Freedom of Expression, Privacy and Anonymity on the Internet

Comments submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression

January 2011

Contact: Katitza Rodriguez, EFF International Rights Director, Katitza@eff.org

Freedom of Expression, Privacy and Anonymity on the Internet

Comments submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression

Introduction

Thank you for providing the Electronic Frontier Foundation (EFF) with the opportunity to add our written contribution to the consultation on freedom of expression online.

EFF is an international civil society non-governmental organization with more than 14,000 members worldwide, dedicated to the protection of citizens' online civil rights, privacy, and freedom of expression. EFF engages in strategic litigation in the United States and works in a range of international and national policy venues to promote balanced laws that protect civil rights, foster innovation and empower consumers. EFF is located in San Francisco, California and has members in 67 countries throughout the world.

EFF has been asked to comment on the importance of privacy vis-à-vis the government, anonymity on the Internet, and some recent trends that have resulted in broader surveillance powers and capabilities for law enforcement and intelligence agencies, which now pose clear threats to citizens' rights of freedom of expression, privacy, and freedom of association.

I. Summary

This paper focuses on the right to privacy vis-à-vis the government and the importance of anonymity on the Internet. Privacy is a universal human right for all individuals regardless of nationality. It strengthens human dignity and other rights such as freedom of expression and association. Almost all international conventions on human rights protect the right to privacy.

The right to privacy of communications and freedom of expression includes the right of every individual to use encryption technology. This means that service providers should be able to design systems for end-to-end privacy, and Internet intermediaries should not

block the transmission of encrypted communication.

The right to freedom of expression includes the right to speak, read, and communicate anonymously. This includes the right of every individual to use circumvention technology and anonymity tools because the right *to seek and receive* information includes the right to read anonymously.

Every individual must have confidence that the service providers that host their discussions will protect their privacy. Internet intermediaries and service providers occupy a key position in online communications. Unlike other Internet users, Internet intermediaries and service providers often know the identity of the person who creates a website or posts material on a platform. Anonymous speech is critical for the protection of freedom of expression and privacy rights. To protect citizens' rights to anonymous expression, the laws must allow and encourage Internet intermediaries to respect the due process rights of an online speaker before identifying that individual in response to a request to do so. EFF believes that judicial systems, not extrajudicial decision-making processes, are best suited to balance citizens' right to anonymous expression with the need to provide a means to redress wrongs when they occur.

EFF is deeply concerned about the impact of overbroad national implementations of the Council of Europe (CoE) Cybercrime Convention on citizens' privacy and freedom of expression. Our central concerns are:

- The Convention establishes a series of offenses, drafted with vague and obscure language, which could endanger legitimate activities and free expression on the Internet.
- The Convention grants broad surveillance powers to law enforcement authorities, and requires ISPs to cooperate with them in the preservation, production, search, and seizure of stored computer data, real-time collection of traffic data, and interception of content data. However, the Convention does not provide any meaningful countervailing civil rights protections to ensure that minimum standards and legal safeguards consistent with international human rights accords are implemented in national laws.
- The Convention does not contain a dual illegality requirement. It requires that government A help enforce other countries' "cybercrime" laws, even if the act being prosecuted is not illegal in country A. Therefore, country B with weaker freedom of expression protections can force law enforcement agencies in country A to uncover the identities of anonymous critics, monitor their communications on behalf of foreign governments, or force ISPs in country A to obey another jurisdiction's requests to log their nationals' behavior without due process or compensation.

We also wish to highlight several other recent disturbing trends which have led to broader surveillance powers and capabilities for law enforcement and government

intelligence agencies, as follows:

- Increased electronic interception capabilities: many countries around the world have enacted legal regimes that force communications carriers to provide wiretapping assistance to law enforcement and intelligence agencies via automated systems. Mandating government back doors for lawful interception weakens network security and could just as easily be exploited by criminals for unrelated matters.
- Lowering privacy protections and oversight mechanisms for the protection of transactional data vis-a-vis the government: transactional data should not have lesser protection based on technical details about how the data is stored, processed, or transmitted. Moreover, the increased collection of transactional information by telecommunications providers of all individuals in a given country can be to used compose a revealing profile of the individual's concerns, interests, and associations, including the identities of journalists' sources by the authorities.
- Budapest PLUS: the enactment of mandatory data retention regimes compels Internet service providers and telecom companies to collect and store data about everyone's telecommunication and Internet transactions, including the information of those not suspected or convicted of any crime; the most prominent example is the EU Data Retention Directive, adopted by the European Union in 2006. However, Australian and Brazilian government officials have respectively announced that they are evaluating mandatory data retention regimes.
- Emerging issues: we have identified the need to strengthen legal safeguards against government access to citizens' data hosted by third party providers, especially cloud computing providers. Because individuals and governments are relying more heavily on those services, information that was previously stored on your hard drive, stored in a file in your office or at your home, is now being hosted by third party cloud providers. EFF believes that there is a need to identify best practices that have been adopted by cloud computing providers where civil subpoenas or court orders are served upon them for third party data that is stored with them. For example, notifying the owner of the data that the provider has received a subpoena or court order, and providing an opportunity for the owner to respond and file a judicial challenge to the disclosure of data held by the cloud-computing provider.

Finally, this paper addresses the role that corporations should play in the protection of citizens' privacy, freedom of expression and fundamental human rights. EFF has called attention to recent reported instances of corporations selling customized surveillance technologies to authoritarian regimes in situations where they know or should have known that the technologies will be used to target people for arrest, torture, or forced disappearance.

II. International Privacy Framework

Privacy is a universal human right for all individuals regardless of borders. It strengthens human dignity and other rights, in particular the right to freedom of expression and

association. Almost all international conventions on human rights protect the right to privacy.[1] Article 17 of the International Covenant on Civil and Political Rights, one of the most important international instruments, provides that:

> "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. Everyone has the right to the protection of the law against such interference or attacks."

The UN Office of the High Commissioner for Human Rights had emphasized that "this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons…The State should adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right."[2]

By making this connection, the UN Office of the High Commissioner made it clear that Article 17 of the Covenant deals with protection against both unlawful and arbitrary interference.

The UN Office of the High Commissioner explained that "it is precisely in State legislation above all that provision must be made for the protection of the right set forth in that article. The term 'unlawful' means that no interference can take place except in cases envisaged by the law, which itself must comply with the provisions, aims and objectives of the Covenant."[3] The UN Committee noted that the phrase 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."[4]

The limitations on the right to privacy or other aspects of Article 17 are subject to a

---

[1] *See* Universal Declaration on Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), the International Convention on the Protection of all Migrant Workers (Article 14), and the Convention on the Rights of the Child (Article 16), American Convention On Human Rights "Pact Of San Jose, Costa Rica. See EFF, International Privacy Standards, available at <http://www.eff.org/issues/international-privacy-standards>.

[2] United Nations Human Rights Commissioner, The right of privacy, family, home and correspondence, and protection of honor and reputation (Article 17), ICCPR General Comment 16, April 8, 1988, available at <http://www.unhchr.ch/tbs/doc.nsf/0/23378a8724595410c12563ed004aeecd?Opendocument>.

[3] *Id.*

[4] *Id.*

permissible limitations test.[5] The test includes the following elements:

- "Any restrictions must be provided by the law (paras. 11-12);
- The essence of a human right is not subject to restrictions (para. 13);
- Restrictions must be necessary in a democratic society (para. 11);
- Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
- For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);
- 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 (paras. 14-15);
- Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18)."[6]

The privacy of communications has also received strong protection at the international level. The Office of the Commissioner for Human Rights has also pointed out that "correspondence should be delivered to the addresses without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[7]

Many regional instruments and countries' national constitutions have also protected the right to respect for private and family life, the home, and the privacy of communications.[8] Interception of communications is only allowed under specific exemptions prescribed in the law.[9]

---

[5] Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," p11, available at <http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf>. See also General Comments No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999, available at <http://www.unhchr.ch/tbs/doc.nsf/0/6c76e1b8ee1710e380256824005a10a9?Opendocument>.

[6] *Id.*

[7] *Supra* note 2.

[8] *See* European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8) and the Cairo Declaration on Human Rights in Islam, available at <https://www.eff.org/issues/international-privacy-standards>.

[9] EPIC, Privacy International, "Privacy and Human Rights 2006. An International Survey of Privacy Law and Developments", 2006, available at

Despite the high degree of apparent protection for the right to privacy and the privacy of communications in international law and national constitutions, we have seen exponential growth in the development and use by governments and their agents of ubiquitous online surveillance technologies that threaten to make meaningless the legal protections for privacy. As more and more of our lives are lived online, the situation is only likely to get worse.

2.1 The Right to Use Encryption Technology

The privacy of communications includes the right of every individual to use encryption technology.[10] In the absence of encryption, online communications can easily be intercepted.[11] Internet intermediaries that store and forward our communications are in a position to possess and read all the communications that pass through their networks.

Service providers should be able to design systems for end-to-end privacy, and Internet intermediaries should not block the transmission of any encrypted communication. Both individuals and government agencies rely on strong encryption in their daily activities.[12] Moreover, human rights activists, journalists, refugees, bloggers, and whistleblowers rely on strong encryption technologies to protect their communications, the names and location of their sources and/or witnesses, etc.

Encryption impacts freedom of expression in two ways. First and foremost, encryption allows individuals to speak confidentially with others, without fear of retribution for unpopular ideas. Second, any attempt to restrict the distribution of encryption technology impacts the rights of the software creators to express their viewpoint through code. Furthermore, many security researchers provide open-source encryption software, and disclose encryption algorithms as an integral part of examining the encryption technology for flaws and weakness. This means that the encryption is available to the

---

<http//:www.privacyinternational.org/phr>.

[10] Encryption allows users to have private conversations over email, web browsing, or cell phones. To learn more: *See*, EFF, Surveillance Self Defense, available at <https://ssd.eff.org/tech/encryption>.

[11] *See* e.g. Firesheep, available at <http://codebutler.com/firesheep>. *See al*so John P. Mello Jr., Free Tool Offered To Combat Firesheep Hackers, PCWorld, November 23, 2010, available at <http://www.pcworld.com/article/211531/free_tool_offered_to_combat_firesheep_hackers.html>. Seth Schoen, Richard Esguerra, The Message of Firesheep: "Baaaad Websites, Implement Sitewide HTTPS Now!", EFF, October 29, 2010, available at <http://www.eff.org/deeplinks/2010/10/message-firesheep-baaaad-websites-implement>. EFF, Tool Offers New Protection Against 'Firesheep', November 23, 2010, available at <http://www.eff.org/press/archives/2010/11/23>.

[12] *See* e.g. Tor project, available at <http://www.torproject.org/about/torusers.html.en>.

world. The privacy of communications and freedom of expression also includes the right of every individual to publish encryption technologies and research;

Recently, the U.S. media reported that the FBI is seeking to increase its ability to spy on people's privacy.[13] From the news, the U.S. government appears to be discussing a new requirement that all communications systems be easily wiretappable by mandating "back doors" into any encryption systems. Government access to keys creates significant risks of abuse of government power. EFF believes that compelling the disclosure of a key to the back door into our houses so the government can read our "papers" in advance of a showing of probable cause will violate people's privacy rights. Therefore, our online communications shouldn't be treated any differently than the protection of the keys of our home.[14] A similar proposal named the Clipper Chip was defeated in 2001.[15] At the end of 2010, the Indian government announced it is exploring mandatory sharing of software by all communication service companies in India. The Indian government has already asked Canada's Research In Motion to hand over the encryption keys for its BlackBerry messaging services to law enforcement agencies by January 31, 2011.[16] Google has said that U.S. law prevents real-time sharing of Gmail's encryption keys with Indian government.[17] On January 13, 2011, Research in Motion reiterated that it did not have capabilities to provide access to Blackberries's encryptions keys.[18]

These threats of government access to encryption technology create significant risks of abuse of government power and raise serious concerns about privacy and online freedom of expression in the face of evolving technological challenges and governmental influences.

---

[13] Seth Schoen, Government Seeks Back Door Into All Our Communications, EFF, September 27, 2010, available at <http://www.eff.org/deeplinks/2010/09/government-seeks>.

[14] Cindy Cohn, Eight Epic Failures of Regulating Cryptography, EFF, October 20, 2010, available at <https://www.eff.org/deeplinks/2010/10/eight-epic-failures-regulating-cryptography>.

[15] *See* Shari Steele, Daniel Weitzner, Chipping Away at Privacy, EFF, 1993, available at <http://w2.eff.org/Privacy/Key_escrow/Clipper/clipper.summary>. *See also* The Clipper Chip, Wikimedia, available at <https://secure.wikimedia.org/wikipedia/en/wiki/Clipper_chip>.

[16] Google won't share encryption keys with Indian sleuths, The Economic Times, December 16, 2010, available at <http://economictimes.indiatimes.com/tech/internet/Google-wont-share-encryption-keys-with-Indian-sleuths/articleshow/7109074.cms>.

[17] *Id*.

[18] Reuters, BlackBerry-Maker Proposes India Solution, New York Times, January 13, 2011, available at <https://www.nytimes.com/reuters/2011/01/13/business/global/news-us-blackberry-india.html>.

III. Freedom of Expression, Privacy and Anonymity

Every individual has the right to freedom of expression, which includes the right to speak, read, and communicate anonymously, and which includes the right of individuals to use circumvention technology and anonymity tools. Throughout history individuals have been writing in anonymous or pseudonymous ways. Anonymous and pseudonymous expression allows individuals to express unpopular opinions, honest observations, and otherwise unheard complaints. On the Internet, every individual can communicate online without connecting their online identities with their offline identities.[19]

Individuals may decide to communicate anonymously out of concern about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.[20] Opposition parties, victims of violence, persons with HIV/AIDS, dissidents, and survivors of abuse can use the Internet to share sensitive and personal information anonymously without fear of harm. For all of these people, securing anonymity can be a matter of life or death.

3.1. Anonymity: Best and Bad Practices

In the United States, the Supreme Court has ruled that the right to speak anonymously is protected by the First Amendment. The Supreme Court has held that: "Anonymity is a shield from the tyranny of the majority," that "exemplifies the purpose" of the First Amendment: "to protect unpopular individuals from retaliation...at the hand of an intolerant society."[21]

It further said, courts must "be vigilant... [and] guard against undue hindrances to political conversations and the exchange of ideas."[22] This vigilant review "must be undertaken and analyzed on a case-by-case basis," where the court's "guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and

---

[19] EFF, Anonymity, available at <http://www.eff.org/issues/free-speech>.

[20] *Id.*

[21] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, available at <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=514&invol=334 >.

[22] Buckley, 525 U.S. at 192, available at <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=525&invol=182>.

rights at issue."[23] That review must take place whether the speech in question takes the form of political pamphlets or Internet postings.[24]

U.S. courts have also recognized that:

> *"People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."*[25]

The policies underlying these opinions provide best practices which are also embodied within the Universal Declaration of Human Rights.

Unfortunately some countries have adopted national legal frameworks that undermine protection of anonymity and their citizens' freedom of expression. For instance, in South Korea, the government has sought cooperation with Internet Service Providers (providers of blogs, and social media) to develop real-name systems for their users since 2003, thereby eliminating anonymity.[26] In Saudi Arabia, the media has reported that the government will require all online newspapers and bloggers to register with the Ministry of Culture and Information and to obtain a license, valid for up to three years. Recently, the media has reported that the Saudi government will ban all blogging without a license.[27] Although not required by law, a similar trend can be discerned in the terms of service adopted by some Internet media services in the U.S.. For instance, Facebook's Terms of Service require that Facebook users provide their real names and information.[28] This practice creates serious risks particularly for dissidents and human rights workers using their names on Facebook in authoritarian regimes. This creates a double negative effect: if Facebook's Terms of Service are violated, Facebook can

---

[23] Dendrite Int'l, Inc. v. Doe, available at <http://www.citmedialaw.org/threats/dendrite-international-v-does>.

[24] Reno v. ACLU, 521 U.S. 844

[25] Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999), <http://legal.web.aol.com/aol/aolpol/seescandy.html>.

[26] Open Net Initiative, Access Controlled, South Korea, available at <http://opennet.net/research/profiles/south-korea>.

[27] Emma Woollacott, Saudi Arabia Bans Blogging Without A Licence, Firetown, January 2011, available at <http://www.tgdaily.com/business-and-law-features/53403-saudi-arabia-bans-blogging-without-a-licence?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+tgdaily_all_sections+%28TG+Daily+-+All+News%29&utm_content=Google+Reader>.

[28] Facebook, Statement of Rights and Responsibilities, available at <https://www.facebook.com/terms.php>.

disable an individual's account, shutting down a key avenue for political discourse.[29]

3.2 Due Process before Disclosure of Identity of Anonymous Speaker

Every individual must have confidence that the service providers that host their discussions will protect their privacy. Internet intermediaries and service providers occupy a key position in online communications. Unlike other entities, Internet intermediaries and service providers often know the identity of the person who creates a website or posts material on a platform.

When an individual posts content on the Internet, third parties may want to sue the individual for posting allegedly defamatory or otherwise illegal content. To do so, the plaintiff will need to identify the online speaker. However, anonymous speech is critical for the protection of freedom of expression and privacy rights. In order to protect citizens' rights to anonymous expression, an Internet intermediary must respect the due process rights of an online speaker before identifying that individual in response to a request to do so. Otherwise, as the U.S. Supreme Court has noted, forced "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[30] While some countries, like Brazil, forbid anonymity in their constitutions,[31] it has proved to be such a compelling tool for enhancing public exchange in the digital environment that Brazilians seem pretty resolute in maintaining their right to communicate anonymously.[32]

Judicial systems are best suited to balance citizens' right to anonymous expression with the need to provide a mechanism to redress wrongs. But judicial systems can only function when a court has an opportunity to review the circumstances before the identity is revealed.

Therefore, to protect citizens' fundamental rights of freedom of expression and privacy, Internet intermediaries should only disclose the identity of an anonymous or

---

[29] Eva Galperin, EFF Calls for Immediate Action to Defend Tunisian Activists Against Government Cyberattacks, EFF, January 2011, available at <https://www.eff.org/deeplinks/2011/01/eff-calls-immediate-action-defend-tunisian>.

[30] Talley v. California, 362 U.S. 60 65 (1960), available at <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=362&invol=60>.

[31] Brazilian Constitution, available at <http://www.v-brazil.com/government/laws/titleII.html>.

[32] Jose Murillo, Holding the Line for Internet Freedoms in Brazilian Cyberspace, Global Voices, available at <http://globalvoicesonline.org/2006/11/11/holding-the-line-for-internet-freedoms-in-brazilian-cyberspace/>.

pseudonymous user of their platform or service upon receipt of a court order, granted after a process of judicial review. Internet intermediaries should:

- Make reasonable efforts to notify the person whose identity is sought.
- If possible, agree to a timetable for disclosure of the information to the party seeking it that provides a reasonable opportunity for the Internet user to file an objection with a court before disclosure.
- Forward the exact statements and material provided by the person seeking the identity, including information about the cause of action alleged in the lawsuit and the evidence provided by the identity-seeker to the court where provided to the service provider.[33]

EFF also recommends that "the user should be provided with a reasonable amount of time, such as 30 days, to respond before the Online Service Provider produces the requested information. This will give the user an opportunity to object to disclosure of his or her identity."[34]

3.3 Disclosure of Identity of Anonymous Speaker: Bad Practice

In the U.S., it is all too common for plaintiffs to issue subpoenas to intermediaries to obtain the identities of their critics in order to intimidate and silence them, even where those seeking to identify have no intention of prosecuting a lawsuit against the speaker or where the posted content is lawful. These subpoenas may be issued by attorneys without prior judicial approval. In some circumstances, such as a subpoena issued pursuant to the Digital Millennium Copyright Act, a lawsuit is not necessarily filed first.[35] In recent years, a few enterprising law firms in the U.S., the U.K. and Europe have used mass copyright litigation to extract settlements from individuals. These law firm groups

[33] This test reflects the exam that has evolved under U.S. law. See EFF, Test for Unmasking Anonymous Speech, Internet Law Treatise, available at <http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers>.

[34] EFF, Best Practices for Online Service Providers, available at <http://www.eff.org/wp/osp>.

[35] Section 512(h) of the Digital Millennium Copyright Act allows copyright holders to subpoena service providers for user identity information without filing a lawsuit. See, Digital Millennium Copyright Act, available at <https://ilt.eff.org/index.php/Copyright:_Digital_Millennium_Copyright_Act>. Although U.S. courts have recognized limitations on when such expedited subpoenas can be used. It does not extend to obtaining the identity of alleged file-sharers extra-judicially. See Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003); Recording Industry Association of America, Inc. v. Charter Communications, Inc., 393 F.3d 771 (8th Cir. 2005).

try to grow businesses out of suing Internet users on behalf of copyright owners.[36] These lawsuits follow the model of those filed by members of the Recording Industry Association of America in 2003.[37] The U.S. lawsuits sued thousands of unnamed "John Doe" defendants and asked courts to issue subpoenas to ISPs to require them to disclose the identities of the alleged infringers to the copyright owners, so that the copyright owners could then sue the identified individuals. Once the Internet user's identity is known, the possibility of an award of pre-established statutory damages (of up to $1500,000 per copyrighted work allegedly used) frequently pressures defendants into settling. These lawsuits raise concerns about due process and the protection of citizens' right to privacy.[38] In particular, the potential for mistaken identification of alleged infringers as occurred in previous mass copyright litigation campaigns raises serious concerns for the many innocent individuals were caught in the crossfire.[39]

3.4 The Right to Read Anonymously

Article 19 of the Universal Declaration of Human Rights enshrines the right to freedom of opinion and expression, which includes the right to *seek, receive and impart* information and ideas through any media. To provide meaningful protection for citizens' freedom of expression rights, this requires that every individual has the right to use circumvention technologies to read and communicate anonymously.

The right *to seek and receive* information is chilled when the government has unchecked access to reading records. The U.S. Supreme Court has supported the right to read anonymously in several decisions: "Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of anyone who reads…. Fear of criticism goes with every person into the bookstall.… Some will fear to read what is unpopular, what the powers-that-be dislike….Fear will take the place of freedom in the libraries, book stores, and homes of the land. Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press."[40]

---

[36] EFF, Copyright Trolls, available at <https://www.eff.org/issues/copyright-trolls>. EFF, USCG v. The People, available at <https://www.eff.org/cases/uscg-v-people>.

[37] They begin by suing unnamed John Does, then seek to subpoena the ISPs of users in order to obtain their identities, then sue the individuals themselves.

[38] Achte-Neunte v. Does, available at <http://www.eff.org/cases/achte-neunte-v-does>. *See also* EFF, Anonymity Protection Lawsuits, available at <https://www.eff.org/issues/anonymity>.

[39] RIAA v. the People: Five Years Later report, EFF, available at <http://www.eff.org/wp/riaa-v-people-years-later>.

[40] *See* United States v. Rumely, 345 U.S. 41, 57 (1953) (Douglas, J., concurring), available at <http://supreme.justia.com/us/345/41/>.

Court decisions in the United States have supported the right to read anonymously on the Internet by denying enforcement of subpoenas that would have compelled a publisher to disclose the identities of subscribers to their materials.[41] Moreover, academics have made clear that "the close interdependence between receipt and expression of information and between reading and freedom of thought make recognition of such a right [the right to read anonymously] sound constitutional policy".[42]

IV. The Budapest Cybercrime Convention

The Council of Europe (CoE) Convention on Cybercrime has been open for signatures since 2001, and entered into force in 2004.[43] In recent years the CoE has prioritized ratification by non-European countries, and has provided extensive technical assistance to countries all over the world that are implementing its provisions in their national law. Even for countries that have not chosen to ratify it, the Convention has become a "guideline" for countries interested in developing national legislation against the perceived increased threats of cybercrime.

EFF remains concerned about the potential impact of the Convention, and overbroad national implementations of it, on citizens' fundamental rights.[44] We have several concerns.

First, the Convention requires parties to create offenses that are drafted with vague and obscure language that could be interpreted as penalizing legitimate expression and activities online. For instance, the Convention provides a narrow exception for "the authorized testing or protection of a computer system." Sometimes computer security researchers will test security without authorization. For example, testing the security of e-voting machines,[45] or ATM machines,[46] among others. These security tests can

---

41 Lubin v. Agora, Inc., 389 Md. 1, 22, 882 A.2d 833, 846 (2005), available at <http://caselaw.findlaw.com/md-court-of-appeals/1237646.html>.

42 Julie Cohen, A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace, 28 CONN. L. REV. 981 (1996).

43 Council of Europe, Cybercrime Convention 185, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

44 Danny O'Brien, The World's Worst Internet Laws Sneaking Through the Senate, EFF, available <http://www.eff.org/deeplinks/2006/08/worlds-worst-internet-laws-sneaking-through-senate>.

45 In this case, Indian security researcher Hari Prasad exposed serious flaws in the electronic voting machines used in India. See, Jim Tyre, Indian Government Detains E-Voting Researchers, available at <http://www.eff.org/deeplinks/2010/12/indian-government-detains-e-voting-researchers>. See also, Marcia Hofmann, Security Researcher Arrested for Refusing to Disclose Anonymous Source, available at

provide crucial information about the security of critical infrastructure even when the companies behind the products have little incentive to publicize security flaws, and should be allowed. The Convention also requires signatory countries to penalize copyright infringement that is done wilfully and on a commercial scale with the use of a computer system. While copyright holders have the exclusive right to reproduce works for a limited time period, many countries have fair use or fair dealing provisions in their national copyright laws, which act as a limitation on copyright holders' exclusive rights. Imposing criminal sanctions for copyright infringement may chill users from making fair uses, especially where the use cannot be determined a fair use a priori. Even a use which is 95% likely to be found fair may be detered, when the creator is looking at a one in twenty chance of jail time. In some countries, the impact of implementing the Cybercrime Convention could be even more damaging where existing exceptions and limitations in national law are outdated for the digital age, overly narrow, or non-existent. This threatens to further unbalance copyright law.

Second, the Convention does not contain a dual dual-criminality requierement. As a result, a signatory government (A) could be required to help enforce other countries' "cybercrime" laws - even if the act being prosecuted is not illegal in country A. Without more procedure protections, this could well lead to a "race to the bottom". Country B with weaker freedom of expression protections might ask law enforcement agencies in Country A to uncover the identities of anonymous critics, monitor their communications on behalf of foreign governments, or force ISPs of country A to obey other jurisdiction's requests to log their users' behavior without due process or compensation.[47]

Third, the Convention also grants broad surveillance powers to law enforcement authorities and requires ISPs to cooperate with them in the preservation, production, search, and seizure of stored computer data, real-time collection of traffic data, and interception of content data. However, the Convention does not provide any meaningful countervailing civil rights protections to ensure that minimum standards and legal safeguards consistent with international human rights accords are actually implemented in national transpositions.

4.1 Increased Powers of Electronic Interception

Many countries around the world have enacted legal regimes that force communications carriers to provide wiretapping assistance to law enforcement and intelligence agencies

---

<http://www.eff.org/deeplinks/2010/08/security-researcher-arrested-refusing-disclose>.

[46] For example, security researcher Barnaby Jack showed a security flaw in two kinds of ATM machines. See, Kim Zetter, Researcher demonstrates ATM "jackpotting" at Black Hat Conference, 2010, available at <http://arstechnica.com/security/news/2010/07/researcher-demonstrates-atm-jackpotting-at-black-hat-conference.ars>.

[47] *Supra* note 42.

via automated systems.[48] At the international level, the requirements for such regimes are established in the CoE Convention on Cybercrime, discussed above. In Europe, the European Council Resolution on Lawful Interception of Telecommunication establishes more specific requirements.[49] In the United States, the Communications Assistance for Law Enforcement Act of 1994 (CALEA) forced telephone companies operating in the U.S. to redesign their network architectures to make wiretapping easier.[50] CALEA expressly excluded interception of data traveling over the Internet, but subsequent regulatory interpretations substantially eroded that exclusion. More recently, CALEA has been interpreted to apply to Internet broadband providers and certain Voice-over-IP providers. Many countries have since passed similar laws.[51] On January 2014, Senator Leahy, chairman of the Senate Judiciary Committee, unveiled an ambitious plan to revised CALEA.[52]

Mandating back doors for lawful interception weakens network security and could just as easily be exploited by criminals seeking to take advantage of these vulnerabilities.[53] These loopholes have been abused and harmed communications security in ways unrelated to lawful interception.[54] For example, in 2005, hackers broke into a Greek telephone network and subverted its built-in wiretapping features to intercept the

---

[48] ITU Technology Watch Report # 6, ITU Technical Aspects of Lawful Interception, (May 2006), available at <http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf>; Council of Europe guidelines on ISP cooperation with Law Enforcement, available at <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/default_EN.asp>.

[49] *See also*, European Council Resolution on Lawful Interception of Telecommunications, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML>.

[50] *See* CALEA: The Perils of Wiretapping the Internet, EFF, <https://www.eff.org/issues/calea>.

[51] *Id*.

[52] Senator Patrick Leahy, An Agenda For The Senate Judiciary Committee In The 112th Congress, Main Justice, January 14, 2011, available at <http://www.mainjustice.com/2011/01/11/leahy-an-agenda-for-the-senate-judiciary-committee-in-the-112th-congress/>.

[53] Steven Bellovin, Matt Blaze, et al, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, June 13, 2006, available at <http://www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf>. See also Susan Landau, Surveillance or Security? The Risks Posed by New Wiretapping Technologies, The MIT Press, February 2011, available at <http://mitpress.mit.edu/catalog/item/default.asp?ttype=2&tid=12455>.

[54] Seth Schoen, Government Seeks Back Door Into All Our Communications, EFF, September 27, 2010, available at <https://www.eff.org/deeplinks/2010/09/government-seeks>.

communications of high-ranking Greek government officials, including the Prime Minister.[55] Some governments have attempted to justify spying on their own citizens by pointing to the United States' CALEA law.[56] In 2010, the Indian government threatened to close BlackBerry services unless it gains access to them by January 31, 2011. On January 13, 2011, Research in Motion said that it had given access to Indian wireless carriers to address lawful access requirements.[57]

In the U.S., government agencies are now proposing to expand the reach of "lawful intercept," as well as to seek more control over the use of encryption.[58] Such expansion would harm privacy, freedom of expression, and innovation.[59]

4.2 Lowering Privacy Protections and Oversight Mechanisms for the Protection of Transactional Data *vis-à-vis* the Government

Our digital lives generate a vast amount of transactional data which can reveal significantly more sensitive information than telephone transactional records and in some cases may directly or indirectly reveal the contents of our Internet communications. Therefore, the traditional distinctions in legal protection standards between communications content and non-content is far less useful or protective in the online context, and such distinctions should be viewed with skepticism.

The fact that Internet communications leave more detailed traces should not entail less privacy protection vis-à-vis the government. Transactional data should not have lesser protection based on technical details about how the data is stored, processed, or transmitted.[60] Moreover, the increased collection by telecommunications providers of transactional information of all individuals in a given country can be used by the

---

[55] Greek telephone tapping case 2004-2005, Wikimedia, available at <https://secure.wikimedia.org/wikipedia/en/wiki/Greek_telephone_tapping_case_2004-2005>. *See also* Vassilis Prevelakis and Diomidis Spinellis, The Athens Affair, available at <http://www.offnews.info/downloads/athensAffaire.pdf>.

[56] Seth Schoen, BlackBerry Bans Suggest a Scary Precedent: Crypto Wars Again?, EFF, August, 4, 2010, <https://www.eff.org/deeplinks/2010/08/blackberry-bans-suggest-scary-precedent>. See also "RIM Offers Interception Solution Using Cloud Computing, January 4, 2011, available at <http://economictimes.indiatimes.com/tech/hardware/rim-offers-interception-solution-using-cloud-computing/articleshow/7214591.cms>.

[57] Reuters, BlackBerry-Maker Proposes India Solution, New York Times, January 13, available at <https://www.nytimes.com/reuters/2011/01/13/business/global/news-us-blackberry-india.html>.

[58] *Supra* note 51

[59] EFF, The Perils of Wiretapping the Internet, September, 2010, available at <https://www.eff.org/issues/calea>.

[60] EFF, EFC, Comments on Lawful Access Consultation, Canada, 2002, available at <http:// w2.eff.org/Privacy/Foreign_and.../20021219-EFC-EFF-comments.pdf>.

authorities to compose a telling profile of the individual's concerns, interests, and associations. For example, a detailed review of transactional records could disclose journalists' sources.

The Explanatory Report on the Convention on Cybercrime acknowledged that: "The collection of [transactional] data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures."[61] However, the text of the Convention did not provide any legal safeguards in this regard. Leaving this to the discretion of countries that are implementing the Convention creates too great a risk of inadequate and divergent approaches to protection for citizens' rights.

Some court rulings have recognized the need to protect transactional data. In *Copland v. UK*, the European Court of Human Rights found that, "The collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8 of the [European] Convention [on Human Rights]."[62]

Location data, the digital records of people's movements, is an important category of transactional data that requires content-like protection. People need to be certain that their location will not be recorded for later use.[63] Governments must procure a court order based on probable cause before secretly tracking people's movement. In the United States, there is a growing consensus in many states and circuit cases in this regard.[64] In 2010, a U.S. Circuit Court of Appeals recognized that the U.S. Constitution might protect the privacy of cell phone location data stored by mobile phone providers even though such records do not reveal the content of communication.[65]

Legal protections for any kind of data are merely legal and therefore depend on government compliance with the law. The U.S. experience demonstrates that we cannot

---

[61] Council of Europe Convention on Cybercrime (ETS no: 185), opened for signature on November 8, 2001.

[62] Copland v. the United Kingdom, (2007) 45 EHRR 37, [2007] ECHR 253, paragraph 43, available at <http://www.bailii.org/eu/cases/ECHR/2007/253.html>.

[63] Peter Eckersley, On Locational Privacy, and How to Avoid Losing it Forever, EFF, available at <https://www.eff.org/wp/locational-privacy>.

[64] Kevin Bankston, Location, Location, Location: Three Recent Court Controversies on Cell Phone & GPS Tracking (and a Congressional Hearing, Too), EFF, available at <https://www.eff.org/deeplinks/2010/11/location-location-location-three-recent-court>.

[65] In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government --- F.3d ----, 2010 WL 3465170, 51 Communications Reg. (P&F) 415 (3rd Cir. (Pa.) September 7, 2010, (NO. 08-4227).

assume that governments will do so. In the past several years, there have been many reports of the U.S. government failing to obey the law, ranging from the National Security Agency's warrantless wiretapping program[66] to the unlawful use of national security letters to obtain transactional data.[67] EFF's litigation and Freedom of Information Act work has helped uncover some of this wrongdoing,[68] which points to yet another problem: government surveillance, especially in the electronic age, is essentially unaccountable, meaning that government abuse of power is often difficult to see and even harder to keep in check.

Recently, Wikileaks, the whistleblower website that hosts a number of leaked U.S. diplomatic cables, has highlighted how interception communication technology might be easily abused, and how foreign governments have been pressured to adopt surveillance programs beyond its original purpose.[69] The cables document how the Paraguayan government was seeking cooperation with the U.S. Government to expand its capacity to spy on cell phone calls to confront the threat by the leftist rebels, the Paraguayan People's Army. The leaked US diplomatic cable revealed that the U.S. Drug Enforcement Agency (DEA) has had an active spy on cell phone program for counter-narcotics efforts since 2009. However, the Paraguayan government apparently requested the US Ambassador to provide access to the software used by the U.S. Drug Enforcement Agency to perform eavesdropping for other purposes.

> "*The Ministry procured Brazilian intercept equipment for USD 1.2 million but needed access to the software available via the DEA … in order to make it operational. The Minister further said that he now understood that the technology did not permit both programs to operate independently*." [70]

The document also highlights how the US diplomats warned about the possibility that this surveillance technologies could be misused for inappropriate purposes and political gain.

---

[66] EFF, NSA Spying, available at <www.eff.org/files/filenode/att/section1006summary101608.pdf>.

[67] Kurt Opsahl, Report Confirms FBI Misuse of Authority to Obtain Phone Records, January, 2010, available at <https://www.eff.org/deeplinks/2010/01/report-confirms-fbi-misuse-authority>.

[68] Kurt Opsahl, FBI General Counsel Questioned on EFF NSL Report, April 15, 2008, available at <http://www.eff.org/deeplinks/2008/04/fbi-general-counsel-questioned-eff-nsl-report>.

[69] Pedro Servin, WikiLeaks: Paraguay Govt Sought DEA Spying Help, December 23, 2010, available at <http://articles.sfgate.com/2010-12-23/world/25547950_1_president-fernando-lugo-dea-intercept>.

[70] 10ASUNCION97, GOP Seeks To Implement New Cell Phone Intercept System, Wikileaks, available at <http://wikileaks.ch/cable/2010/02/10ASUNCION97.html>.

> *"The Ambassador made clear that the U.S. had no interest in involving itself in the intercept program if the potential existed for it to be abused for political gain, but confirmed U.S. interest in cooperating on an intercept program with safeguards, as long as it included counternarcotics. While noting that the Interior Ministry's current personnel are trustworthy, the Ambassador noted that others could abuse this technology in the future*." [71]

The Embassy repeatedly denied the Paraguayan government requests for unrestricted access to its surveillance software. However, the Embassy believed that it could not refuse to cooperate indefinitely without jeopardizing DEA's broader agenda.

> *"Our participation and concurrence is key to our counternarcotics-- and broader law enforcement-- goals in Paraguay. If we are not supportive, the GOP will view us as an obstacle to a key priority, which could jeopardize our broader relationship and the DEA's ability to pursue counternarcotics leads."*[72]

The cables highlight how easily surveillance technologies can be misused for secondary purposes without public accountability and oversight,

4.3 Budapest PLUS: the Enactment of Mandatory Data Retention Regimes

Law enforcement agencies throughout the world are pushing for invasive legal frameworks that force ISPs and telecom providers to collect and store citizens' Internet and telecom traffic data. The obligation to log users' Internet use is usually paired with provisions that allow the government to obtain those records, ultimately expanding the governments' ability to surveil its citizens. These types of provisions go well beyond the Data Preservation measures established in the Cybercrime Convention, which is often referred to as the Budapest Treaty.

The EU Data Retention Directive, adopted by the European Union in 2006, is the most prominent example of a mandatory data retention framework.[73] The highly controversial Directive compels all ISPs and telecommunications service providers operating in Europe to retain a subscriber's incoming and outgoing phone numbers, IP addresses,

---

[71] *Id.*
[72] *Id*.
[73] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>.

location data, and other key telecom and Internet traffic data for a period of at least 6 months, up to 2 years, for all European citizens, including those not suspected or convicted of any crime.[74]

Since its passage, the Data Retention Directive has faced intense criticism and now has an uncertain future in the EU.[75] The constitutional courts of Germany[76] and Romania ruled that their respective national data retention laws are in violation of their constitutions;[77] the Irish [High] Court has allowed a challenge to the Irish data retention law to be referred to the European Court of Justice,[78] Austria,[79] Belgium,[80] Greece,[81] Luxembourg,[82] and Sweden[83] have not yet transposed the Directive into national law. The European Commission has decided to take a few countries (most notably Sweden[84] and Austria[85]) to the European Court of Justice for failing to implement the Directive.

---

[74] Danny O'Brien, Freedom Not Fear: Europe's Growing Protest Against Net Surveillance, May 30,2008, available at <http://www.eff.org/deeplinks/2008/05/freedom-not-fear>. See also, Eddan Katz, The Beginning of the End of Data Retention, March 10, 2010, available at <https://www.eff.org/deeplinks/2010/03/beginning-end-data-retention>.

[75] EDRI, End of 5 Year Struggle Against Data Retention, January, 2006, available at <http://www.edri.org/campaigns/dataretention>.

[76] Leitsätze, zum Urteil des Ersten Senats vom 2, March 2010, available at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html> (German) translated in English <http://www.bundesverfassungsgericht.de/en/index.html>.

[77] The European Convention on Human Rights, November 4, 1950, available at <http://www.hri.org/docs/ECHR50.html>.

[78] Irish Court allows Data Retention Law to be challenged in ECJ, May 19, 2010, available at <http://www.edri.org/edrigram/number8.10/data-retention-ireland-ecj>.

[79] Christof Tschohl, Austria: BIM delivers draft act on implementing Data Retention Directive, Dec 2, 2010, available at <http://www.edri.org/edrigram/number7.23/austria-data-retention-law>.

[80] Maartje De Schutter - Liga voor Mensenrechten, Update on the Belgian transposition of the Data Retention Directive, February 10, 2010, available at <http://www.edri.org/edrigram/number8.3/belgium-data-retention-draft-law>.

[81] Greece: Overview of national data retention policies, AKVorrat, available at <http://wiki.vorratsdatenspeicherung.de/Transposition#Greece>.

[82] Luxemburg: Overview of national data retention policies, AKVorrat available at <http://wiki.vorratsdatenspeicherung.de/Transposition#Luxemburg>

[83] EDRI, Sweden obliged by EU to implement data retention directive, July 15, 2009, <http://www.edri.org/edri-gram/number7.14/sweden-data-retention>

[84] *Id.*

[85] *Supra* note 75

Meanwhile, in the countries where data retention has been implemented, European privacy officials have discovered damning evidence of excessive tracking and illegal over-collection by carriers and ISPs, and no empirical evidence that mandatory data retention has actually helped law enforcement.[86] Privacy officials across the European Union have made it clear that the mandatory data retention regime is disproportionate and makes surveillance that is authorized in exceptional circumstances the rule.[87] At the same time, national law enforcement agencies have shown little willingness to expend resources on the forensic analysis of the existing data in their control, which experts agree would be more fruitful than the wholesale retention of data of many innocent citizens.

European organizations, including many major civil society organizations, have criticized the Directive. Among others:

- The European Federation of Journalists has warned the European Union that data retention rules are a threat to press freedom and that anti-terrorism and policing measures should never compromise the core principle of journalism to protect the confidentiality of sources. The President of the European Federation of Journalists stated, "Any EU legislation must respect citizens' fundamental rights to freedom of expression which is guaranteed by International law."[88] And [t]he Directive … undermines this important principle which has been reaffirmed by the European Court of Human Rights as a cornerstone of press freedom."
- Pan-European digital rights group, the European Digital Rights Initiative (EDRI),[89] AK Vorrat,[90] EFF, and a coalition of civil society advocates are calling for the

[86] Katitza Rodriguez, EU Authorities: Implementation of Net Surveillance Directive Is Unlawful, EFF, July 15, 2010, <https://www.eff.org/deeplinks/2010/07/eu-authorities>.
[87] Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)] available at <http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm>.
[88] European Journalists Warn EU Home Affairs Chief that European Data Law Threatens Freedom, October 1, 2010, <http://europe.ifj.org/en/articles/european-journalists-warn-eu-home-affairs-chief-that-european-data-law-threatens-freedom>.
[89] European Digital Rights, available at <http://www.edri.org/>.
[90] German Working Group on Data Retention, available at <http://www.vorratsdatenspeicherung.de/component/option,com_frontpage/Itemid,1/lang,en/>

repeal of the Directive, and opposing blanket mandatory data retention proposals.

- In October 2010, the German Data Protection Commissioner Peter Schaar re-emphasized opposition to the data retention Directive and support for an alternative quick-freeze data preservation model.[91]

The United States government has led efforts demanding that other countries, in particular the European Union, limit individuals' privacy by calling for the retention of critical data for a reasonable period,[92] even though the United States has not implemented a general data retention regime.[93] The U.S. has instead adopted a targeted collection and expedited data preservation order regime.[94]

Mandatory data retention regimes threaten citizen's fundamental rights, including citizen's rights to communicate anonymously and privacy, as well as due process, and the presumption of innocence.

4.4 Mandatory Data retention Regimes in Australia and South America

In May 2009, the Argentinean Supreme Court re-affirmed that a controversial data retention law that amended the National Telecommunications Law of 2003 was unconstitutional. This law and its secondary regulation compelled all telecommunications companies and Internet Service Providers to record, index, and store traffic data for a 10-year period, in order to give information to the Argentinean Judicial Branch and the Attorney General's Office when required.[95]

Recently, Australian and Brazilian officials respectively announced that they are evaluating mandatory data retention regimes that compel communication providers to

---

[91] German Data Protection Commissioner Peter Schaar Video, available at <http://modultool.zdf.de/public/Pro_und_Contra_Vorratsdatenspeicherung/resources/101008_schaar4_onl_h.flv> (in German only).

[92] "Revise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period." United States Mission to the European Union, Proposals for US-EU counter-terrorism cooperation, October 16, 2001, available at <http://www.statewatch.org/news/2001/nov/06Ausalet.htm>.

[93] Declan McCullagh, FBI, politicos renew push for ISP data retention laws, April 23, 2008, available at <http://news.cnet.com/8301-13578_3-9926803-38.html>.

[94] Title 18 U.S.C. § 2703 (f), November 8, 2010, available at <http://www.law.cornell.edu/uscode/18/usc_sec_18_00002703----000-.html>.

[95] Pablo Palazzi, La Corte Suprema confirma la inconstitucionalidad de la ley de datos de tráfico, February 24, 2009, available at <http://www.habeasdata.org/fallo-corte-datos-de-trafico?PHPSESSID=e7597c3532300a2c91d560f00227ddb8>.

collect and store citizens' Internet and telecom traffic data for a certain period of time for possible use by law enforcement agencies. Each country's mandatory data retention regimes would require the collection of different sets of traffic data.

In Brazil, a controversial bill introduced by Congressman Azeredo, which was buried in 2009 and revived in 2010, would create new criminal offenses that would affect Brazilian Internet users.[96] The Brazilian Committee on Constitution and Justice from the Federal Chamber of Deputies brought back the bill into the Brazilian agenda at the end of 2010.[97] The bill threatens restricts freedom of expression rights, and creates vaguely worded and overbroad offenses subject to different interpretations, which is likely to harm legitimate expression.[98] For example, consumers who modify their cell phones can be sued for their non-infringing or fair use activities.[99] Internet Service providers are required to report suspicious behaviors of users. They are also obliged to keep, under penalty of fine, connection logs for 3 years of all innocent Brazilians. This provision will threaten the anonymity of online speakers, privacy, and due process. Moreover, the bill extends such obligations to providers of all kinds of Internet services, which can include bloggers, news portals, among others.[100]

Brazilian have strongly protested against that bill.[101] As a response to the Brazilian uproar, the Ministry of Justice in partnership with the Fundação Getulio Vargas Law

---

[96] Brazilian Cybercrime Bill, available at <ttp://www.nardol.org/assets/2008/7/18/azeredo-law.en.txt>.

[97] Joana Varon, Brazilian Internet Regulation: New Challenges Imposed by Misguided Cybercrime draft bill, [Centro de Tecnologia e Sociedade apresenta estudo sobre o texto substitutivo do PL Azeredo], November 2010, available at <http://www.a2kbrasil.org.br/wordpress/lang/pt-br/2010/11/centro-de-tecnologia-e-sociedade-apresenta-estudo-sobre-o-texto-substitutivo-do-pl-azeredo/>, [Portugues] <http://www.a2kbrasil.org.br/wordpress/lang/pt-br/2010/11/brazilian-internet-regulation-new-challenges-imposed-by-misguided-cybercrime-draft-bill/?> [English].

[98] Marcel Leonardi, President Lula and the Brazilian Cybercrime Bill, July 17, 2009, EFF, available at <https://www.eff.org/deeplinks/2009/07/lula-and-cybercrime>. See also, David Sasaki, Internet Censorship and Freedom of Expression in Latin America, November 1, 2010, available at <http://informacioncivica.info/mexico/internet-censorship-and-freedom-of-expression-in-latin-america/>.

[99] Fundacão Getulio Vargas Centro de Tecnologia e Sociedade, Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrô nicos (PL n. 84/99) apresentado pela Comissão de Constituiç ão e Justiç a e de Cidadania, available at <http://www.a2kbrasil.org.br/wordpress/wp-content/uploads/2010/11/coment%C3%A1rios-ao-substitutivo-PL-88-99.pdf>.

[100] *Id.*

[101] *Supra* note 94.

School launched an innovative process to build an Internet Civil Framework (*Marco Civil*). By using the Internet as a platform for discussions, from blogs to Twitter, Internet users, academia, business sector representatives, law enforcement agencies, and government representatives have held an open consultation to draft the above-mentioned proposal that foster citizen's fundamental rights and foster innovation.

Unfortunately, a mandatory data retention provision has been included in the Draft Proposal framework.[102] It would create an obligation to keep records of the connection logs (specifically, the date, start time and end time of an Internet connection, duration and IP numbers used by the terminal for receiving data packets) of all Brazilian Internet users, even those not suspected or convicted of any crime, for a term of up to six months. For the reasons explained above, that proposal would threaten anonymity, privacy and freedom of expression rights, as well as the presumption of innocence, since it is unreasonable to require the registration of the connection logs of all Brazilian users, compromising their privacy for crimes that might be committed by only a few users.[103]

In Australia, a few months ago, ZDNet Australia reported that the Australian Attorney General's Office "has been holding confidential discussions with internet service providers about the possibility of recording details of all Australian Internet usage for later potential use by law enforcement agencies, and to extend the retention obligations to search engines.[104] The Australian Government has denied those claims,[105] and has stated that Australia is considering following the EU's Data Retention Directive as a model.[106]

These blanket surveillance regimes of transactional data and/or search log data

---

[102] Draft Bill Proposition for Collaborative Debate, available at <http://direitorio.fgv.br/sites/direitorio.fgv.br/files/DraftBillProposition.doc.>

[103] Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da Universidade de São Paulo, available at <http://culturadigital.br/marcocivil/2010/05/31/contribuicao-do-gpopai-para-o-marco-civil-da-internet/>.

[104] Ben Grubb, Government wants ISPs to record browsing history, June 11, 2010, available at <http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm?omnRef=NULL>.

[105] Renai LeMay, Govt denies it wants web history records, June 14, 2010, available at <http://www.zdnet.com.au/govt-denies-it-wants-web-history-records-339303834.htm>.

[106] Stilgherrian, Is Australia's data retention idea that scary?, July 5, 2010, available at <http://www.zdnet.com.au/is-australia-s-data-retention-idea-that-scary-339304290.htm>. See also Katitza Rodriguez, EU Search Engine Snooping Mandate Sneaked Into Child Protection Declaration, available at <http://www.eff.org/deeplinks/2010/06/eu-search-engine-snooping-mandate-sneaked-child>.

undermine other important public policy objectives, such as efforts to combat crime or protect children online. Any data retention measures adopted in national laws must be proportionate and necessary in a democratic society, and should not undermine the protection of other human rights such as the rights of freedom of expression and privacy.

V. Emerging issues: Lowering Legal Safeguards against Government Access to Citizens' Data hosted by Third Parties Providers, especially Cloud Computing Providers

Cloud computing has interesting implications and potential for both developed and developing countries. Because individuals and governments are relying more and more on those services, information that was previously stored in your hard drive, in a file in your office or at your home, is now being hosted by third party providers.

From an individual perspective, the cloud provider itself poses the most obvious potential privacy threat, since it holds the data we care about. Additional threats are posed to personal data by subpoenas issued to the cloud provider, unauthorized access from cloud employees, civil litigants' access to data, computer hackers, and compelled disclosure of cloud data to law enforcement and national security investigators. In the cloud, many individuals' data may be seized or searched even if only one or a few persons' data is actually targeted because data may be stored collectively with a single cloud provider or on a single cloud storage device.

In regard to government access to cloud data, we wish to highlight the efforts of the U.S. Digital Due Process coalition, comprising public interest groups and U.S. technology companies, to strengthen the due process requirements that should apply in these situations.[107] The coalition is working to simplify, clarify, and unify the U.S. privacy standards, by proposing stronger privacy protections for communications and associated data in response to changes in technology. For example, the coalition has recommended that the law should require the government to obtain a probable cause-based search warrant from a judge before it may compel the disclosure of any type of communications content stored by a third party provider, and before tracking the location of a mobile device or obtaining records of such a device's past location.

EFF believes that there is a need to identify best practices that have been adopted by cloud providers where civil subpoenas or court orders are served upon them for others' data that is stored with them. For instance, cloud computing providers should notify the owner of the data that it has received a subpoena or court order, and provide an opportunity for the owner to respond and file a judicial challenge to the disclosure of data held by the cloud provider.

---

[107] See Digital Due Process Coalition website, available at <http://www.digitaldueprocess.org/

In February 2008, the German Constitutional Court ruled provided important safeguards against secret online searches of peoples' hard drives.[108] The court limited the use of those techniques for cases where there are evidence of a concrete danger for the life, body and freedom of a person, or for the foundation of the state, and in specific cases.[109] Moreover, the court ruled that those measures can be used only by law enforcements agencies after a judge's approval.[110] The ruling also created a basic right to the confidentiality and integrity of information-technological systems.[111] The Court granted that information technology systems, including laptops and mobile phones, can contain vast amount of personal information so access to the system makes it possible to get an insight of the conduct of life of a person or a meaningful picture of the personality.[112]

VI. Corporate Social Responsibility

We respectfully recommend that the annual report of the UN Special Rapporteur on Freedom of Expression address the role that corporations should play in the protection of citizens' privacy, freedom of expression and fundamental human rights.

Most of people's communication and interactions online are on websites and networks that are privately owned and operated. Omitting the role of corporations corporations, even beyond the obligations of law, would fall short of meaningful protection for individuals rights online. Corporate social responsibility is a crucial part of developing international human rights norms, especially at a time when government action on the Internet is increasingly more indirect and may fall outside of limitations on government power.

EFF believes that the selling of customized surveillance technologies to authoritarian regimes in situations where companies know, or should know, that governments may use those technologies to target people for arrest, torture, and enforced disappearance is in violation of international human rights standards, and deserves close scrutiny.[113]

---

[108] German Federal Constitutional Court Decision, available at <http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html> [German]. A non official translation can be found at <http://www.bverfg.de/en/decisions/rs20080227_1bvr037007en.html>.

[109] Annika Kremer, Ralf Bendrath, Germany Privacy In Germany 2008: A New Fundamental Right, A Privacy Mass Movement, And The Usual Surveillance Suspects, 28 January 2008, available at <http://www.edri.org/edri-gram/number7.2/germany-2008-surveillance-fundamental-right>.

[110] *Id*.

[111] Ralf Bendrath, Germany: New Basic Right To Privacy Of Computer Systems, February 27, 2008, available at <http://www.edri.org/edrigram/number6.4/germany-constitutional-searches>.

[112] *Id.*

[113] Danny O'Brien, Seven "Corporations of Interest" in Selling Surveillance Tools to

It is the combination of the technologies' capabilities and the knowledge about its use and/or misused that is dispositive. Corporations that sell technologies that could be used to violate human rights should undertake thorough and independent human rights impact assessments before engaging with authoritarian regimes.[114]

Conclusion

We respectfully recommend that the UN Special Rapporteur on Freedom of Expression takes appropriate action to increase the protection of privacy in the online environment in order to secure citizens' ability to meaningfully engage in freedom of expression.

In particular, we recommend that the Special Rapporteur's report:

- Recognize that the privacy of communications and freedom of expression includes the right of every individual to use encryption technology, to publish encryption technologies and research;
- Recommend that Internet intermediaries should not block the transmission of encrypted communication;
- Recommend that Internet service providers be encouraged to design systems for end-to-end privacy;
- Recognize that every individual has the right to freedom of expression, which includes the right to speak, read and communicate anonymously.
- Recognize the particular threats that overbroad national implementations of the Cybercrime Convention pose to citizens' rights of freedom of expression and privacy.
- Recommend that countries' laws should not forbid citizens from using technologies to seek and impart information anonymously and securely, including circumvention tools, encryption and anonymity technologies;
- Recommend that Internet service providers and Internet intermediaries should only be required to remove content from websites, blogs, social media, or other platforms, terminate Internet users' accounts, or disclose the identity or personal information about Internet users to private parties upon receipt of a court order, after a process of judicial review, consistent with the statutory and constitutional protections afforded to those users.
- Recognize that data retention data retention rules are a threat to privacy, freedom of expression and press freedom. Policy measures should not affect the protection of the confidentiality of journalism sources.

China, EFF, February 1, 2010, available at <https://www.eff.org/deeplinks/2010/01/selling-china-surveillance>.

[114] Eddan Katz, Holding Nokia Responsible for Surveilling Dissidents in Iran, EFF, October 13, 2010, available at <https://www.eff.org/deeplinks/2010/10/saharkhiz-v-nokia>.

- Address the role that corporations should play in the protection of citizens' privacy, freedom of expression and fundamental human rights, with special attention to recent reported instances of corporations selling customized surveillance technologies to authoritarian regimes in situations where they know, or should know, that these technologies will be used to target people for arrest, torture, and forced disappearance.