(5) The absence of easily available encryption technology hinders the ability of citizens to protect their online identities against government monitoring mechanisms and practices.

iii. On Wickr's World Encryption Map project

Based on the preliminary findings of Wickr's World Encryption Map, HRF and Wickr provisionally conclude that many authoritarian regimes have restrictions or reporting requirements in place for personal use of encryption technology. Comparatively, there's not a single case where a democratic country has these restrictions in place.

b. Recommendations

HRF and Wickr respectfully recommend the Special Rapporteur to:

(i) Further elaborate on the areas where the current state of international law is silent, unclear, vague or ambiguous, regarding the ability of individuals to communicate anonymously online and the important role encryption technologies play to that end. Specifically, HRF and Wickr recommend that the Special Rapporteur pursue a comparative constitutional study consisting of/aimed at: (1) determining the state of the law and actual State practice in all member States of the United Nations, (2) identifying as accurately as possible the most protective laws and practices among UN members States (only information that can be verified or corroborated independently should be considered, and the highest level of scrutiny should be given to information provided by nondemocratic States), and (3) based on these findings, issue recommendations establishing a concrete, narrowly tailored minimum standard, which should be followed by all UN member States in order to comply with international law (for example, the Special Rapporteur could suggest a specific balancing test where (*a*) a very strong protection to speech content, and (*b*) a low threshold for finding a reasonable expectation of privacy, akin to the ones established under the U.S. Constitution's First and Fourth Amendments, are guaranteed).

(ii) Issue a recommendation stating that even small restrictions to the rights to privacy and freedom of expression in the following areas trigger a strong presumption that international law is being violated: any criticism of government policies; human rights reporting; any exposure of government corruption; nonviolent demonstrations; nonviolent partisan political activity; any statement of opinion; any expression of religious belief; any criticism or satire aimed at religion or religious authorities, specially in States where no separation of government and religion exists.

(iii) Ratify and further elaborate on a previous statement by the Special Rapporteur, stating that communications represent a valuable source of evidence upon which the State can draw to prevent and/or prosecute serious crimes, like as human trafficking and child pornography; and to forestall serious national security threats, such as acts of terrorism.

(iv) Ratify and further elaborate on a previous statement by the Special Rapporteur, stating that "restrictions on anonymity facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of State surveillance."

(v) Ratify and further elaborate on a previous statement by the Special Rapporteur, stating that "States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys."

(vi) Ratify and further elaborate on a previous statement by the Special Rapporteur, stating that "States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption."

(vii) Ratify or restate the following recommendations and general opinions by the former U.N. Special Rapporteur on Freedom of Expression, in order to further consolidate a consistent interpretation of the universal standard on the rights to privacy and freedom of expression. Specifically, ratify or restate that:

> (1) The right to privacy [should be] understood as an essential requirement for the realization of the right to freedom of expression;
>
> (2) In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous;
>
> (3) 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; and
>
> (4) Individuals should be free to use whatever technology they choose to secure their communications.

Contact information

Human Rights Foundation
(To the attention of Javier El-Hage, General Counsel)
Address: 350 Fifth Avenue, #4515
New York, NY 10118
Tel: (212) 246-8486
Email: javier@thehrf.org
Website: www.thehrf.org

Wickr Inc.
(To the attention of Jennifer DeTrani, General Counsel)
Address: 1459 18th Street, #313
San Francisco, CA 94107
Email: jen@wickr.com
Website: www.wickr.com