KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY ON THE USE OF ENCRYPTION AND ANONYMITY IN DIGITAL COMMUNICATIONS

13 February 2015

The Center for Democracy & Technology welcomes the opportunity to provide input for the report that the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, David Kaye, is preparing on the relationship between freedom of expression and the use of encryption and other technologies to transact and communicate anonymously online.

Since the initial June 2013 revelations from Edward Snowden of mass government surveillance of global communications networks, engineers, mathematicians, and technology and telecommunications companies around the world have devoted significant time and effort to strengthening communications networks, services, and devices against overbroad government surveillance. In recent months, high-ranking officials from some of the worst perpetrators of government surveillance have challenged the use of strong encryption and have demanded "backdoors" into encrypted communications products and services. Governments are actively trying to pressure Internet companies to weaken the encryption they apply to their users' communications, so that government may more easily intercept private data and surveil individuals around the world.

This is the wrong approach. Weakening encryption or prohibiting its use damages the security of online transactions, the confidentiality and integrity of communications, and the individual rights to freedom of opinion and expression. Governments are obligated to protect and promote fundamental rights and should not take steps to undermine individuals' ability to protect the security, integrity, and confidentiality of their communications. Further, as individuals increasingly rely on Internet-connected devices and remote-storage facilities to preserve their private thoughts, ideas, and creations, encryption will be essential to ensuring that they can engage in the exploration of concepts and ideas that forms the foundation for freedom of opinion.

In the following four sections, we:

1. Explain the role of Internet intermediaries in the online communications environment and the consequences of intermediation for individuals' right to freedom of expression;

2. Reinforce the relationship between anonymity and free expression and underscore the threat to free expression posed by widespread surveillance;

3. Describe the value of encryption and other security-enhancing technologies in safeguarding human rights online; and

4. Urge intermediaries to respect their users' fundamental rights and implement strong encryption.

We hope this will be a useful submission in assessing government demands for weakened encryption standards and greater access to individuals' information via Internet intermediaries.

I. Individual freedom of expression online depends on intermediaries.

The global Internet has become an indispensible platform for the freedom of expression. Billions of individuals around the world use the Internet to exchange ideas and information; gather and disseminate news and research; discuss and debate social and economic policy; create, share, and preserve art and literature; conduct business; contact loved ones and meet new people; and record their private thoughts.

Out of technical necessity, all of this expression is intermediated: individuals depend on the interconnected network of backbone network operators, Internet access providers and telecommunications carriers, content delivery networks, and remote hosting providers to exchange and store data. They rely on the millions of websites, online services, and applications that run on this infrastructure to facilitate their access to information and communication with other individuals around the world. Increasingly, they depend on remote storage even of their private data, as keeping their personal notes, drafts, journals, and photographs in the cloud allows them to access this information across a range of personal devices.

As we discuss below, potential scrutiny by third parties can have a chilling effect on individuals' exercise of their freedom of expression. The particular challenge of the Internet is that, because all Internet-based communication necessarily involves and depends upon intermediaries, Internet users' communications are potentially exposed to a number of third parties as a matter of course. These third-parties may be the technically anticipated intermediaries – for example, when one person sends an email to another, the intermediaries involved include the sender's Internet access provider, the backbone network, the email service provider, and the ISP and email provider of the email's recipient.

Along the way, however, other third parties may also attempt to gain access to the communication; these could include government officials and malicious private actors. These third parties may attempt to access this communication while it is in the control of any one of these intermediaries—while in transit on the access and backbone networks or in storage on the email service provider's servers—or while it is in possession of the sender or recipient. There are many potential points of vulnerability between the sender and recipient of the email, where third-party scrutiny could intrude.

The same is true for online expressive activity outside of person-to-person communications. When a person reads an online news source, posts to her social media account, plays a game on her mobile device, makes a purchase from an online book store, or looks up information via a search engine, multiple intermediaries facilitate that activity. And it is increasingly the case that intermediaries are involved even in expressive activity that a person would consider wholly private, as more services move to cloud storage. Apple's iCloud service, for example, stores a

person's files—photos, documents, contacts, spreadsheets, presentations, notes, and other types of files—on remote servers so that individuals can access them from any device.[1] Cloud-based email services store the email sent and received from an account, and will also preserve copies of draft emails that contain thoughts and ideas a person has formulated but never sent. Many social media platforms give users the opportunity to store drafts of posts and comments, to refine, complete, or delete at a later date. Even the thoughts and ideas that a person records locally on her own devices, using software that has no network capability, may end up in the custody of an intermediary: some automated back-up services store archival copies of a person's hard drive on remote servers,[2] meaning that even private notes, journal entries, and other non-public records of a person's thoughts and developing opinions will be under the technical control of an intermediary.

The role of Internet intermediaries in facilitating individuals' freedom of expression online has been well-documented by a number of expert commentators, including in previous reports from the Special Rapporteur on freedom of opinion and expression. As the former Special Rapporteur, Frank La Rue, noted in his 2011 report, "With the advent of Web 2.0 services, individuals can now publish information without the centralized gateway of editorial review common in traditional publication formats."[3] A recent report from UNESCO provides a comprehensive review of the many forms and functions of intermediaries in the Internet ecosystem and discusses the way these entities enable freedom of expression for Internet users around the world.[4]

Crucially, as La Rue and others have noted, intermediaries also have the potential to leverage their technical control over their users' communications to negatively impact individuals' freedom of expression.[5] ISPs are technically able to inspect traffic that flows over their networks and block or filter certain content; operators of websites that host user-generated content can decide to take down users' speech or to deactivate their accounts entirely. This is not to say that this exertion of technical control by intermediaries is necessarily inappropriate in every case. To the contrary: filtering of unwanted spam by ISPs is an accepted and beneficial practice, and website operators routinely take down content that violates their terms of service.[6]

The threat to individuals' rights is heightened, however, when governments compel intermediaries to use their technical control over individuals' communications in order to impose censorship and conduct secret surveillance. This can occur in an indirect form, as when

---

[1] *See* iCloud, http://www.apple.com/icloud/.

[2] *See, e.g.*, CrashPlan (online backup service), http://www.code42.com/crashplan/; SpiderOak (online backup and cloud-syncing service), https://spideroak.com/.

[3] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly document A/66/290 (16 May 2011), p. 11, *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (hereinafter "La Rue Internet Report").

[4] *See* UNESCO, Fostering Freedom Online: The Role of Internet Intermediaries (2014), *available at* http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

[5] *See, e.g.*, La Rue Internet Report, p. 13.

[6] For CDT's recommendations for content takedown policies that respect users' rights, *see* Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users (2011), *available at* https://www.cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf.

governments enact laws that hold intermediaries legally liable for unlawful content created and posted by their users.[7] These laws incentivizes intermediaries to restrict users' speech well beyond what is prohibited by law, rather than risk incurring legal penalties themselves.[8] Governments also act directly to compel intermediaries; as La Rue noted in his 2013 report on the relationship between surveillance and free expression, "Corporate actors have had to respond to requirements that digital networks and communications infrastructure be designed to enable intrusion by the State. . . . Increasingly, States are adopting legislation requiring that communications service providers allow States direct access to communications data or modify infrastructure to facilitate new forms of State intrusion."[9] State action to compel intermediaries to provide insecure communications facilities to their users represents a significant threat to the fundamental rights to privacy and freedom of expression.

II. Privacy and anonymity are deeply entwined with the right to freedom of expression.

The ability to speak and to seek information anonymously is a crucial enabler of the right to freedom of expression. Many individuals around the world face potential reprisal – whether from their government, their employers, their community, or their families – for daring to express their opinions and ideas. The protective veil of anonymity allows these individuals to engage in discourse about political and social topics that might otherwise be off-limits, and to explore information and ideas about sensitive issues without the chilling effect of potential scrutiny.

In the wake of the Snowden revelations, a number of researchers have documented the contemporary chilling effects of mass surveillance on individuals around the world. Human Rights Watch and the American Civil Liberties Union have reported on the chill faced by journalists and lawyers, who have professional ethical obligations to maintain the security and confidentiality of their communications with sources and clients.[10] PEN American Center conducted an international survey of writers in late 2014 and found that one in three writers in liberal democratic countries "had avoided writing or speaking on a particular topic, or had seriously considered it, due to concerns about surveillance."[11]

The chilling effect of potential scrutiny impacts not only those who speak, but those who seek and receive information as well. In the United States, librarians – who play a key intermediary

---

[7] La Rue Internet Report pg. 11-13; *see generally* UNESCO, Fostering Freedom Online, pg. 39-53.

[8] *See* Center for Democracy & Technology, Shielding the Messengers: Protecting Platforms for Innovation and Expression (2012), *available at* https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf.

[9] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 (17 April 2013), p. 19, *available at* www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (hereinafter "La Rue Surveillance Report"). La Rue also noted that some companies voluntarily collaborate with state agencies to facilitate state surveillance of communications. *Id.* at 19-20. He further noted, "The private sector has also often failed to deploy privacy-enhancing technologies, or has implemented them less than secure ways that do not represent the state of the art." *Id.* at 20.

[10] Human Rights Watch and American Civil Liberties Union, With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy (2014), *available at* http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

[11] PEN American Center, Global Chilling: The Impact of Mass Surveillance on Global Writers (2015), p. 6, *available at* http://www.pen.org/sites/default/files/globalchilling_2015.pdf.

role in society, enabling people's right to access to information – have been at the forefront of the fight to protect individuals' reading records against overbroad state surveillance powers (notably Section 215 of the PATRIOT Act).[12] The American Library Association has expressed concerns about surveillance and its impact on free expression, noting: "Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society. . . . One cannot exercise the right to read if the possible consequences include damage to one's reputation, ostracism from the community or workplace, or criminal penalties. Choice requires both a varied selection and the assurance that one's choice is not monitored." The International Federation of Library Associations and Institutions likewise affirms that, "Library users shall have the right to personal privacy and anonymity. Librarians and other library staff shall not disclose the identity of users or the materials they use to a third party."

By its technical nature, the Internet can support anonymous communication on a mass scale. This is because communications sent over Internet protocol are not inherently linked to an individual's identity; the sole identifier required for an Internet-based communication is an IP address, which, unlike a persistent identifier such as a government-issued identification number, can be randomly assigned and re-assigned, carries no additional identifying information within itself, and is technically an address for a specific device as opposed to a specific individual. Of course, in practice there is great potential for entities to combine information associated with IP addresses to glean identifying information about an individual, and it is typically appropriate to protect IP addresses as personal information under consumer data protection legislation. It is a particular threat to individuals' privacy and free expression rights when governments create data retention mandates, as the Court of Justice of the European Union recognized last year.[13] Unfortunately, governments have not all heeded this decision, as demonstrated by recent proposals in the United Kingdom that would require websites to maintain IP address logs, so that the anonymous visitors to a site could later be matched with IP address allocation records maintained by their Internet service providers.[14]

But even in the face of these efforts to identify individuals online, people have a number of options for using the Internet in an anonymous or less-identifiable way. The simplest of these is using a pseudonym; because Internet communications are not inherently connected to an individual's specific identity, users are constantly faced with a choice of whether to link their

[12] American Library Association, Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users (2003), *available at* http://www.ala.org/offices/oif/statementspols/ifresolutions/resolutionusa.

[13] Emily Barabas, "European Court of Justice: EU Data Retention Directive Infringes on Human Rights" (10 April 2014), https://cdt.org/blog/european-court-of-justice-eu-data-retention-directive-infringes-on-human-rights/.

[14] Rita Cant and Sarah St.Vincent, Comments on Part 3 of the draft Counter-Terrorism and Security Bill (15 December 2014), p. 3-7, https://cdt.org/insight/cdts-comments-on-part-3-of-the-uks-draft-counter-terrorism-and-security-bill/.

communications to their legal identity or to use a pseudonym.[15] Every account that individuals create – email, social media, commenting on newspapers or message boards – involves this choice, allowing people to easily switch to new and different names and to independently maintain both highly identified and pseudonymous accounts. Those concerned with further obscuring their digital trail can use tools such as virtual private networks (VPNs)[16] or Tor[17] to secure greater protection of their identifying information from governments, companies, intermediaries, and malicious actors who might attempt to identify them or scrutinize their online activity. These more robust privacy-protecting tools depend on encryption.

It is important to note that individuals can use privacy-enhancing tools to achieve varying degrees of anonymity – not all tools provide, and not all users seek, "perfect anonymity" or total protection against ever being identified by any adversary. For many people, preserving a separation between their online commentary and exploration and their offline identities is both necessary and sufficient. If the scrutiny that a person fears would come from their local community, family members, potential employers, or others who would not be using sophisticated surveillance techniques, then merely the ability to use a pseudonym online could provide meaningful protection. Even these relatively simple privacy-preserving measures can have an important impact on individuals' right to freedom of expression, and their use should be protected by law.

In this age of mass communications surveillance by government, however, most individuals face threats to the confidentiality and security of their communications from sophisticated government actors. Responding to these threats, and to the persistent threats from malicious private actors,[18] requires the use of strong encryption technology.

III. Encryption is essential to protecting and respecting individuals' right to freedom of expression.

On the Internet, the discipline of computer security – which includes cryptography – focuses on creating the technical means for protecting stores of personal information and ensuring that computer programs operate only in an authorized manner. Computer security rests on three pillars – confidentiality, integrity, and authentication – each of which are implemented through cryptographic methods.

Confidentiality is the property most commonly associated with encryption and cryptography. Cryptographic methods can be used to turn data (e.g., emails, chat messages, website requests, files) into seemingly unintelligible information that is indistinguishable from random

---

[15] Some governments have responded to the Internet's potential to enable anonymous communication by creating requirements that users register for online accounts with their legal names. *See, e.g.*, BBC News, "South Korea's real-name net law is rejected by court" (23 August 2012), *available at* http://www.bbc.com/news/technology-19357160; Josh Chin, "China Is Requiring People to Register Real Names for Some Internet Services," Wall Street Journal (Feb. 4, 2015), *available at* http://www.wsj.com/articles/china-to-enforce-real-name-registration-for-internet-users-1423033973.

[16] *See, e.g.*, Astrill (personal VPN service), https://www.astrill.com/.

[17] Tor (onion routing service), https://www.torproject.org/.

[18] *See, e.g.*, Bill Hardekopf, "The Big Data Breaches of 2014," Forbes (13 January 2015), *available at* http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

data. This encrypted data can only be rendered comprehensible again with the application of the same cryptographic method and the use of a secret key. Confidentiality in communications is achieved when the contents of the communication between two or more parties are incomprehensible to potential eavesdroppers.

Integrity involves ensuring communications content remains unmodified in transit. There are many cases where two parties communicating online want to make sure that content they send – the message in a chat session, or instructions to transfer a certain amount of money to a bank account – is unmodified during transmission and receipt. Communications intermediaries such as web servers and web browsers can ensure integrity by, for example, calculating a "cryptographic hash" for each communication. A cryptographic hash is the digital equivalent to a fingerprint; it is a short set of alphanumeric characters that is always unique for the same input value (e.g., a file or an email) and which changes noticeably with a slight change in the input.[19] When one or both parties to a communication want to ensure that it is not modified in transit, a cryptographic hash of the communication can be calculated and sent along with the message. The recipient can calculate the hash of the message she receives and compare it to the hash value that was sent; if the two are equal, then the contents of the message were not modified.

Authentication, the third pillar of computer security, ensures that the parties on the other side of the communication are indeed who they claim to be. This requires that one party to the communication present credentials that the other party can verify. Offline, for example, the details on a person's government-issued identity card are backed or verified by the government agency that issues it. This allows others presented with the credential to rely on those details (e.g., a person's birthdate) after making their own verification that the credential matches the person who offers it (e.g., matching the photo on the ID with the person's face). Online, authentication works within a system of cryptographic credentials. When a person visits an authenticated website, that site transmits a form of cryptographic credential called a "certificate." The person's web browser checks that the certificate was validly issued and compares the domain name in the certificate to the domain name in the web address the person is trying to visit. The certificate in question is essentially an encryption key that has been issued by a "certificate authority." When the website operator applies for a certificate, the certificate authority verifies that the person requesting the certificate for a given domain name is authorized to communicate from that domain name. This verification can be done through various processes, which can be as simple as an email confirmation sent to an email address at the domain in question, to complex processes including real-world site visits, notarized documents, and audits.

Together, the three elements of confidentiality, integrity, and authentication embodied through cryptography work in concert to protect us online. When a user visits an encrypted website like https://www.cdt.org, the user's browser first receives and checks the validity of the website's certificate. To authenticate the server, the browser checks to ensure that a known certificate authority has vouched for the certificate and that the certificate is valid for the domain cdt.org. The certificate contains an encryption key that the user's browser then uses to talk to the server in a confidential (encrypted) communications session. Every encrypted communication between cdt.org and the user's browser will include integrity checks – cryptographic hashes – that both

[19] For example, a cryptographic hash (using the SHA-1 algorithm) of the phrase "cryptographic hash" is `5da4ce48dfd652f875f076556e607a03e4f160ca` while a hash of a slightly different phrase "kryptographic hash" is `74b69dd6eb7ee1f8ad69e239a3a369ee1baab8aa`, i.e., very different.

sides can use to check and make sure that the contents of their communications have been undisturbed in transit.

In addition to protecting the confidentiality and integrity of communications in transit, encryption can also be used to secure information when it is at rest—in storage on an individual's device or on a remote server. Apple and Google recently announced their intentions for their mobile devices to be "encrypted by default."[20] This means that all the data stored on the phone itself will be unreadable to anyone who accesses the phone without knowing the owner's password or cryptographic key. Encryption of all data on a device by default ensures that if a third party acquires the device, he will be unable to access the sensitive information—photos, videos, emails, call records, voicemail, text messages, web search history—stored on the device. Similarly, encrypted cloud storage ensures that a person's private thoughts and communications will not be vulnerable to unauthorized access by a third party—an essential guarantor of privacy to enable individuals to enjoy their freedom of opinion and expression.

Thus, we see that encryption offers a compelling answer to the challenge to free expression posed by the intermediated nature of the Internet: strong encryption prevents exploitation of the many points of potential vulnerability that intermediaries inescapably create in online communications. .

IV. Intermediaries have a responsibility to respect their users' human rights and should implement strong encryption.

Further, when companies offer stronger encryption capabilities to their users, they are upholding their responsibilities to respect the human rights of the people who are impacted by their business practices. The UN Guiding Principles on Business & Human Rights holds as a foundational principle that "Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."[21] In the context of Internet intermediaries, this calls for companies to evaluate their practices for their impact on their users' rights to freedom of expression and privacy. A number of information and communications technology (ICT) companies have taken up this responsibility explicitly, joining initiatives such as the Telecommunications Industry Dialogue[22] and embracing human rights standards when engaging in corporate transparency reporting.[23]

---

[20] Joe Miller, "Google and Apple to introduce default encryption," BBC News (19 September 2014), http://www.bbc.com/news/technology-29276955.

[21] United Nations, Office of the High Commissioner on Human Rights, Guiding Principles on Business and Human Rights (2011), p. 18, *available at* http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[22] Telecommunications Industry Dialogue on Freedom of Expression and Privacy: Guiding Principles (2013), *available at* http://www.teliasonera.com/Documents/Public%20policy%20documents/Telecoms_Industry_Dialogue_Principles_Version_1_-_ENGLISH.pdf.

[23] Sarah St.Vincent, "Human Rights and Surveillance: Governments Must Comply with Their Transparency Obligations" (20 June 2014), *available at* https://cdt.org/blog/human-rights-and-surveillance-governments-must-comply-with-their-transparency-obligations/.

Another such effort, the Global Network Initiative, brings together leading ICT companies, civil society, academics, and investors to collaborate on issues of users' rights to freedom of expression and privacy; GNI member companies agree to a set of guiding principles, which include commitments to respect the free expression rights of their users "by seeking to avoid or minimize the impact of government restrictions on freedom of expression."[24] GNI companies also commit to "employ protections with respect to personal information in all countries where they operate" and to "respect and protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards."[25] As ICT companies become increasingly essential intermediaries for people's access to information and opportunities for expression, these initiatives and commitments are increasingly vital to preserving an online communications environment that promotes and respects human rights.

The revelations of extensive mass surveillance activity by the US National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ), and other intelligence agencies around the world have provided ample opportunity for intermediaries to identify and take steps to "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur."[26] For example, Edward Snowden's disclosures about the MUSCULAR program conducted by the NSA revealed that the NSA was tapping unencrypted data links within companies' internal networks.[27] Large online service providers have servers and data warehouses around the world, and it had been relatively common practice to treat this distributed network as a company's internal (and presumably secure) network. But, because the actual fiber connecting these servers was maintained by third parties, the NSA was able to obtain access to these unencrypted data streams without alerting the companies.

Clearly, secret government surveillance that involves mass collection and review of millions of users' communications is a threat to those individuals' human rights. This vulnerability of user communication to overreaching government surveillance was created, however inadvertently, by companies' decision to transmit data in unencrypted form across infrastructure not wholly within their control. Companies who have begun encrypting these data transfers have appropriately taken steps to address the demonstrated adverse impact on their users' privacy and free expression rights.[28] While it remains the obligation of governments to reform their surveillance practices and to cease their incursion into the fundamental rights of people around the world,

---

[24] Global Network Initiative: Principles, *available at* https://globalnetworkinitiative.org/principles/index.php.

[25] Id.

[26] UN Guiding Principles, p. 14.

[27] CDT and American Civil Liberties Union, Secret Surveillance: Five Large-Scale Global Programs, Joint Submission to the United Nations Twenty-Second Session of the Universal Periodic Review Working Group (May 2015), p.8, *available at* https://cdt.org/insight/secret-surveillance-five-large-scale-global-programs/.

[28] *See, e.g.*, Ben Kepes, "In An Attempt to Beat the NSA, Google Encrypts Inter-Server Gmail Traffic", Forbes (20 March 2014), http://www.forbes.com/sites/benkepes/2014/03/20/in-an-attempt-to-beat-the-nsa-google-encrypts-inter-server-gmail-traffic/; Sean Gallagher, "Web giants encrypt their services—but leaks remain", Ars Technica (10 June 2014), http://arstechnica.com/information-technology/2014/06/a-year-after-snowden-internet-crypto-remains-spotty/.

the UN Guiding Principles are clear that businesses have an independent responsibility to respect human rights even in the face of recalcitrant governments.[29]

Moreover, governments should not interfere with intermediaries' efforts to provide stronger encryption for their users' communications. Article 17 of the International Covenant on Civil and Political Rights provides that "(1) no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) everyone has the right to the protection of the law against such interference or attacks." Today, "correspondence" is understood to refer to all forms of communication, including email and "information derived from the monitoring of personal internet usage."[30] As the Special Rapporteur noted in 2011, "The right to private correspondence thus gives rise to a comprehensive obligation on the part of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without interference or inspection by State organs or by third parties."[31]

We agree with the previous conclusion of the Special Rapporteur that "Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys."[32] As discussed above, encryption provides for the security from interference and integrity of source for emails and other communications sent via the Internet. Encryption of online communications is by far the best way to "ensure that emails and other forms of online communication are actually delivered to the desired recipient without interference or inspection by State organs or by third parties." States should not interfere with efforts to provide exactly this sort of protection to individuals' communications, and should support intermediaries' efforts to respect the privacy and free expression rights of their users.

About the Center for Democracy & Technology // www.cdt.org
The Center for Democracy & Technology is a non-profit public interest organization that works to advance human rights online, and is committed to finding forward-looking and technically-sound solutions to the most pressing challenges facing users of electronic communications technologies. With expertise in law, technology, and policy, CDT seeks to enhance free expression and privacy in communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For more information, please contact **Emma J. Llansó, Director, Free Expression Project, ellanso@cdt.org**
Joseph Lorenzo Hall, Chief Technologist, jhall@cdt.org

[29] UN Guiding Principles, p. 13.

[30] C*opland v. the United Kingdom*, European Court of Human Rights (Application no. 62617/00), para. 41, *available at* http://www.bailii.org/eu/cases/ECHR/2007/253.html (interpreting "correspondence" in Article 8 of the European Convention on Human Rights).

[31] La Rue Internet Report, p. 16 (citing Manfred Nowak, UN Covenant on Civil and Political Rights, CCPR Commentary, p. 401).

[32] La Rue Surveillance Report, p. 22.