Thank you for this opportunity to provide commentary on Encryption and Anonymity in Digital Communications. Below you will find the joint submission of Access and PEN American Center to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

Table of Contents

Introduction

Right now, the global debate is raging over anonymity, pseudonymity, and encryption in the digital sphere. Some governments have claimed that technologies that enable users to communicate securely and protect their private information, like encryption, pose threats to national security. For example, Ethiopian officials jailed six bloggers last year in part because the journalists took part in a digital security training. The training was designed to teach users to use basic encryption.[1] Spanish authorities recently arrested eleven people who were using "extreme security measures," including encrypted email.[2] Policies have been proposed or implemented to require backdoors through encryption protocols (intentional vulnerabilities granting access to users' information, or that force users to link their real identities to their online speech). Such invasive policies restrict privacy and demonstrably chill speech, limiting the online exercise of expression.

Private speech, which includes anonymous and pseudonymous speech, has long been recognized as protected by international human rights standards. International agreements, including the International Covenant on Civil and Political Rights (ICCPR), recognize the right to privacy and the right to freedom of expression.[3] The Human Rights Council has affirmed that these rights apply online, just as they do offline.[4] **As we demonstrate below, it is clear that the exercise of anonymity, pseudonymity, and encryption should be protected under the same human rights standards as the rights to free expression and privacy that they enable.**

Access[5] and PEN American Center[6] welcome UN Special Rapporteur David Kaye's decision to study anonymous speech and encryption as a free expression issue. As he prepares his report, we encourage Special Rapporteur Kaye to fully consider the points identified below.

---

[1] Deji Olukotun, *Encryption and the Faustian Bargain*, Pen American Center, Aug. 15, 2014, *available at* http://www.pen.org/blog/encryption-and-faustian-bargain.
[2] RiseUp, *Security is not a Crime* (Jan. 6, 2015), available at https://help.riseup.net/en/about-us/press/security-not-a-crime.
[3] The right of privacy is guaranteed under the European Convention on Human Rights (art. 8) ("ECHR"), the Universal Declaration of Human Rights (art. 12), and the International Covenant on Civil and Political Rights ("ICCPR")(art. 17). The right to privacy is also enshrined and recognized by the Convention on the Rights of the Child (art. 16), the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14), and the American Convention on Human Rights (art. 11).
[4] U.N. Human Rights Council Res. 20/8, U.N Doc. A/HR/20/L.13 (June 29, 2012), available at undocs.org/A/HRC/20/L.13.
[5] Access defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.
[6] For the last 90 years, PEN American Center has been working to ensure that people everywhere have the freedom to create literature, to convey information and ideas, to express their views, and to make it possible for everyone to access the views, ideas, and literatures of others.

Discussion

1. Privacy enables expression

Government surveillance programs and authorities unquestionably intrude upon the privacy rights of individuals. In some cases these intrusions have been allowed by governments under several different justifications, including national security and foreign intelligence gathering.[7] These surveillance programs, in turn, have been shown to chill expression. In fact, Special Rapporteur Frank La Rue stated that any restrictions on the right to privacy should be subject to the same "permissible limitations" test as the right to freedom of expression.[8] Two recent surveys conducted by PEN and the nonpartisan research firm FDR Group demonstrated concrete harms to free expression caused by mass surveillance.[9] The most recent of these, a survey conducted from August – October 2014 of more than 770 writers and journalists in 50 countries around the world, clearly concluded that mass surveillance has a harmful impact on expression.[10] Writers in countries around the world, in both democratic and non-democratic states, are self-censoring in response to concerns about global surveillance.[11]

The survey results showed that writers and journalists are very concerned about privacy and anonymity online. Many reported taking extra precautions in their online communications out of concern that those communications might be monitored by a government authority. This was true regardless of whether the writer lived in a country considered to be democratic: 24% of writers living in countries classified as "Free" by Freedom House, 24% of writers in "Partly Free" countries, and 37% of writers in "Not Free" countries reported having taken extra steps to cover or protect their digital footprints—like using encryption or changing to a more secure service provider—or having seriously considered doing so. In addition, particularly in less democratic countries, many writers

---

[7] U.S. Presidential Policy Directive 28 (Jan. 17, 2014), available at http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. Whether or not these justifications are warranted is a question which we do not confront here.

[8] U.N Doc. A/HRC/17/27. Pursuant to General Comment no. 34 of the Human Rights Committee, such "permissible" restrictions must be provided by law, strictly serve a legitimate aim (respect of the rights and reputations of others, protection of national security or of public order, or of public morals or health, as defined by General Comment 34), and meet a high standard of legality, proportionality, and necessity. The International Principles on the Application of Human Rights to Communications Surveillance, available at https://necessaryandproportionate.org/.

[9] PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (Nov. 12, 2013), aavailable at http://pen.org/chilling-effects; PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers* (Jan. 5, 2015), available at http://pen.org/global-chill.

[10] PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers* (Jan. 5, 2015), available at http://pen.org/global-chill.

[11] Id at 9-12; see also PEN America, *Chilling Effects* at 5-8.

have used internet cafes in an attempt to anonymously access the internet, or have seriously considered doing so: 22% of writers in "Partly Free" countries, 24% of writers in "Not Free" countries, and 9% of writers in "Free" countries.[12]

Many writers also took steps to protect their sources' identities: 33% of writers living in countries classified as "Free" by Freedom House, 48% of writers in "Partly Free" countries, and 69% of writers in "Not Free" countries reported taking extra precautions, or seriously considering it, to protect the anonymity of their sources, out of concern that their communications might be monitored by their government.[13]

As part of the research for this report, PEN sent a request for feedback to its approximately 4,000 members regarding why anonymity and encryption are important to them. Their responses were instructive, and many of the members who responded cited the protection of their sources' identities and personal information as chief among their concerns:

> "I am especially concerned about confidentiality and my current inability to promise this to my subjects beyond my own limited best efforts which, given the realities, are inadequate. As an independent journalist with limited resources, I cannot provide even the basic available additional securities (which don't seem to be so secure after all). Since I spend so much time in certain places, I develop a network of contacts and relationships, and any violation of the terms would have a grave and far-reaching effect… As someone who writes about people who are typically described as marginalized, I am most concerned my notes will somehow be used against my sources, often vulnerable people I write about and who I follow for years. I amass a great deal of highly detailed information. I often type notes directly into the computer during phone calls. I am in contact with incarcerated people, directly and through people they refer me to because I also write about criminal justice and crime. The people I write about are at risk for losing their freedom, their children, and jobs.
>
> Lastly, the long-term nature of the work also requires real freedom for my own thinking, questioning, and developing thoughts. I can already feel the impact of self-censorship in terms of what I write on the computer and in email. I have taken to writing certain drafts of my work on a typewriter in part because I cannot shake the feeling of potential unwanted scrutiny. It can be hard enough for any writer to claim

[12] Some of the survey results cited here were not included in PEN's *Global Chilling* report; full survey results are available upon request from PEN American Center. Note also that the results cited here are similar to the results found in PEN's survey of its US membership in October 2013; see http://pen.org/chilling-effects at p. 24-25.

[13] Id; see also Pen America, *Chilling Effects* at 8.

that sense of intellectual freedom within herself to figure out what she's saying, but to have an actual risk of invasion of a work-in-progress, much of which can be unformed and out of context, is, for me, is potentially paralyzing."

--

"I have worked for some years on Sri Lanka-related activism, and with activists in Sri Lanka, many of whom have had security concerns. In light of serious media freedom issues in recent years—and impunity for attacks on journalists there, including abductions and murders—it has been very important to me to support my friends, allies, and journalist colleagues through secure communications.

The government in Sri Lanka has recently changed, but this is a time of transition, and things could easily go a number of ways. I plan to continue to communicate securely and sometimes anonymously about issues connected to Sri Lanka. Ensuring that this remains possible is also a way to maximize the inclusion of marginalized voices: those belonging to women, children, and minority populations."

--

"I often work in dodgy areas, and teach courses on conflict reporting at graduate journalism schools and beyond. (I recently ran safety workshops in Mexico and Palestine.) I can't stress enough the need for people to learn how to navigate encrypted communications. The more people who use them, the less they will throw up red flags to authoritarian governments. Having said that, like many human rights activists I think the best way to safeguard communications, in compromised newsrooms and with sensitive sources, is to go low tech. Meet in person. Speak in code. Unplug as much as possible so that your chances of being hacked are minimized. Encryption software lends a false sense of security, and eventually it too will likely be compromised by sophisticated hackers."

--

"I live in Russia . As far as I know, encryption modules are disabled on notebooks officially supplied to Russia, and using encryption in my country is not allowed. For me, using encryption would make sense, because, increasingly, email accounts are broken, fished for sensitive information etc. So that not just freedom of expression is challenged, but the very privacy of communication. [But] perhaps encryption is the least of our troubles…absence of freedom of speech non-encrypted is more like it!"

These responses demonstrate the personal impact surveillance can have on individual users and the clear need for encryption tools and other ways to protect sensitive information and confidential sources.

2. Anonymity and pseudonymity are crucial to promoting and protecting free expression and democratic debate

Privacy includes the ability to exchange communication "beyond the reach" of the state, and anonymity, facilitating that communication, "is one of the most important advances enabled by the internet."[14]

Restrictions on anonymous and pseudonymous expression impair the very essence of the rights to privacy and freedom of expression. The "imposition of obstacles to the free flow of information" is a violation of the right to freedom of expression.[15] Such limitations place users in danger of physical harm, threats, and harassment, among other things. As a result, many would-be speakers may choose not to express themselves, impoverishing public debate and narrowing the "marketplace of ideas" engendered by free speech.[16] By forcing individuals to communicate through insecure, unsafe platforms attached to their true identity, governments are violating individual rights.

Marginalized groups, whether domestic abuse victims, political minorities, corporate whistleblowers, or other members of at-risk communities are often those who most need the protection afforded by anonymity and/or pseudonymity, so that they may speak out against injustice and raise arguments that may be unpopular or controversial to some without fearing for their safety. For example, PEN is currently engaged in research on the LGBT community in Nigeria. In numerous interviews, people reiterated the importance of the ability to protect one's true identity online. Being able to remain anonymous or to use a pseudonym enables members of the community to correspond, meet new people, and engage in free expression. Many interviewees have expressed fear for what would happen to them and their friends and loved ones if the police or private individuals who wish them harm were able to uncover their real identities.[17]

---

[14] U.N Special Rapporteur on the promotion and protection of the right to freedom of expression, U.N Doc. A/HRC/17/27 (May 16, 2011), available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[15] Declaration of Principles on Freedom of Expression, Inter-American Commission (Oct. 2000), available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26; *see also* American Convention on Human Rights, Nov. 21, 1969, 1144 U.N.T.S. 143, explaining that rights to freedom of thought and expression shall not be subject to prior censorship.

[16] Supra note 8.

[17] See also Anna Lekas Millter, *In the Middle East, Marginalized LGBT Youth Find Supportive Communities Online*, Tech President (Sep. 6, 2012), available at http://techpresident.com/news/wegov/22823/middle-east-marginalized-lgbt-youth-find-supportive-communities-online.

Historical examples also demonstrate the importance of private communication. Thomas Paine originally published the pamphlet Common Sense—which played a significant role in the lead-up to the American Revolution—anonymously because the ideas it contained were considered treasonous under colonial-era law.[18] In the 18th Century United States, Alexander Hamilton, James Madison, and John Jay authored the Federalist Papers, a series of essays advocating the adoption of the United States Constitution, under the pseudonym Publius.[19] The Anti-Federalists, who responded with critiques to the Federalist Papers, published anonymously as well.

Some of the world's most celebrated authors operated under pseudonyms. George Orwell, who wrote 1984 and Animal Farm, was not born George Orwell, but, instead, Eric Blair. Authors like Samuel Clemens (Mark Twain), Mary Ann Evans (George Eliot), and J.K. Rowling (Robert Galbraith), and artists like Caravaggio (Michelangelo Merisi) and Banksy (unknown), adopted different names. Names may be changed or withheld for a variety of reasons, ranging from persecution to prejudice to privacy.[20]

PEN members who offered their thoughts on the importance of anonymity and pesudonymity noted their role in facilitating political dialogue and democratic debate:

> "[W]e need to provide writers and artists the privilege and security to express their views without fear of retribution or persecution. There are many other examples. Many of Jonathan Swift's works were published anonymously, or under various pseudonyms, as they were sharply political in nature. To protect and promote uncensored ideas and expressions should be of paramount importance to everyone with a deep commitment to freedom of expression and uncensored, critical thought."
>
> --
>
> "The sheer possibility of comprehensive data-collection breaks a long-standing tacit agreement between citizens and liberal-democratic states: that the citizens will be left alone so long as their actions are not provably criminal. Now, conceivably, any opposition leader can be tracked and spied upon; any whistle-blower can be preventively blocked from going to the media; no lawyer can be sure of confidential

[18] See Thomas Paine, *Common Sense* (1776), available at http://publicliterature.org/books/common_sense/1.
[19] The Federalist Papers, avialable at http://thomas.loc.gov/home/histdox/fedpapers.html.
[20] Tierney Sneed, *Robert Galbraith and the Story Behind 7 Other Famous Pen Names*, U.S. News & World Report (July 15, 2013), available http://www.usnews.com/news/articles/2013/07/15/jk-rowlings-robert-galbraith-joins-mark-twain-george-orwell-and-lewis-carrol-as-world-famous-pen-name

> communication with his client, no reporter can promise his sources anonymity. The result is that a tyrannical status quo is at least technically achievable, by impeding citizens from communicating freely with one another and acting to supplant the present order of things.
>
> The danger to the very idea of democracy is extreme. On the one hand, electronic communications media offer ordinary citizens unprecedented means for investigating and organizing; on the other hand, spying technologies readily subvert the democratic potential of cheap, open communication.

Anonymity may also be critical for individual health and welfare. People often feel more comfortable seeking professional care and assistance in anonymous settings, including health support groups, and curtail communication when privacy is threatened. For instance, Alcoholics Anonymous of Australia has recognized the benefits of the organization's anonymity policy.[21] Individuals are more likely to seek assistance if their participation remains private, according to the group. The organization cites the spiritual impact of anonymity, which "discourages the drives for personal recognition, power, prestige, or profit that have caused difficulties in some societies. Much of our relative effectiveness in working with alcoholics might be impaired if we sought or accepted public recognition."[22]

Online communication has demonstrated the freeing effect of pseudonymity. Disqus, a discussion system for websites, conducted research that showed pseudonymous posters were significantly more expressive than those using their real names or even those going without a name.[23]

However, usage of new technologies illustrate the ongoing tension between anonymity and government authority. Many countries, including Thailand as well as at least 49 countries in Africa, have implemented mandatory SIM card registration policies or are in the process of doing so.[24] Several governments have considered and passed similar, though arguably more egregious, policies of mandating that users register their communications hardware devices.[25] While voluntary registration of SIMs can provide certain perceived benefits, such

---

[21] Alcoholics Anonymous Australia, *The Importance of Anonymity*, available at http://www.aa.org.au/members/anonymity.php.
[22] Id.
[23] Disqus, *Pseudonyms Drive Communities!, available at* https://disqus.com/research/pseudonyms/
[24] Larry Banks, *Mandatory Registration of SIM Cards in Thailand*, Thai Tech (Jan. 22, 2015), available at http://tech.thaivisa.com/sim-card-registration-thailand-update/3112/; Kevin Donovan and Aaron Martin, *The Rise of African SIM registration: The emerging dynamics of regulatory change*, First Monday (February 2014), available at http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820.
[25] This registration is done through the IMEI number, a unique identification number attached to each cell phone. See, e.g. a recent ITU event on "Combating Counterfeit and Substandard ICT Devices"

as access to e-governance services, mandatory registration is essentially a means to enable a greater amount of government surveillance of private information, consequently chilling users' free expression.[26]

3. Anonymity and pseudonymity are rights

Domestic and international courts have long connected anonymity as an element of the right to privacy. In the United States, the Supreme Court has protected the right to anonymous speech.[27] In *Talley v. California*, the Supreme Court recognized that anonymous writings, such as leaflets, have played a key role in allowing persecuted groups to criticize oppressive conditions. That is to say, they do so "either anonymously or not at all."[28]

In the context of the internet, the Supreme Court of Canada identified the connection between the right to privacy and anonymity. In *R. v. Spencer* the Court noted, "[i]nformational privacy is often equated with secrecy or confidentiality, and also includes the related but wider notion of control over, access to and use of information. However, particularly important in the context of [i]nternet usage is the understanding of privacy as anonymity."[29] Courts in the United Kingdom have found similar protections for anonymous speech.[30] A German court found, "[t]he typical use of anonymity on the internet corresponds to the fundamental rights interests."[31] From the cases outlined above, a robust global tradition has emerged that protects anonymous expression as an essential aspect of the rights to privacy and freedom of expression, online and offline.

---

http://www.itu.int/en/ITU-T/C-I/Pages/Programme.aspx; and laws in Kenya (Article 19, *Kenya: Free expression standards should guide fight against "counterfeit" mobile phones* (6 Oct. 2011), available at http://www.article19.org/resources.php/resource/2762/en/kenya:-free-expression-standards-should-guide-fight-against-%E2%80%9Ccounterfeit%E2%80%9D-mobile-phones); India (Techline Info, *How to get IMEI number legally in India for Chinese Mobiles* (30 Nov. 2009), available at http://www.techlineinfo.com/how-to-get-imei-number-legally-in-india-for-chinese-mobiles); and Uganda (UCC, *Counterfeit Mobile Phones FAQs*, available at http://ucc.co.ug/data/dnews/8/Counterfeit-Mobile-Phones-FAQs.html).

[26] Access, *Comments on Myanmar Code of Practice for Mobile Registration* (June 2014), available at https://s3.amazonaws.com/access.3cdn.net/4f9d64de32582dddbb_1rm6bebo4.pdf; GSMA,*White Paper: Mandatory Registration of Prepaid SIM Users* (Nov. 2013), available at http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf.

[27] *See* Talley v. California, 362 U.S. 60 (1960); Watchtower v. Vill. of Stratton, 536 U.S. 150, 166 - 67 (2002), and McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

[28] Talley v. California, 362 U.S. 60 (1960).

[29] R v. Spence, 2014 SCC 43 (2014), available at http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.

[30] Totalise Plc v. The Motley Fool Ltd & Anor EWHC 706 (QB) (19 February 2001); Sheffield Wednesday Football Club Ltd and others v. Hargreaves EWHC 2375 (QB).

[31] Oberlandesgericht Hamm, Case n. I-3 U 196/10 (Oct. 3, 2011), available at http://www.justiz.nrw.de/nrwe/olgs/hamm/j2011/I_3_U_196_10beschluss20110803.html.

Because of the close nature of the practice to the right, the legality of any government restriction on anonymous speech should be assessed in the same way any other infringement on free expression would be. Any law or regulation that broadly or indiscriminately penalizes or limits anonymous speech prohibits the speaker from omitting their identity from their expression, and is impermissible under international human rights law.[32]

4. Encryption is ubiquitous

As restrictions on anonymization and pseudonymity impair the right to free expression, so too do restrictions on the technologies that facilitate anonymous and pseudonymous expression. Encryption has become ubiquitous. It provides security for much of the everyday data transmitted and stored online. Increasingly, bank records, health records, and the content of our electronic communication are encrypted to permit greater control over personal information. Encryption also serves to protect vulnerable users around the world by promoting confidence that their communications have not been altered or viewed without permission.

The promotion of encryption is not anti-law enforcement, it is pro-user. Encryption protects against data breaches, overreach of repressive regimes, and other unauthorized access that chills expression, a fact reflected in PEN members' comments:

> I personally have little need for encryption… But I can well imagine that investigative reporters, muckrakers, whistle-blowers, victims of certain kinds of abuse, have an absolute need of secure encryption, without which they may be exposed to retaliation (in the case of the whistle-blower or the abuse victim) or simply may be unable to perform their work (as in the case of the muckraking reporter). With such cases in mind, I urge you to consider the availability of secure encryption a public good, to be maintained in the interest of civil society and democratic governance."
>
> --
>
> "I think it is important to recognize how many sensitive stories there are out there and protect the independence of journalists working to legally get to the truth. I am working with people who are or have been and may still be under government surveillance, and others who are facing long prison sentences for crimes that appear

[32] Supra note 7. Applying the test for speech infringements, we find that restrictions on anonymous expression apply disproportionately, to all potential speakers; do not strictly serve any particular aim; and are not necessary to achieve any legitimate aim.

> to have been instigated by others. We are using the best workarounds we can and would not be able in any way to do the work we are doing without encryption tools…The sources I'm dealing with can't even afford anything but a cheap supermarket phone. They are especially at risk."

Governments also depend on encryption for their own security. The U.S. Navy developed Tor, an encrypted, anonymous browsing network, to protect the flow of government data.[33] In a recent interview, President Barack Obama indicated he is a "strong believer in strong encryption," and explained "there's no scenario in which we don't want really strong encryption."[34]

However, limitations on individual use of encryption help to facilitate government surveillance programs. There exists an inherent conflict of interest between the government's desire to protect systems and to break into them, demonstrated first-hand in the U.S. National Security Agency's dual mission of information assurance and intelligence gathering.[35] United Kingdom Prime Minister David Cameron has indicated plans to introduce legislation strictly limiting the use of encryption to enable more effective terrorist investigations.[36] Such a law would potentially prohibit the public use of certain encryption services and leave users vulnerable to a wide range of bad actors. In Iran, for example, broad surveillance programs operated by the government are able to locate activists who have criticized the State or its officials.[37] The Iranian government maintains these capabilities by preventing use of secure communications technologies, such as WhatsApp, which was blocked only months after the service encrypted all transmissions.[38] Online activists who defy the government often face jail time or corporal punishment.

Despite these prohibitions, users are increasing their use of encryption. Use of Tor doubled between October 2012 and October 2013. The search engine Duck Duck Go, a privacy-

---

[33] Tor: Overview, available at https://www.torproject.org/about/overview.
[34] Interview by Kara Swisher, Re/code, with U.S. President Barack Obama (Feb. 13, 2015), available at https://www.youtube.com/watch?v=yaylQmnXztU.
[35] Amie Stepanovich, *Virtual Integrity, Three Steps Toward Building a Stronger Cryptographic Standard* (Sep. 18, 2014), available at https://www.accessnow.org/blog/2014/09/18/virtual-integrity-the-importance-of-building-strong-cryptographic-standards.
[36] Alex Hern, How has David Cameron Caused a Storm Over Encryption (Jan. 15, 2015), available at http://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws.
[37] Freedom House, *Freedom on the Net 2014: Iran*, available at https://freedomhouse.org/sites/default/files/resources/Iran.pdf.
[38] The Associated Press, *Iran Blocks Communication Apps LINE, WhatsApp, Tango* (Jan. 7, 2015), available at http://www.ctvnews.ca/sci-tech/iran-blocks-communication-apps-line-whatsapp-tango-1.2176978; Iain Thomson, What do UK and Iran have in Common? Both Want to Outlaw Encrypted Apps (Jan. 12, 2015), available at http://www.theregister.co.uk/2015/01/12/iranuk_in_accord_as_pm_promises_to_block_encrypted_comms_after_election/.

themed tool, has nearly tripled its traffic since June 2013. Duck Duck Go utilizes HTTP Secure (HTTPS), a combination of the HTTP and encrypted SLS/TLS, to protect information as it is shared across networks.[39] The company also automatically changes links to external websites to their encrypted, HTTPS version.[40] These statistics and more demonstrate how internet users are motivated to find ways to confidentially utilize the many tools and resources available online, in order to exercise their rights to privacy, access to information, and freedom of expression.

Like anonymity and pseudonymity, the use of encryption is inseparable from the rights it protects. Limitations hurt users, and leave them vulnerable to state surveillance as well as criminal malfeasance, and are largely unacceptable under human rights standards.

Conclusion

Undermining anonymity, pseudonymity, and encryption undermines the foundational rights of internet users. Backdoors into encryption are not reasonable, feasible, nor permissible. User-protective technologies and standards should be as strong as they can be and not artificially weakened to promote surveillance**.** Governments should not treat all users of online communications platforms as criminals simply because terrorists may occasionally use the same tools. The use of anonymity- or pseudonymity-friendly tools or encryption technologies on must be protected under the same standards as free expression itself. We hope Special Rapporteur Kaye will agree that any restrictions to these rights-protective practices are essentially restrictions on the rights themselves and must be protected with the same high standards.

For more information, please contact:

Drew Mitnick
Policy Counsel
Access
1110 Vermont Ave NW
Washington, DC 20005
drew@accessnow.org

Katherine Glenn Bass
Deputy Director, Free Expression Programs
PEN American Center
588 Broadway, Suite 303
New York, NY 10012
kglennbass@pen.org

[39] Duck Duck Go Privacy Policy, available at https://duckduckgo.com/privacy.
[40] Id