# Encryption and Anonymity in Digital Communications

## Office of the High Commissioner for Human Rights
## Consultation on the Right to Freedom of Expression and the Use of Encryption and Anonymizing Tools Online

**February 10, 2015**

### About Freedom House

Freedom House is an independent watchdog organization dedicated to the expansion of freedom around the world. The Global Internet Freedom Program at Freedom House seeks to empower digital activists and civil society groups to safely promote and protect their human rights online, particularly in the most repressive environments. In national, regional, and international debates on the future of the internet, we work with key stakeholders to elevate civil society voices and ensure human rights perspectives are central to determining the way forward. In addition, we conduct groundbreaking research on the degree of internet and digital media freedom in countries around the world.

Freedom House welcomes the opportunity to provide input for the study by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the use of encryption and anonymity in digital communications, and to offer recommendations based on Freedom House's research and advocacy.

### Overview of the Use of Encryption and Anonymizing Tools Online

Emerging information and communication technologies (ICTs) have undoubtedly expanded the potential for the realization of internationally recognized human rights. Not only has the use of ICT tools empowered an ever-increasing population of netizens to enjoy their rights in unprecedented ways, it has also helped eliminate certain previously existing technological barriers to the fulfilment of these rights. The ability to transact and communicate privately and anonymously online, through the use of encryption software and other tools, is a necessary requirement for the full realization of the rights to freedom of expression and privacy, particularly when speech may be socially taboo or critical of those in positions of power. Such online anonymity enables and emboldens individuals, particularly vulnerable groups and those in sensitive professions, to safely and effectively exercise their right to free expression, while also curbing the chilling effects posed by the fear of reprisals or invasion of privacy.

Journalists, human rights defenders, and lawyers—to name just a few of the actors whose work is vital to a functioning democratic society—depend on access to encryption tools to ensure their online communications are confidential and secure. Likewise, women, LGBTI people, religious minorities, and other marginalized populations are empowered to exercise their right to freedom of expression when they are sure of the security and privacy of their communications. For many netizens, if not all, online anonymity within the boundaries of the rule of law is a necessary condition for the full enjoyment of the right to free expression.

Freedom House works with many individuals and groups matching these profiles throughout more than 80 countries, and the organization has witnessed the benefits for these partners in using encryption software and anonymous communication platforms to communicate and transact online. Freedom House is concerned that States are increasingly enacting laws and policies to restrict or criminalize these tools, and encourages steps to guarantee the right to freedom of expression online through stronger protections for citizens to use encryption software and communicate anonymously.

**International Legal Context**

The right to privacy and freedom of expression are grounded in Article 12 and Article 19 of the Universal Declaration of Human Rights, and these principles are further articulated in the International Covenant on Civil and Political Rights (ICCPR), which provides for the right to freedom of expression through Article 19 and the right to privacy through Article 17, stating that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence […]." The Human Rights Council and the General Assembly of the United Nations have affirmed that the rights people enjoy offline—particularly the right to freedom of expression[1] and the right to privacy[2]—must also be protected online. Additionally, in his report in April 2013, former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, specifically noted the importance of anonymity in online communications: "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."[3]

---

[1] Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet," 29 June 2012, http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf.

[2] Resolution 68/167, "The right to privacy in the digital age," adopted by the General Assembly on 18 December 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.

[3] Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," 17 April 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Despite these protections, the right to privacy in digital communications—and specifically the right to anonymous communication—is increasingly under threat worldwide. As more of people's communications and activities take place online, governments face the challenge of reassessing the right to privacy as it applies to the online sphere.

For example, recognizing the growing scale and importance of the internet, Brazil's president signed into law the Marco Civil da Internet in April 2014, which established a number of rights and regulations specific to the online sphere. Among these provisions, Marco Civil specifically guarantees the right to privacy and freedom of expression online (Article 8) and guarantees the inviolability and secrecy of the flow of users' communications online, except by a court order (Article 7.2).[4] The legislation is one of the first to specifically and comprehensively address the rights of internet users online, and may set a strong precedent for establishing protections for the right to privacy as it pertains to digital communications. However, the legislation does not expand the right to privacy online to specifically include the right to anonymity, and in fact, anonymity is prohibited under the Brazilian constitution. In August 2014, months after Marco Civil was passed, a Brazilian judge ordered the anonymous communications app "Secret" to be banned based on the argument that an individual's right to privacy could be threatened by the app's facilitation of anonymous rumor-spreading.[5] This decision failed to take into account that law enforcement could have access to user's account information if they provided a court order, and that banning the app altogether infringes on the rights of those who use the app for legitimate anonymous speech. In many such cases where rights are seemingly in competition with one another, governments are taking a blunt approach to the regulation of anonymous speech online and are failing to issue rulings or regulations that are necessary and proportionate to the stated aims.

Examples where the concept of the right to privacy in digital communications has been expanded to protect anonymous communication are the exception rather than the norm: worldwide, a growing number of countries are restricting anonymity online. Of 65 countries surveyed in Freedom House's 2014 *Freedom on the Net* report,[6] 18 passed new laws between May 2013 and May 2014 restricting anonymity in online communications through measures such as real-name registration requirements or SIM card registration. In May 2014, the Russian government enacted a law requiring bloggers with more than 3,000 daily readers to register with regulators, share user data with authorities, and store data on servers located in Russian territory. Most recently, in early 2015, the Chinese government announced that it would be extending real-name registration guidelines to require all internet users on social media

---

[4] Law No. 12.965, April 23, 2014 (English translation), https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf.
[5] Court decision, August 18, 2014, https://drive.google.com/file/d/0BzcBZYaOx4TaS0tMcnFOcHVZdDQ/edit
[6] https://freedomhouse.org/report/freedom-net/freedom-net-2014.

platforms, websites, and forums to register with their real names and official ID. Additionally, in January 2015 Chinese government officials admitted to interfering with the use of many virtual private network (VPN) platforms in the country that were primarily being used by members of the business community or others (VPNs with stronger privacy protections that are primarily used by activists were already restricted). As more trusted VPN platforms become unavailable, Chinese internet users will increasingly be forced to turn to platforms with fewer privacy safeguards, potentially subjecting their communications to monitoring and surveillance by the government.

**The Growing Threat to Privacy and Freedom of Expression Online**

While encryption technologies were historically associated primarily with military or government activities, the broad public expansion of internet access in the early 1990s and ease of digital encryption led to battles between governments and freedom of expression advocates over legitimate uses of encryption tools for private communication. In the United States, for instance, where encryption technologies were regulated as a weapon for national security purposes until 1996, privacy advocates won court cases removing restrictions on the use and export of digital encryption software on the grounds of freedom of expression. In response, U.S. government representatives warned about diminished capabilities of law enforcement to fight crime and terrorism, and floated proposals to require the installation of decryption backdoors into software. Despite widespread public outrage following recent revelations of expansive surveillance efforts by the U.S. National Security Agency and other intelligence agencies—including initiatives to crack or undermine encryption technologies—American and British government officials continue to cite national security concerns as more private companies have announced plans to implement end-to-end digital encryption. At the same time, backdoor access to encryption undermines the security of such tools, and there is no conclusive evidence to support the claim that such warrantless access is necessary to combat threats to national security.

That the right to privacy through encryption is again coming under attack by governments in established democracies, which have protections for individual privacy rights and freedom of expression, not only raises new concerns for the use of these technologies but also provides further fodder for repressive measures by more authoritarian governments. In July 2014, seven bloggers in Ethiopia were charged with terrorism, with part of the charge sheet presented against them citing their use of encryption, on the assumption that concealed communications are suspicious and can be equated with criminal activity. Additionally, the import, export, and use of encryption software without government approval is still regulated in 13 countries (Tunisia, Belarus, Myanmar, China, Hungary, Iran, Israel, Kazakhstan, Moldova, Morocco, Russia, Saudi Arabia, and Ukraine). While these laws are not consistently applied, as long as they remain on the books they can be used to criminalize the download and legitimate use of digital encryption technologies by private citizens.

**Case Studies: Impact on Journalists, Lawyers, and Human Rights Defenders**

Private and anonymous communication is essential to the work of human rights defenders and organizations, especially those defending the rights of vulnerable groups. Interference in the right to private communication between individuals can have a detrimental chilling effect not only on human rights defenders and their individual rights but also those of the groups and people on whose behalf they work, fostering fear that the often personal and sensitive information human rights defenders collect, receive, and transmit could be shared without their knowledge or approval. Freedom House's extensive experience working with and supporting human rights defenders and developing their capacities to defend and protect the privacy of their digital communications and data shows how privacy rights violations can interfere with their work by fostering fear about the publication of sensitive information or leading to their persecution and prosecution:

- **Iran**: Surveillance of the private communications and data of privacy-rights activists in Iran has led to their arrest and persecution, interfering in their human rights defense work and forcing some to flee. In April 2013, the Iranian Islamic Revolutionary Guard Corps (IRGC) discovered that a human rights defender was producing and distributing proxies and anti-filtering software to a wide variety of activists inside and outside of the country. The IRGC penetrated the defender's database of approximately 6,000 users, exposing the defender's significant efforts to assist people in Iran to maintain the privacy of their electronic communications with basic software tools. Fearing prosecution for his work and following a clear threat of retribution by a government representative, the defender, who had been previously jailed in 2012, held in solitary confinement, and subjected to electric shock, fled the country.

- **Angola**: In a case that highlights the role private companies play in enabling governments and others to reveal individuals' private communications, an Angolan investigative journalist and human rights defender was targeted with malicious surveillance software sold by a company in Portugal for his reporting on government corruption tied to the mining industry. He learned in 2013 that malware produced by a company which sold its products to the Angolan government had been placed on his laptop, sending screenshots of his computer's desktop every 20 seconds to an Internet server and revealing the private communications he made using the compromised computer. From the information gleaned from his computer, the defender was summoned to court without a warrant, interrogated without legal representation, and informed that he had been indicted on charges of defamation. Due to the malicious software installed on his computer, his equipment became non-operational and his data was non-recoverable.

- **Vietnam:** In the past two years, numerous Vietnamese bloggers have been arrested under Articles 79 and 88 of the Vietnamese Penal Code for “subversion” and “conducting propaganda against the state,” stemming from their online activism on human rights issues, including multi-party democracy and democratic reform, religious freedom, and freedom of expression. In 2014, several well-known Vietnamese bloggers and activists fled to Thailand after the Vietnamese Ministry of Public Security posted nation-wide warrants for their arrest. This incident mirrors dozens of similar cases in the country, as human rights defenders and their families are jailed, physical assaulted, and intimidated for simply expressing opposing viewpoints on online forums. While Freedom House has assisted dozens of Vietnamese activists and bloggers with their relocation, they are often detained by security forces in Thailand and returned to Vietnam, where they face imprisonment.

In these and similar cases, the right to privacy and anonymity in digital communications is essential to ensuring one’s physical safety while exercising the right to freely express opinions and criticisms online.

**Recommendations**

Based on Freedom House’s research and work with human rights defenders worldwide, we submit the following recommendations:

**To the UN Human Rights Council:**

- Pass a resolution affirming that the right to anonymity is a fundamental and inalienable cornerstone to the internationally guaranteed rights of freedom of expression and belief; and, acknowledging that the ability to communicate privately and remain anonymous is essential to the work of certain sectors necessary for a democratic and just society.

**To Governments:**

- Recognize the important role that anonymity and the use of encryption technology for private communication plays in enabling journalists, bloggers, human rights defenders, and non-governmental organizations to conduct their work safely and effectively.
- Repeal or amend laws and regulations that criminalize the use of encryption technology or anonymous communication, and ensure that all laws and regulations adhere to internationally recognized principles protecting the right to freedom of expression.
- Collaborate with the private sector and civil society to design laws and regulations that adequately protect citizens from legitimate threats to public safety and security, while also upholding the right to freedom of expression.

**To the Private Sector:**

- Turn to international multi-stakeholder initiatives and guidelines when determining anonymity and privacy policies and industry best practices.
- Include input from civil society when designing anonymity and privacy policies, making particular effort to understand how policies could affect civil society's ability to operate effectively and safely; take measures to include input from a broad range of civil society, including groups working with typically marginalized and vulnerable populations.
- Promote transparency around efforts to limit or prevent anonymity by publicly publishing the number and type of requests received by governments asking to reveal the identity and activity of users.

**To Civil Society:**

- Recognize that civil society has a unique perspective on the potential and the perils of an unrestricted internet; use this perspective to develop and propose constructive solutions to the concerns of governments about anonymous communication and the use of encryption software.
- Pledge to work within the boundaries of the law when laws and regulations adhere to the internationally guaranteed rights of freedom of expression and belief.