



# Anonymity and Encryption

*Comments submitted to the United Nations Special Rapporteur on  
the Promotion and Protection of the Right to Freedom of Opinion  
and Expression*

February 10, 2015

*Contact:*

*Katitza Rodriguez, EFF International Rights Director  
katitza@eff.org*

Thank you for providing the Electronic Frontier Foundation (EFF) with the opportunity to add our submission to the consultation on the use of encryption and anonymity in digital communications. EFF is an international civil society non-governmental organization with more than 26,000 donors worldwide, dedicated to the protection of individuals' fundamental freedoms online. EFF engages in strategic litigation in the United States and works in a range of international and national policy venues to protect civil liberties, foster innovation, and empower consumers. EFF is located in San Francisco, California and has members in 90 countries throughout the world.

# Contents

## [I. Anonymity](#)

[What is Anonymity?](#)

[Who Needs Anonymity?](#)

[Anonymity and Society](#)

[Anonymity and International Human Rights Standards](#)

[Freedom of Expression](#)

[The Right to Seek and Receive Information](#)

[Press Freedom and the Protection of Sources](#)

[Privacy and Freedom of Expression](#)

[An Anonymity Strong Enough for Human Rights](#)

[Issues in Digital Anonymity](#)

[Anonymity is Necessary for Digital Privacy](#)

[Weak Anonymity May Be Easy, But Strong Anonymity is Not](#)

[Piercing the Veil: Identity Disclosure and the Role of Intermediaries](#)

[Anonymity Policies of Non-Governmental Actors](#)

[The Regulation of Anonymity](#)

[Positive Policies for the Protection of Anonymity](#)

[United States](#)

[Canada](#)

[South Korea](#)

[Mexico](#)

[Policies that Undermine the Right to Anonymity](#)

[South Korea](#)

[Brazil](#)

[Vietnam](#)

[Russia](#)

[Europe](#)

[United States](#)

[Mass Copyright Litigation](#)

[Mass Surveillance](#)

## [II. Encryption](#)

[Encryption and Free Expression](#)

[The Use of Encryption in Digital Communications](#)

[Encryption and the State](#)

[Defending the Right to Encrypt](#)

## [III. Conclusion](#)

# I. Anonymity

## What is Anonymity?

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, or as acting or communicating in a way that protects the determination of one's name or identity, or using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.<sup>1</sup>

Anonymity can be seen as existing on a spectrum, from strong to weak. Anonymity is strong when there are technical and legal protections that make it very difficult to unmask the identity of an anonymous person. Anonymity is weak when an anonymous person can be unmasked through easy means, such as a government request to a service provider or looking the assumed name up in an existing database.

We can assess the degree of anonymity that people can achieve online by considering questions such as: Can people refrain from signing what they write? Can they choose how to sign (or not to sign) their communications? Can they access services without registering, or without registering with their legal identity? Do service providers require an account to be linked to a government-issued identity document, or to other systems that are linked to legal identity, such as payment systems? Do service providers retain data, such as logs, that could be used to identify their users in the future? Do users have access to technical

---

<sup>1</sup> Some sources distinguish between *anonymity* (taking no name at all) and *pseudonymity* (using an assumed name), but for the purposes of this submission we do not draw this distinction. In practice, digital pseudonyms require strong or weak anonymity as part of the process of separating the assumed name from the details of the person's identity.

means to conceal their identity, such as privacy-enhancing technologies that make it hard to identify them? Do users have confidence that their identity will not be associated with their activities against their will? In order to strip an individual of the anonymity they choose, what effort must be taken by other parties? Can third parties determine an individual's identity without recourse to the courts, or must a legal process be pursued?

### **Who Needs Anonymity?**

Everyone who does not want the things they say to be connected to their permanent identity has an interest in anonymity. They may be concerned about political or economic retribution, harassment, or even threats to their lives, or they may use anonymity as part of their personal expression or self-development. Some need to cloak their identity from the casual investigation of their colleagues. Others need stronger protections against more determined and well-funded adversaries. Some will need protection against their own governments.<sup>2</sup>

Parents try to create a safe way for children to explore online.<sup>3</sup> Teenagers exploring their own identity are often harassed online and in their own communities, and may choose online anonymity to protect themselves.<sup>4</sup>

As individuals mature, they may change their names over time as an expression of their religion, beliefs, or as part of the full development of their

---

<sup>2</sup> Electronic Frontier Foundation (2013). *Speech: anonymity*. Retrieved February 6, 2015, from [https://ilt.eff.org/index.php/Speech:\\_Anonymity](https://ilt.eff.org/index.php/Speech:_Anonymity).

<sup>3</sup> Patti M. Valkenburg et al. (2005). 'Adolescents' identity experiments on the Internet'. *New Media & Society*, vol. 7 no. 3 383-402. Retrieved February 6, 2015, from <http://nms.sagepub.com/content/7/3/383>

<sup>4</sup> Livescience (2010), *Cyberbullying Rampant for Lesbian and Gay Teens*. Retrieved February 6, 2015, from <http://www.livescience.com/6199-cyberbullying-rampant-lesbian-y-teens.html>

personality. They may seek to do this in order to avoid discrimination, or establish a name that is easier to pronounce or spell in a given culture.<sup>5</sup>

Others will have a need to rebuild their lives safe from former oppression. Survivors of domestic abuse who need protection from their abusers must ensure they do not leave a digital trace.<sup>6</sup> Individuals whose spouses or partners work for the government or are well-known may wish to conceal aspects of their own life, and often feel more comfortable using anonymity tools. Witness and victim protection programs need anonymity to operate safely.

Occupations that enable free expression use anonymity to protect their customers and clients. Librarians believe library patrons should have the right to read anonymously—an essential prerequisite for intellectual freedom and privacy.<sup>7</sup> Publishers have fought to preserve the anonymity of their customers on the grounds that being known as a reader of controversial works can create a chilling effect.<sup>8</sup>

Anonymity allows journalists' sources to come forward and speak without fear of retaliation; whistle-blowers report news that companies and governments

---

<sup>5</sup> On the cultural variety of naming conventions and the inability of computing systems to deal with them properly, see Patrick McKenzie (2010), *Falsehoods Programmers Believe About Names*, Kalzumeus. Retrieved February 8, 2015, from <http://www.kalzumeus.com/2010/06/17/falsehoods-programmers-believe-about-names>

<sup>6</sup> See Meghan Neal (2014). *Tor Is Being Used as a Safe Haven for Victims of Cyberstalking*, MotherBoard. Retrieved February 8, 2015, from <http://motherboard.vice.com/read/tor-is-being-used-as-a-safe-haven-for-victims-of-cyberstalking>

<sup>7</sup> The International Federation of Library Associations and Institutions (1999). *Statement on Libraries and Intellectual Freedom*. Retrieved February 6, 2015, from <http://www.ifla.org/publications/ifla-statement-on-libraries-and-intellectual-freedom>.

<sup>8</sup> For instance, in U.S. jurisprudence, in *Rumley*, 345 U.S. 41, a bookseller could not be convicted for refusing to provide a list of individuals to whom he had made bulk sales of political books for further distribution. For more examples, see *Privacy Authors and Publishers' Objection to Proposed Settlement*, *Authors Guild v. Google, Inc.*, No. 05-CV-8136-DC, Retrieved February 9, 2015, from [https://www.eff.org/files/filenode/authorsguild\\_v\\_google/file\\_stamped\\_brf.pdf](https://www.eff.org/files/filenode/authorsguild_v_google/file_stamped_brf.pdf).

would prefer to suppress.<sup>9</sup> Anonymity is also essential in the human rights context. Human rights workers use it in their struggle against human rights violations;<sup>10</sup> it functions as a shield for those who seek to challenge entrenched, centralized powers, or an intolerant majority.<sup>11</sup>

### **Anonymity and Society**

Anonymity is vital for an open and free society. We care about anonymity offline and online because it allows individuals to express unpopular opinions, honest observations, and otherwise unheard complaints. It allows them to avoid potential violent retaliation from those who they may offend, and it plays a central role in the fight to expose crimes and abuses of power.

We care about anonymity because we want a society where people can speak honestly. Anonymity allows voices to be heard, and ideas to be judged based on their substance, not their source. Anonymity can help protect a speaker from the logical fallacy of *ad hominem* attacks (responding to arguments by attacking a person's character, rather than the content of their arguments).

Our present society does not require us to show our identity cards or sign our names before we express ourselves. The values we have developed over many decades were built from the frank and wide-ranging debate that such freedom provides. Those values, including anonymity itself, should continue to be upheld in the digital age.

---

<sup>9</sup> For example, a number of environmental activists protesting the damage to the Amazon caused by Chevron's oil extraction activities go by pseudonyms out of fear of retaliation by the company. Retrieved February 6, 2015, from <https://www.eff.org/files/filenode/effmotionquash.pdf>.

<sup>10</sup> EFF has sued the Ethiopian government on behalf of an Ethiopian democracy activist living in the Washington DC area who is proceeding under the pseudonym "Kidane" out of concern for his and his family's safety. Retrieved February 6, 2015, from <http://phys.org/news66401288.html> or <https://www.eff.org/cases/kidane-v-ethionia>

<sup>11</sup> Prominent bloggers and environment activist Nguyen Van Hai blogged under the pen name "Dieu Cay." Authorities discovered his identity and imprisoned him from 2010 to 2014. Retrieved February 6, 2015, from <https://eff.org/civilrightsdefenders-anonymity>.

## **Anonymity and International Human Rights Standards**

The rights to freedom of expression and privacy were recognized by the Universal Declaration of Human Rights (“UDHR”) on December 10, 1948.<sup>12</sup> Since then, these rights have been affirmed by subsequent United Nations international human rights treaties as well as various regional treaties and other human rights instruments. While these more recent treaties and instruments adapted differing language than that employed by the UDHR in setting forth the right to privacy and the right to freedom of expression, a comparative analysis shows that a coherent consensus has emerged on the specific protections afforded to individuals as well as the obligations imposed on state parties.

### **Freedom of Expression**

Freedom of expression is bolstered when one can do so anonymously. There are many circumstances when a person will not speak because of a fear of retribution, an inherent power imbalance, or other reason, or an association of individuals will not speak unless it can be sure to protect the identity of its members. The Special Rapporteur on Free Expression of the Inter-American Commission on Human Rights (IACHR) made clear that “in all cases, users have the right to remain anonymous and any dispute on this point needs to be resolved exclusively in court.”<sup>13</sup>

### **The Right to Seek and Receive Information**

The ability to read and access information anonymously is also crucial for the exercise of free expression. Article 19 of the Universal Declaration of Human Rights, which enshrines the right to freedom of opinion and expression, includes

---

<sup>12</sup> UDHR. Art. 12 (privacy), Art. 19 (expression).

<sup>13</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*. Chapter IV (Freedom of Expression and the Internet). OEA /Serv.LV/II.149. December 31, 2013. Para. 109. Retrieved February 6, 2015, from [http://www.oas.org/en/iachr/expression/docs/reports/2014\\_04\\_22\\_%20IA\\_2013\\_ENG%20FINALweb.pdf](http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20FINALweb.pdf)

the right to seek, receive, and impart information and ideas through any media. This inclusion is necessary because there can be no meaningful protection for citizens' freedom of expression if individuals lack the right to read and communicate anonymously. 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."<sup>14</sup>

In other words, the right to seek and receive information is chilled when the government or others have unchecked access to records that document the viewing or reading habits of individuals:

"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."<sup>15</sup>

Even the existence of these records is sufficient for a chilling effect, especially given that many readers are not just afraid of government tracking of their reading habits, but also of discovery by family members or other close associates.

---

<sup>14</sup> Julie Cohen (1996). *A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace*, 28 CONN. L. REV. 981.

<sup>15</sup> See *United States v. Rumely*, 345 U.S. 41, 57 (1953) (Douglas, J., concurring). Retrieved February 6, 2015, from <http://supreme.justia.com/us/345/41>.



As the author Michael Chabon says “If there is no privacy of thought — which includes implicitly the right to read what one wants, without the approval, consent or knowledge of others — then there is no privacy, period.”<sup>16</sup>

### **Press Freedom and the Protection of Sources**

A well-established corollary to the right of free expression is the importance of a functional and free press. To that end, the basic principle that journalists have a right to protect their sources is well established in international law.<sup>17</sup> In particular, the IACHR made clear that:<sup>18</sup>

“A principal rationale underlying the right to confidentiality is that, in the scope of his or her work to supply the public with information necessary to satisfy the right to inform, the journalist is providing an important public service when he or she collects and disseminates information that would not be made known without protecting the confidentiality of the sources. Professional confidentiality consists of “observing discretion about the identity of the source to ensure the right to information; it has to do with granting legal guarantees to ensure anonymity and preventing possible reprisals that may result from having disclosed certain information.”<sup>19</sup>

Moreover, the IACHR have noted that the right to keep confidential their sources of information, notes, personal and professional archives, extend to every social communicator including journalists.”<sup>20</sup>

---

<sup>16</sup> EFF. *Google Book Search Settlement and Reader Privacy*. Retrieved February 6, 2015, from <https://www.eff.org/pages/google-book-search-s>

<sup>17</sup> It has been recognized by the European Parliament, the Committee of Ministers of the Council of Europe, and the Inter-American Commission on Human Rights.

<sup>18</sup> IACHR. *Background and Interpretation of the Declaration of Principles on Freedom of Expression*. Retrieved February 6, 2015, from <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=132>

<sup>19</sup> See Marc Carrillo (1993). *La clausura de conciencia y el secreto profesional de los periodistas*. Civitas y Centro de Investigación, Barcelona. p. 170.

<sup>20</sup> See also IACHR. *Principle 8 of the Declaration of Principles on Freedom of Expression*: “Every social communicator has the right to keep his/her source of information, notes, personal and professional archives confidential.” Retrieved February 6, 2015, from <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26&IID=1>

Sources such as government whistle-blowers need the strongest protections against exposure, even from actors wielding the full power of the state. In the age of the Internet, anyone can be such a source, and anyone can have the responsibility to protect sources, as they perform the role of a journalist or social communicator.

### **Privacy and Freedom of Expression**

The issue of anonymity online also necessarily incorporates concerns for both expression and privacy, and the careful analysis of the interaction between those two rights. As stated in the 2011 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, “The right to privacy is essential for individuals to express themselves freely.”<sup>21</sup>

Building upon that, the IACHR Special Rapporteur on Free Expression noted that in view of this close relationship between freedom of expression and privacy:

“Both the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions. Participation in public debate without revealing one’s identity is a normal practice in modern democracies. The protection of anonymous speech is conducive to the participation of individuals in public debate since—by not revealing their identity—they can avoid being subject to unfair retaliation for the exercise of a fundamental right. Indeed, those who exercise the right to freedom of thought and expression take part in public debate and the political life of a community. It does not solely entail writing opinion articles or participating in debate forums—it also involves the ability to call for social mobilizations, to call upon other citizens to protest, to organize politically, or to challenge the authorities even in risky situation.”<sup>22</sup>

---

<sup>21</sup> See, e.g., Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue (2011). Human Rights Council, U.N. Doc. A/HRC/17/27 pag 15;

<sup>22</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*. Chapter IV (Freedom of Expression and the Internet). OEA /Serv.LV/II.149. Para. 134. Retrieved February 6, 2015, from [http://www.oas.org/en/iachr/expression/docs/reports/2014\\_04\\_22\\_%20IA\\_2013\\_ENG%20FINALweb.pdf](http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20FINALweb.pdf)

The Council of Europe Committee of Ministers' Declaration on freedom of communication on the Internet has also noted,

“In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity.”<sup>23</sup>

As the IACHR Special Rapporteur on Free Expression explained, “both the right to freedom of thought and expression and the right to private life, protect anonymous speech from government restrictions.”<sup>24</sup> He further emphasized, “Participation in public debate without revealing one’s identity is a normal practice in modern democracies. The protection of anonymous speech is conducive to the participation of individuals in public debate since—by not revealing their identity—they can avoid being subject to unfair retaliation for the exercise of fundamental rights.”<sup>25</sup> The report continues, “those who exercise the right to freedom of thought and expression take part in public debate and the political life of a community. It does not solely entail writing opinion articles or participating in debate forums—it also involves the ability to call for social mobilizations, to call upon other citizens to protest, to organize politically, or to challenge the authorities even in risky situations.”<sup>26</sup>

---

<sup>23</sup> Council of Europe (2003). *Declaration on freedom of communication on the Internet* (Adopted by the Committee of Ministers at the 840th meeting of the Ministers' Deputies). Article 7 on Anonymity. Retrieved February 6, 2015, from <https://wcd.coe.int/ViewDoc.jsp?id=37031>

<sup>24</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter IV (Freedom of Expression and the Internet)*. OEA /Serv.LN/II.149. Para. 134.

<sup>25</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter IV (Freedom of Expression and the Internet)*. OEA /Serv.LN/II.149. Para. 134.

<sup>26</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter IV (Freedom of Expression and the Internet)*. OEA /Serv.LN/II.149. Para. 133.

## **An Anonymity Strong Enough for Human Rights**

The right to anonymity is grounded in these fundamental human rights. Anonymity is an essential precondition for the exercise of the rights to privacy and freedom of expression and should be guaranteed by the State.

Anonymity must not be restricted *a priori*. Compelled disclosure must only occur once a legally defined offense has been committed. The due process rights of a speaker should be respected before identifying that individual in response to a request to do so. Legal regimes must ensure rigorous consideration of the free expression and privacy rights of the speaker before compelling any identification.

In many of the core societal functions of anonymity, speakers are defending their identity from groups or individuals that may wield state or allied institutional powers. Therefore, strong anonymity, where records are not kept, and where privacy-protecting tools obscure the identity of an individual, should always be available.

## **Issues in Digital Anonymity**

### **Anonymity is Necessary for Digital Privacy**

Anonymity involves more than the shielding of one's name. Rather, it entails the ability to keep confidential a wide variety of one's online activities including location, frequency of communications, and myriad of other information. Online anonymity must be understood not only as the state of being *unidentified by* third-parties, but also as the quality of being *unknowable to* third-parties.

It is incomplete to conceptualize the right to anonymity online simply as the right to freely participate in any online activity without disclosing one's *name* to anyone. Indeed, the IACHR rapporteur explained that the protection to private

life involves at least two specific policies related to the exercise to freedom of thought and expression: “the protection of anonymous speech and the protection of personal data.”<sup>27</sup>

“Online anonymity” also includes a full range of data protection concerns, and the ability to be untraceable in a medium that as a structural default records, potentially down to the keystroke, everything a person does. Every online transaction, be it sending a simple email or viewing a popular website, may generate communications metadata, which is information associated with an online transaction other than the content of a message itself. For example, an email from Person A to Person B through a third-party email provider such as Google or Yahoo reveals that these people are in contact with one another, and contains further information related to where the Person A was when they sent the email, the time at that location when they sent the email, the software Person A used to compose the email, and frequently the subject line of the email.<sup>28</sup>

Similarly, if Person A visits a popular website like bing.com, the website will know the physical location of Person A, the time they visited, and if they have used the same device to visit the website before. In the process of visiting a website or sending an email, Person A has given this information to his or her Internet service provider, along with, potentially, a search engine, and numerous other third-parties which provide services that enable our daily use of the Internet.

Indeed, this understanding that a person’s right to privacy does not merely pertain to content of communications but also to the fact of the communication and information about the communication itself (i.e. point of origin, duration, recipient, etc.) is neither novel nor limited to online media.

---

<sup>27</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*. Chapter IV (Freedom of Expression and the Internet). OEA /Serv.LV/II.149. Para. 134.

<sup>28</sup> For a good explanation on this, <http://whatismyipaddress.com/email-header>. Retrieved February 6, 2015.

Moreover, even though the information contained in a single email, for example, may not identify the user, communications metadata can be aggregated to create detailed profiles of individuals that contain Person A's name, shopping habits, personal interests, religious affiliations, political inclinations, friends, colleagues, career, ambitions, and other intimate aspects of Person A's identity. Such aggregation is not only becoming more common as processing power and data storage become cheaper, but it has spawned an industry centered on this data aggregation, analysis, and resale.<sup>29</sup>

### **Weak Anonymity May Be Easy, But Strong Anonymity is Not**

The Internet easily facilitates *superficial* anonymity—such as the use of an email or commenter alias. In the 1990s, commentators often saw the use of online pseudonyms as a reason that Internet communications were highly anonymous; a much-circulated 1993 cartoon by Peter Steiner shows one computer-using canine telling another that “[o]n the Internet, nobody knows you’re a dog.”<sup>30</sup>

But truly preserving anonymity requires some effort. Vast amounts of information about online communications is routinely recorded. Because this information can be collected, disclosed and subpoenaed, any discussion of

---

<sup>29</sup> See *Escher et al. v. Brazil*, IACHR, ¶ 114 (“Article 11 [the right to privacy] applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation.”). See also: Background and Supporting International Legal Analysis of the International Principles on the Application of Human Rights to Communications Surveillance. Retrieved February 6, 2015, from <https://en.necessaryandproportionate.org/LegalAnalysis/protected-information>

<sup>30</sup> Wikipedia (2015). *On the Internet, Nobody Knows You're a Dog*. Retrieved February 6, 2015, from [https://en.wikipedia.org/wiki/On\\_the\\_Internet\\_nobody\\_knows\\_you%27re\\_a\\_dog](https://en.wikipedia.org/wiki/On_the_Internet_nobody_knows_you%27re_a_dog)

anonymity online must address what information is disclosed to whom and under what restrictions (if any).<sup>31</sup> Often, people (or dogs) who haven't deliberately revealed their legal identities in online communications have nonetheless revealed a wide range of identifying and potentially identifying data to others—sometimes in ways that are not especially visible or apparent to less sophisticated users.

Even when a platform allows people to read and write without attaching their legal names to these activities, the platform operator may well know precisely who its users are, as well as the particular locations from which they have connected, by analyzing information such as the users' Internet Protocol (IP) addresses. So the lack of conspicuous or deliberate use of a name online by no means implies that a range of entities don't know (or couldn't deduce) one's name, online history, and whereabouts, by examining the data that communications systems have made available to them.

The variety of ways that anonymity is protected online thus ranges from individuals' decisions not to use their legal names, through the policies and practices of some intermediaries (telecommunications service providers, e-mail and chat providers, online forums, and others) to avoid requiring registration or the use of a legal name, through intermediaries' policies on data retention, to the development and use of software tools that are specifically engineered to try to ensure anonymity. The latter group encompasses a portion of the software tools often known as Privacy-Enhancing Technologies (or PETS), but many of the tools in this category do not attempt to provide *anonymity*, only other properties such as secrecy or confidentiality of communications.

---

<sup>31</sup> Of course, a plethora of security tools exist to protect specific bits of communications data.

For instance, an envelope or wax seal may provide stronger protections of the secrecy of a letter one person sends to another, but if post offices or couriers succeed in requiring that letters bear accurate address information for their senders and recipients, the patterns of who is in contact with whom will still be clear to those delivering the letters—they will not be anonymous in that sense, even if the letter carriers never surreptitiously open or attempt to open any of the correspondence. In the online environment, protection of anonymity is more technically challenging than providing other sorts of privacy protection.

Only a few software tools and systems, such as the invisible Internet project (I2P),<sup>32</sup> the Tor project,<sup>33</sup> Jondo,<sup>34</sup> or SecureDrop<sup>35</sup> attempt to provide strong technical guarantees of their users' anonymity even in the face of a sophisticated attempt to reveal a user's identity. These systems go beyond the simple notion of not requiring people to state their names; they try to avoid creating a meaningful record that would reveal a user's identity.

Typically these tools work by obfuscating the link between a sender and a recipient of information by forwarding the information repeatedly through intermediaries that deliberately avoid recording information about how it was delivered. Where multiple independent parties provide links in the chain, no one entity may know enough to associate the original sender with the ultimate recipient. However, research has shown that the anonymity thus obtained may still be fragile, for example when a wiretapper sees that the volume of data sent

---

<sup>32</sup> Wikipedia. *I2P*. Retrieved February 6, 2015, from <https://en.wikipedia.org/wiki/I2P>

<sup>33</sup> *The Tor Project*. Retrieved February 6, 2015, from <https://www.torproject.org/>

<sup>34</sup> JonDoNym, *JonDo – the IP Changer*. Retrieved February 6, 2015, from <https://anonymous-proxy-servers.net/en/jondo.html>

<sup>35</sup> Freedom of the Press Foundation, *SecureDrop*. Retrieved February 6, 2015, from <https://freedom.press/securedrop>



by one party matches the volume of data received by another party at about the same time.<sup>36</sup>

Given a technical means of exchanging anonymous messages, software developers can try to build applications on top, as in the case of SecureDrop, which allows journalistic sources to contact press organizations anonymously, and anonymously submit documents to them and receive questions and replies in return.

Even the most sophisticated and strong anonymity systems can have points of failure. If, for example, a government suspected that a dissident was likely to attempt to speak anonymously, it might place malware on the dissident's computer, recording every keystroke. While the malware was operational, the strength of the anonymity system would become irrelevant because the government would monitor the dissident's activities and contacts directly.

### **Piercing the Veil: Identity Disclosure and the Role of Intermediaries**

Every individual must have confidence that the service providers that host their discussions will protect their privacy and expression. 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.

To protect individuals' 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

---

<sup>36</sup> See *Selected Papers in Anonymity*, presenting scholarly research on the techniques for achieving anonymity by technical means, and their limitations, since 1977. Retrieved February 6, 2015, from <https://freedom.press/securedrop> <http://www.freehaven.net/anonbib/>

so. Compelled disclosure must only occur once a legally defined offense has been committed. And even in those cases, all the rights of an online speaker must be considered before identifying that individual in response to a request to do so.

As the Inter-American Commission on Human Rights noted:

“[The protection of anonymity], does not, however, mean that anonymity safeguards all types of information. For example, the anonymity of the sender would in no way protect those who disseminate child pornography, engage in pro-war propaganda or the advocacy of hatred that constitutes the incitement of violence, or the direct and public incitement of genocide. 180 This kind of speech is not protected by the American Convention, and anonymity cannot protect its issuers from the legal consequences established — in accordance with international human rights law — in each domestic legal system with respect to each one of those cases. The same thing would occur if the exercise of the right to freedom of thought and expression were subject to the subsequent imposition of liability of the kind authorized by the American Convention. In all of those cases, judicial authorities would be authorized to take reasonable measures to determine the identity of the sender engaged in prohibited acts, in order to take proportionate action in response, as provided by law.”<sup>37</sup>

Judicial systems, not extrajudicial decision-making processes, are best suited to balance citizens’ right to anonymous expression with the need to provide a mechanism to redress wrongs.<sup>38</sup> Therefore, it is imperative that the

---

<sup>37</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*. Chapter IV (Freedom of Expression and the Internet). OEA /Serv.L/V/II.149. December 31, 2013. Para. 135. See also IACHR (2009). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*. Chapter III (Inter-American Legal Framework of the Right to Freedom of Expression). OEA/Ser. L/V/II. Doc. 51. Para. 80.

<sup>38</sup> In the United States, before a service provider can be forced to turn over the identity of someone who posted anonymously, many courts apply a very stringent test and only order that the disclosure of identities “is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs” the free expression rights of the person wishing to remain anonymous. See, for example, *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

laws do not require or permit Internet intermediaries to reveal the identity of the users without judicial decision-making. 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 pseudonymous user of their platform or service upon receipt of a court order, granted after a process of judicial review.

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.

As best practices, those third parties 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.<sup>39</sup>

Users should be provided with a reasonable amount of time to respond before the service provider produces the requested information. This will give the user an opportunity to object to disclosure of his or her identity.<sup>40</sup>

---

<sup>39</sup> This test reflects U.S. law on the issue. See EFF, *Test for Unmasking Anonymous Speech*, Internet Law Treatise. Retrieved February 6, 2015, from [http://ilt.eff.org/index.php/Speech:\\_Anonymity#Tests\\_for\\_Unmasking\\_Anonymous\\_Speakers](http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers).

<sup>40</sup> See EFF, Best Practices for Online Service Providers. Retrieved February 6, 2015, from <http://www.eff.org/wp/osp>. Canadian courts have also developed a test for determining whether to order a third party such as an ISP to disclose the identity of an anonymous defendant in scenarios where a reasonable expectation or privacy exists or freedom of

While intermediaries are often seen as a key source of information that can pierce the veil of anonymity online, they are by no means the sole source. As we have seen, the fragility of concealing identity in the face of sophisticated data analysis and the detecting and storage of data in all forms of everyday behavior (from walking down a CCTV-monitored street to purchasing goods electronically) means that suspects' identity can be ascertained by determined and targeted police work.<sup>41</sup> Intermediaries should therefore not be required to track all their users (thereby eliminating strong anonymity for all users). Nor should they be held responsible for the actions of users who are not identifiable as a result of the actions or inaction of the intermediary.

In some rare cases, it may be very hard, if not impossible, to identify a speaker after the fact. For example, if someone makes a single post online from the Wi-Fi of an popular Internet cafe that does not have records of its customer or camera in the vicinity. This is nothing new for the Internet age; for centuries people have been able to write graffiti in the dead of night, communicating anonymously. Indeed, it is much harder in the modern era to successfully communicate without leaving telltale traces. While there can be a legitimate interest in unmasking speakers who have violated a law, a requirement for always being able to unmask pays too high a price.

---

expression concerns are implicated. While variations exist, the test seeks to ensure that the order is necessary, the litigant intends to pursue the claim and that the claim is legally valid. See Canadian Internet Policy and Public Interest Clinic, *Online Anonymity & John/Jane Doe lawsuits*. Retrieved February 6, 2015, from <https://cippic.ca/index.php?q=online-anonymity-and-doe-lawsuits>

<sup>41</sup> For example, see *How Informants, Undercover Agents And Old-Fashioned Police Work Brought Down The Silk Road*. Retrieved February 6, 2015, from <http://www.ibtimes.com/how-informants-undercover-agents-old-fashioned-police-work-brought-down-silk-road-1807130>

## Anonymity Policies of Non-Governmental Actors

One way for a speaker to protect their anonymity is to not disclose their identity to intermediaries. These intermediaries may be compelled to disclose such information to the government or private litigants. But many intermediaries employ authentication procedures that require disclosure and registration of identity and other personal data, thus creating individually identifiable databases of user activity. The use of such tools is not always unreasonable. But such procedures should be used sparingly and proportionally to the concern the intermediary is trying to address. As noted by the IACHR free speech watchdog,

Online identification and authentication requirements need to be used exclusively in sensitive and risky transactions and interactions, and not broadly for all services and applications.<sup>42</sup> Authentication requirements must follow the principles of proportionality, which in this case indicate that if the risk is high, the collection of additional information from the user is justified. However, if the risk is low, there is no reason to do so. Among other things, this balance encourages anonymous platforms and services on the Internet, which enable freedom of expression in contexts of repression or self-censorship. Also, the principles of diversity indicate that multiple identification schemes must be encouraged for online users, in order to avoid single or concentrated identifiers that can lead to security abuses and privacy intrusions.<sup>43</sup>

As stated in the 2013 Annual Report of the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights: “online spaces where people’s activities and identities are not observed or documented should be promoted. This includes, for instance, the

---

<sup>42</sup> United Nations General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27*. May 16, 2011. Para. 84. Retrieved February 6, 2015, from [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

<sup>43</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression*. Chapter IV (Freedom of Expression and the Internet). OEA /Serv.LV/II.149. December 31, 2013. Para. 136.

preservation of anonymous platforms for the exchange of content and use of proportionate authentication services.”<sup>44</sup>

For instance, Facebook’s terms of service require that Facebook users provide their real names and information.<sup>45</sup> This practice creates serious risks particularly for dissidents and human rights workers using their names on Facebook in authoritarian regimes. The transmission of such identifiers, if mass harvested, can also be used to identify other anonymous online browsing activity.

This creates a negative effect: if Facebook’s terms of service are violated, Facebook can disable an individuals’ account. Given the current ubiquity of Facebook, this risks shutting down a key avenue for political discourse.<sup>46</sup> The way these policies against anonymity are enforced subjects the most vulnerable populations (that is, people with enemies or unpopular opinions) to the most risk because of the ease with which another user can report them and thus have their account suspended. For example, when a user is reported for using a “fake” name, Facebook will prompt the user to submit their official identification. For pseudonymous users, this is impossible; it also comes with other privacy risks.

---

<sup>44</sup> IACHR (2013). *Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter IV* (Freedom of Expression and the Internet). OEA /Serv.LV/II.149. December 31, 2013. Para. 23.

<sup>45</sup> Facebook, *Statement of Rights and Responsibilities*. Retrieved February 6, 2015, from <https://www.facebook.com/terms.php>

<sup>46</sup> Eva Galperin, *EFF Calls for Immediate Action to Defend Tunisian Activists Against Government Cyberattacks*, EFF, January 2011. Retrieved February 6, 2015, from <https://www.eff.org/deeplinks/2011/01/eff-calls-immediate-action-defend-tunisian>.

## The Regulation of Anonymity

### Positive Policies for the Protection of Anonymity

#### *United States*

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.”<sup>47</sup> The Supreme Court has also said that forced “identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance.”<sup>48</sup>

The U.S. Supreme Court has further noted that courts must “be vigilant... [and] guard against undue hindrances to political conversations and the exchange of ideas.”<sup>49</sup> 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 equity rights at issue.”<sup>50</sup> That review must take place whether the speech in question takes the form of political pamphlets or Internet postings or anything else.<sup>51</sup>

As a result, U.S. courts have strongly protected against the compelled disclosure of identities in a variety of situations: the rights of organizations to

---

<sup>47</sup> *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334. Retrieved February 6, 2015, from <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=514&invol=334?>

<sup>48</sup> *Talley v. California*, 362 U.S. 60 65 (1960). Retrieved February 6, 2015, from <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=362&invol=60>.

<sup>49</sup> *Buckley*, 525 U.S. at 192. Retrieved February 6, 2015, from <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=525&invol=182>

<sup>50</sup> *Dendrite Int’l, Inc. v. Doe*. Retrieved February 6, 2015, from <http://www.dmlp.org/threats/dendrite-international-v-does>

<sup>51</sup> *Reno v. ACLU*, 521 U.S. 844

keep the identities of their members confidential,<sup>52</sup> and the rights of online users to make sure that intermediaries are not compelled to disclose their identities unless such disclosure is truly necessary. As one court addressing the latter situation explained:

“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.”<sup>53</sup>

Additional 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.<sup>54</sup>

### Canada

Other jurisdictions have also recognized the importance of anonymity as a component of the right to privacy. The Supreme Court of Canada, in particular, recently issued a statement for the protection of anonymity of individuals online at the point of disclosure when they struck down warrantless acquisition of a user identity by the police as unconstitutional, stating:<sup>55</sup>

---

<sup>52</sup> See, for example, *NAACP v Alabama*, 357 U.S. 449 (1958), *Perry v Schwarzenegger*, 591 F.3d 1126 (9th Cir. 2009); *Britt v. Superior Court*, 20 Cal. 3d 824 (1978).

<sup>53</sup> *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999), Retrieved February 6, 2015, from <http://legal.web.aol.com/aol/aolpol/seescandy.html>

<sup>54</sup> *Lubin v. Agora, Inc.*, 389 Md. 1, 22, 882 A.2d 833, 846 (2005). Retrieved February 6, 2015, from <http://caselaw.findlaw.com/md-court-of-appeals/1237646.html>. See also *Tattered Cover v. The City of Thornton*, 2002 Colo. LEXIS 269 (2002). Retrieved February 6, 2015, from [http://scholar.google.com/scholar\\_case?case=8628043461770653869&hl=en&as\\_sdt=2&as\\_vis=1&oi=scholar](http://scholar.google.com/scholar_case?case=8628043461770653869&hl=en&as_sdt=2&as_vis=1&oi=scholar), regarding the right of bookstores to keep customer book purchase records confidential.

<sup>55</sup> *R. v. Spencer*, 2014 SCC 43, June 13, 2014



“[P]articularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person’s name, address and telephone number found in the subscriber information. Subscriber information, by tending to link particular kinds of information to identifiable individuals may implicate privacy interests relating to an individuals’ identity as the source, possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure. In this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests. . . The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.”

### **South Korea**

In 2007, the South Korean legislature passed Article 44-5 of the Information Communication Network Act (“ICNA,” hereinafter) which obligated all the Internet intermediaries receiving more than 100,000 average daily users to accept postings from only those users who verify their identities. The legislative purpose of this provision was to make the posters’ identity “trackable” and thereby deter illegal activities online. However, there was no evidence that illegal activities decreased over time as revealed by six empirical studies including one commissioned by the government itself.<sup>56</sup> Five years later, the Korean Constitutional Court struck down the ICNA provision and took the decision as an

---

<sup>56</sup> For a discussion of the six studies, see PARK Kyung Sin, *Freedom of Speech and Communications – Theories and Practices* (표현 통신의 자유), published by Non-Hyung(논형) in 2013, p. 433-435

opportunity to make probably the most refined statement on the relationship between anonymous speech online and democracy as follows<sup>57</sup>:

“Anonymous speech in the Internet, rapidly spreading and reciprocal, allows people to overcome the economic or political hierarchy off-line and therefore allow them to form public opinions free from class, social status, age, and gender distinctions, which make governance more reflective of the opinions of people from diverse classes, and thereby further promotes democracy. Therefore, anonymous speech in the Internet, though fraught with harmful side-effects, should be strongly protected in view of its constitutional values.”

The Court also reasoned clearly why mandatory user identification is almost always disproportionate as follows:

“The rule here mandates identity verification regardless of the content of the posting from almost all users on all major websites. Many prospective posters, not completely sure of what is a prohibited posting, are likely to give up on posting at all in fear of discipline or prosecution, the risk of which flows from the exposure of the names and resident registration numbers. Such result of suppressing a great majority's legal postings on the account of the existence of a minority of people abusing the Internet is an excessive restriction on freedom of anonymous speech. . . [it] treats all people as potential criminals in favor of investigative expediency (emphasis added).”

### *Mexico*

Anonymity has been protected as a precondition to the exercise of the confidentiality of sources and the journalistic right to professional secrecy. The Mexican Supreme Court has held, for example, that:

“(…) The journalist has the right to maintain the secret identity of the sources that have given information on reserved condition, express or implied. Thus, (…) the reporter called to testify in civil proceedings may invoke their right to secrecy and refuse to identify

---

<sup>57</sup> Constitutional Court's Decision 2010 Hunma 47, 252 (consolidated) announced August 28, 2012

their sources and to excuse the answers that could reveal the identity of the same."

The Mexican Federal and Federal District legislation also recognized this right. For example the Mexican Federal Code of Civil Procedures recognizes by professional secrecy, as precluding the obligation to produce documents and provide all kinds of assistance to the courts in their inquiries.<sup>58</sup> Similarly, the Federal Code of Criminal Procedure recognizes that journalists are not obliged to testify about the information received, known or in their possession of:

"III. Journalists, for the names or recordings, telephone records, notes, documentary and digital files and anything that directly or indirectly may lead to identification of persons, with the performance of its business, provide them as reserved character information on which they base any publication or statement."<sup>59</sup>

The new Code of Criminal Procedure, which will enter into force gradually throughout the Mexican country, also recognizes this right.<sup>60</sup> Finally, the Law on Professional Secrecy of Journalists in Mexico City grants broad protections to journalists and media partners.<sup>61</sup> These protections include the right to reserve the identity of their sources; the right not to be required to report data or disseminated facts that are part of investigative journalism; the right not to be subject to inspection by any authority that want access to the journalists notes, recording equipment, computer, directories, telephone records and any document that may lead to the identification of sources; the right not to be subjected to inspection on their personal data, among others.

---

<sup>58</sup> Article 90 of the Mexican Federal Code of Civil Procedures.

<sup>59</sup> Article 243 Bis of the Mexican Federal Code of Criminal Procedures.

<sup>60</sup> See Article 244 and 362. *New Mexican Federal Code of Criminal Procedures*. Retrieved February 6, 2015, from [http://dof.gob.mx/nota\\_detalle.php?codigo=5334903&fecha=05/03/2014](http://dof.gob.mx/nota_detalle.php?codigo=5334903&fecha=05/03/2014)

<sup>61</sup> Law of the professional journalistic secrecy and confidentiality of sources in Mexican federal district (*Ley del secreto profesional del periodista en el distrito federal*). Retrieved February 6, 2015, from <https://eff.org/r.lb34v0>.

These decisions establish a strong and principled policy for the protection of anonymity.

### **Policies that Undermine the Right to Anonymity**

#### ***South Korea***

South Korea's overall practices cannot be counted as solely best practices because even with its historic Constitutional Court's decision, three other identity verification requirements remain in full force: (1) Article 82-6(1) and 82-6(5) of the Public Officials Election Act, requiring practically all relevant Internet intermediaries to accept user-created postings publicly supporting or opposing a candidate during an election campaign period (usually 2-3 weeks) only when the users verify their identities;<sup>62</sup> (2) Article 16(4) of Juveniles Protection Act, requiring all Internet intermediaries servicing adult material to verify in advance the identity of the users of that material;<sup>63</sup> (3) Article 12(3) Paragraph 1 Item 1 of Game Industry Promotion Act, requiring all "Internet game" providers to verify in advance the age and therefore the identity of the players.<sup>64</sup>

The most glaring deficiencies in the protection of online anonymity is the laws that require or permit Internet intermediaries to reveal the identities of the users without a warrant or any other judicial approval. The U.S.,<sup>65</sup> UK,<sup>66</sup> Germany,<sup>67</sup> and France<sup>68</sup> all fare badly in this regard, but South Korea's<sup>69</sup> policies

---

<sup>62</sup> Public Officials Election Act. Retrieved February 6, 2015, from [http://elaw.klri.re.kr/kor\\_service/lawView.do?hseq=25035&lang=ENG](http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25035&lang=ENG)

<sup>63</sup> Article 16(4) of Juveniles Protection Act. Retrieved February 6, 2015, from [http://elaw.klri.re.kr/kor\\_service/lawView.do?hseq=27676&lang=ENG](http://elaw.klri.re.kr/kor_service/lawView.do?hseq=27676&lang=ENG)

<sup>64</sup> Game Industry Promotion Act. Retrieved February 6, 2015, from [http://elaw.klri.re.kr/kor\\_service/lawView.do?hseq=28802&lang=ENG](http://elaw.klri.re.kr/kor_service/lawView.do?hseq=28802&lang=ENG)

<sup>65</sup> 18 U.S. Code, Sections 2703(c)(1)(E), (2)

<sup>66</sup> UK Regulation of Investigatory Powers Act 2000, Article 23

<sup>67</sup> Federal Electronic Communications Act, Article 113 (1)

<sup>68</sup> Code des Postes et Communications Électroniques, Article L34-1 through L34-6

<sup>69</sup> Korea's Telecommunications Business Act, Article 83(3)

have led to a massive warrant-less disclosure of user identities by Internet intermediaries to the police, sometimes reaching as much as 20% of a country's whole population in some years.<sup>70</sup> In an attempt to rein in this practice, an intermediary appellate court of Korea in October 2012 held a major portal liable for disclosing a blogger's identity to the police investigating a case of defamation against a politician when no warrant was produced. The decision resulted in Internet content and application providers halting altogether the provision of data without a warrant. Korean telecommunication companies continue the practice.

### **Brazil**

In Brazil, the Constitution prohibits anonymous speech.<sup>71</sup> The intention behind the prohibition is to keep the possibility of identifying anyone who expresses any opinions, beliefs or comments, both in the online or in the offline world. As we have stated above, anonymity is a precondition for the exercise of freedom of expression and privacy, which makes it possible for citizens to express themselves freely and without fear of retaliation. By not allowing Brazilian citizens to engage in anonymous speech, the Constitution imposes significant obstacles to their ability to report abuses of power or express unpopular opinions. Nevertheless, that prohibition does not extend to the protection of privacy.

Even though the use of pseudonyms is not explicitly forbidden by the Brazilian Constitution, the ban on anonymous speech has been used as legal grounds for disclosure of identity requests, which are often granted by Brazilian

---

<sup>70</sup> Park Kyung Sin, *Communications Surveillance in Korea*. Retrieved February 6, 2015, from <https://eff.org/r.internetsurveillanceprivacy987>

<sup>71</sup> Constitution of the Federal Republic of Brazil of 1988, article 5, IV: "the expression of thought is free, and anonymity is forbidden".

Courts. This practice has been leading to the consolidation of case law that takes a strong stance against the use of non-real profiles.<sup>72</sup>

The Brazilian Civil Rights Framework for the Internet (“*Marco Civil da Internet*”), enacted in 2014, reinforces that freedom of speech is a foundational principle for Internet users in Brazil.<sup>73</sup> However, this has to be construed under limitations imposed by the Constitution, leaving very little room for interpretations that could allow anonymity for free expression purposes.<sup>74</sup>

The Brazilian Civil Rights Framework for the Internet also establishes that Brazilian law should be applicable to any products or services used by individuals located in Brazil.<sup>75</sup> This provision has empowered Public Prosecutors and law enforcement officials to claim that the constitutional ban on anonymous speech should prevent the use of Internet applications that allow anonymous expression.

---

<sup>72</sup> Research suggests that in more than 48% of cases, judges issued preliminary injunctions demanding disclosure of identification information from intermediaries such as application logs and IP addresses.

<sup>73</sup> Article 2: “The discipline of Internet use in Brazil has as fundamentals the respect for freedom of expression, as well as: [...]”.

<sup>74</sup> Article 3: “The discipline of Internet use in Brazil has the following principles: I – guarantee of freedom of expression, communication and expression of thoughts, under the terms of the Federal Constitution; [...]”.

<sup>75</sup> Article 11. “Any process of collection, storage, custody and treatment of records, personal or communications data by connection providers and Internet applications providers, in which at least one of these acts occurs in the national territory, shall respect Brazilian law, the rights to privacy, and the confidentiality of personal data, of private communications and records. § 1st The aforementioned provisions apply to data collected in national territory and to the content of communications, in which at least one of the terminals is located in Brazil. § 2nd The provisions aforementioned apply even if the activities are carried out by a legal person located abroad, since that the offered services to Brazilian public or that at least one member of the same economic group owns establishments in Brazil. § 3rd The connection providers and Internet applications provider shall provide, in the form of regulations, information that allow the verification of their compliance with Brazilian legislation regarding the collection, custody, storage and processing of data, as well as how the provider respects the privacy and secrecy of communications. § 4th Decree shall regulate the procedure for finding violations of the provisions of this article.”

A recent example of this restriction is the ban imposed to “Secret,” an Internet application that markets itself as a “safe place to say what’s on your mind anonymously.” Invoking the Brazilian Constitution’s prohibition, the Public Prosecutors Office brought a lawsuit against the service, which had quickly become extremely popular in Brazil. Although later overturned, an injunction was granted to ban “Secret” from online application stores (Google and Apple) in Brazil and to have it remotely removed from devices where it had been already installed.

This high-profile case points to a potential danger of broadening the scope of the Constitution’s prohibition and applying it to prevent the use of privacy enhancing technologies, which would also bring undesirable repercussions to the rights of reading and browsing anonymously.

### *Vietnam*

In 2013, the government of Vietnam passed Decree 72 or the "Management, Provision, Use of Internet Services and Information Content Online" which outlawed the use of pseudonyms, forcing individuals with personal blogs to publicly list their real name and address. The main aim of the decree was to privatize censorship by placing the burden of the task onto technology companies, and to silence dissident voices that are not in line with the Vietnamese Communist Party.

### *Russia*

Russia has also cracked down on anonymous and pseudonymous bloggers, who once made up a lively civil society on the RuNet. In April 2014, the Russian Duma passed a law that required bloggers to declare their family name, initials, and e-mail address. Any author writing primarily in Russian (including those located outside of Russia) whose web page or social network has 3,000

visitors or more a day must register on a special list and abide by restrictions applicable to the mass media.

### *Europe*

Europe's strong data protection regulations establish limits on the disclosure and storage of personally identifying information. German law establishes that online service providers "must enable the use of telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable."<sup>76</sup> However, German regulators have found it difficult to enforce such rules against providers such as Facebook whose terms of service forbid pseudonyms.<sup>77</sup>

Another challenge to protecting anonymity in Europe is a recent decision by the Chamber of the European Court of Human Rights which judged that a "[intermediary] company's choice to allow comments by non-registered users" indicated that the intermediary should be liable for the defamatory nature of the hosted comments.<sup>78</sup> While the decision is currently being appealed to the Grand Chamber of the same court, the effect of expanding liability in cases of an intermediary's ignorance of its users' identities will inevitably limit commercial support for users who seek to strongly protect their identity.

### *United States*

The U.S. Congress has not done well in protecting anonymity either. In some situations, the information identifying a party to telecommunications is

---

<sup>76</sup> Telemedia Act Section 2007 Section 13(6). "Telemedia" here refers to to all electronic communication services except broadcast and pure telecommunication (signal transmission) services.

<sup>77</sup> Facebook's European offices are based in Ireland, and the German courts have determined that German law would not apply to the company's data-processing outside Germany. See IDG News Service (2013), *Facebook can keep its real name policy, German appellate court decides*. Retrieved February 9, 2015, from <http://news.idg.no/cw/art.cfm?id=2872E148-CD11-E822-FFF3051EA573B6DD>

<sup>78</sup> *Delfi AS v. Estoni*, [2013] ECHR 941, 58 EHRR 29, (2014) 58 EHRR 29. Retrieved February 9, 2015, from <http://www.bailii.org/eu/cases/ECHR/2013/941.html>



made accessible without either a warrant or any before the fact judicial supervision,<sup>79</sup> allowing the bad practices of intermediaries, described below, of complying with a tremendous number of simple attorney-signed subpoenas requesting identities of the users.

In the U.S., it is all too common for plaintiffs in civil cases 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 rare circumstances, such as a subpoena issued pursuant to the Digital Millennium Copyright Act, a lawsuit is not necessarily filed first.<sup>80</sup>

The U.S. also allows for the state to issue national security letters (NSLs), which can demand the identity information about an online speaker without judicial review.<sup>81</sup> These NSLs are almost always accompanied by a gag order, forbidding the service provider from disclosing that it has received an NSL to anyone, effectively make it impossible for the subject to contest the demand in a court. While a U.S. court has declared the NSL power to be unconstitutional, that decision is stayed pending the government's ongoing appeal.<sup>82</sup>

---

<sup>79</sup> 18 U.S. Code, Sections 2703(c)(1)(E), (2)

<sup>80</sup> 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](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)

<sup>81</sup> 18 U.S.C. § 2709.

<sup>82</sup> *In re Matter of National Security Letters*, No. 13-1165 (N.D. Cal. Mar. 14, 2013), <https://www.eff.org/document/nsl-ruling-march-14-2013>

### **Mass Copyright Litigation**

In recent years, a few enterprising law firms in the U.S., the UK and Europe have used mass copyright litigation to extract settlements from individuals. These law firm groups try to grow businesses out of suing Internet users on behalf of copyright owners.<sup>83</sup> These lawsuits follow the model of those filed by members of the Recording Industry Association of America in 2003.<sup>84</sup>

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 \$150,000 per copyrighted work allegedly wilfully infringed) frequently pressures defendants into settling. These lawsuits raise concerns about due process and the protection of citizens' right to privacy.<sup>85</sup> 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.<sup>86</sup>

### **Mass Surveillance**

Finally, a pervasive attack on the anonymity rights of those communicating digitally must be the programs of unchecked digital mass surveillance currently

---

<sup>83</sup> EFF, *Copyright Trolls*. Retrieved February 6, 2015. Retrieved February 6, 2015, from <https://www.eff.org/issues/copyright-trolls>. EFF, *USCG v. The People*. Retrieved February 6, 2015, from <https://www.eff.org/cases/uscg-v-people>.

<sup>84</sup> 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.

<sup>85</sup> *Achte - Neunte v. Does*. Retrieved February 6, 2015, from <http://www.eff.org/cases/achte-neunte-v-does>. See also EFF, *Anonymity Protection Lawsuits*. Retrieved February 6, 2015, from <https://www.eff.org/issues/anonymity>.

<sup>86</sup> *RIAA v. the People: Five Years Later Report*, EFF. Retrieved February 6, 2015, from <http://www.eff.org/wp/riaa-v-people-years-later>

being conducted by the signals intelligence services of the Five Eyes countries (the United States,<sup>87</sup> Canada,<sup>88</sup> the United Kingdom, Australia, and New Zealand<sup>89</sup>), and potentially many more states.

The collation and correlation of so much communications data and metadata provides these intelligence agencies with an unparalleled capability to strip anonymity from millions of innocent users of telecommunication systems. In some cases, these mass interception programs have included projects specifically aimed at undermining general purpose anonymity tools, such as the Tor network.<sup>90</sup>

A full critique of these programs and the damage they represent to free expression is beyond the scope of this submission, but it should be noted that their existence both highlights the fragility of protecting online anonymity, and the importance of strong legal<sup>91</sup> and technical<sup>92</sup> safeguards to defend it.

## II. Encryption

### Encryption and Free Expression

In the online environment, the freedom to use encryption technology is often a prerequisite for the exercise of the rights of privacy and expression.<sup>93</sup> In the absence of encryption, online communications can easily be intercepted.<sup>94</sup>

---

<sup>87</sup> See *NSA Spying on Americans*, <https://www.eff.org/nsa-spying>

<sup>88</sup> See *Ottawa Statement on Mass Surveillance in Canada*, <https://openmedia.ca/statement>

<sup>89</sup> See *Eyes Wide Open*, <https://www.privacyinternational.org/?q=node/301>

<sup>90</sup> See Guardian (2013), *NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users*. Retrieved February 9, 2015, from <http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>

<sup>91</sup> For instance, the *International Principles on the Application of Human Rights to Communications Surveillance*. Retrieved February 9, 2015, from <https://necessaryandproportionate.org>

<sup>92</sup> For instance, see RFC 7258, *Pervasive Monitoring Is an Attack*, Retrieved February 9, 2015, from <https://tools.ietf.org/html/rfc7258>

<sup>93</sup> Encryption allows users to have private conversations over email, web browsing, or cell phones. To learn more: See, EFF (2014), *Surveillance Self Defense*. Retrieved February 6, 2015, from <https://ssd.eff.org/>.

<sup>94</sup> See e.g. *Firesheep* (2010). Retrieved February 6, 2015, from <http://codebutler.com/firesheep>. See also John P. Mello Jr., *Free Tool Offered To Combat Firesheep Hackers*, PCWorld, Retrieved February 6, 2015, from

Because of the way that the Internet has developed, Internet intermediaries that store and forward our communications are often in a position to possess and read all the communications that pass through their networks. In order to preserve their users' security and privacy, service providers should be able to design systems that ensure end-to-end privacy, which is to say systems that ensure that a message can be read by its intended recipient and no one else.

The freedom of expression has various intersections with the right to develop and use encryption. Encryption directly protects expression by preventing automated technical censorship systems from blocking access to particular content (or even particular key words). It protects expression indirectly by giving users confidence that the confidentiality of their controversial communications or controversial reading decisions is protected by technical means. Developers of encryption software are engaged in their own expressive activity when they publish code. Any attempt to prohibit encryption would also run up against the freedom of expression. Many strong end-to-end encryption programs are open source code, publicly posted and available to anyone to download from a wide variety of sources. If a state were to attempt to prohibit these programs, it would need to control access to this information, prohibit publication, or institute the infrastructure necessary to detect and penalize use. All of these methods would have severe and negative consequences for freedom of expression.

In 1999, a U.S. Court of Appeal agreed with EFF that a broad range of individual rights interests were implicated by pervasive government controls on

---

[http://www.pcworld.com/article/211531/free\\_tool\\_offered\\_to\\_combat\\_firesheep\\_hackers.html](http://www.pcworld.com/article/211531/free_tool_offered_to_combat_firesheep_hackers.html). Seth Schoen, Richard Esguerra (2010). *The Message of Firesheep: "Baaaad Websites, Implement Sitewide HTTPS Now!*, EFF. Retrieved February 6, 2015, from <http://www.eff.org/deeplinks/2010/10/message-firesheep-baaaad-websites-implement>. EFF, *Tool Offers New Protection Against 'Firesheep'*, November 23, 2010. Retrieved February 6, 2015, from <http://www.eff.org/press/archives/2010/11/23>.

publishing encryption source code—both the rights of those seeking to publish the code and, potentially, of those seeking to use it to protect their privacy.

[W]e note that the government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the Internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously [...], the right against compelled speech [...], and the right to informational privacy [...].<sup>95</sup>

## The Use of Encryption in Digital Communications

Encryption is the mathematical process of using codes and ciphers to communicate privately. Throughout history, people have used increasingly sophisticated methods of encryption to send messages to each other with the objective that they cannot be read by anyone besides the intended recipients. Early forms of encryption were often simple operations that could be performed

---

<sup>95</sup> *Bernstein v. U.S. Dept. of Justice*, 176 F.3d 1132, 1145-1146 (9th Cir. 1999) (internal citations omitted). The opinion is not precedential.

by hand, e.g. the “Caesar cipher” of ancient Rome.<sup>96</sup> Today, computers are capable of performing vastly more complex and secure encryption for us. The purposes to which cryptographic technology is put have expanded beyond secret messages; today, cryptography can be used for additional purposes, for example to verify the authorship of messages<sup>97</sup> or the integrity of software downloads, or to browse the Web anonymously with Tor.<sup>98</sup>

Most modern encryption for communications applications relies on a concept known as public-key cryptography. Public-key cryptography relies on a matched pair of keys: a private key, which is a file kept secret by the user and allows her to read messages that are intended only for her, and a public key, which is a file that the user publishes or gives to others that allows people to communicate with her privately. A private key also lets the user place unforgeable digital signatures on messages sent to other people so that they can verify that messages purporting to be from her have not been forged or modified. Private and public keys come in matched pairs, generated at the same time by a process that creates a special mathematical relationship between the public and private key. The result is that anyone can verify that a message was signed by a user with a particular private key by examining that user’s public key. Together, these features of public-key cryptography allow Internet users to have confidential communications with sites and services or with other users, and allow them to be confident that the content of their communications hasn’t been tampered with. They can also use public-key cryptography to ensure the integrity of documents and software downloads; an essential tool for preventing the installation of maliciously-modified software applications.

---

<sup>96</sup> Chris Savarese and Brian Hart '99, *The Caesar Cipher*. Retrieved February 6, 2015, from <http://www.cs.trincoll.edu/~crypto/historical/caesar.html>

<sup>97</sup> PGPi, “Digital Signatures - How PGP Works”. *Introduction to Cryptography*. Retrieved February 6, 2015, from <http://www.pgpi.org/doc/pgpintro/#p12>

<sup>98</sup> “Staying Anonymous,” Tor Project Overview. February 6, 2015, from <https://www.torproject.org/about/overview.html.en#stayinganonymous>

Encryption is also vital for protecting data “at rest” when stored on a hard drive or portable device. Many of us carry entire histories of our contacts, our communications, and our current documents on laptops, or even mobile phones. That data can include the confidential information of dozens, even thousands, of people. A phone or laptop can be stolen, or copied in seconds. The electronic devices we trust and rely on to store and manage our personal information in turn rely on a different application of encryption to protect the data we entrust to them.

Most computers and smartphones offer complete, full-disk encryption as an option, and some manufacturers—especially those of mobile devices—now enable full-disk encryption by default. Here’s how Apple describes its full-disk encryption implementation, which it calls FileVault 2:

With FileVault 2, your data is safe and secure — even if your Mac falls into the wrong hands. FileVault 2 encrypts the entire drive on your Mac, protecting your data with XTS-AES 128 encryption. ... Want to start fresh or give your Mac to someone else? FileVault 2 makes it easy to clean data off your Mac. Instant wipe removes the encryption keys from your Mac — making the data completely inaccessible — then proceeds with a thorough wipe of all data from the disk.<sup>99</sup>

Apple’s description highlights another use for encryption: without full-disk encryption, it is extremely difficult to ensure that private data is completely gone from a computer or storage device when it comes time to sell or otherwise dispose of it.<sup>100</sup> Only with encryption can users be sure that their data won’t be accessible to the next person who takes possession of the device. Without encryption, the personal data of former owners of discarded or resold devices is

---

<sup>99</sup> Apple Inc, *Safety. Built Right In.* Retrieved February 6, 2015, from <https://www.apple.com/osx/what-is/security/>

<sup>100</sup> The encrypted data could still be present in encrypted form, but the next person with the device will be unable to read it.

at risk—indeed, so is *everyone's* personal data when legal and medical practices, schools, government entities, and others discard devices containing unencrypted personal records.<sup>101</sup> Encryption is also widely recognized as a standard precaution for preventing or mitigating the effects of data breaches.<sup>102</sup>

## Encryption and the State

Despite encryption's centrality for every aspect of information security, efforts to make it more readily and conveniently available to the public have often drawn the ire of those in government. For more than two decades, the Internet has provided us with a truly global platform for expression. Today, anyone can write an opposition party blog, post photographs of their cats, organize a street protest, contribute to an open source cryptography project, participate in the search for extraterrestrial life, or mine for Bitcoins. Some of the activity on the Internet—rightly or wrongly—has drawn the ire of governments around the world. Their reactions have been unfortunately predictable; they not only proscribe the activities they consider harmful, but attempt to prescribe the manner in which the Internet itself operates. That they fail repeatedly somehow fails to deter them from trying time and time again.

Many states have attempted to use export or import control regulations, or domestic legislation or regulation, to limit the public's access to encryption tools or to try to exact security-weakening concessions from manufacturers and software developers.<sup>103</sup> In high-profile cases, as well as in closed-door negotiations, governments have directly pressured individual manufacturers by

---

<sup>101</sup> Compare Simson L. Garfinkel and Abhi Shelat, "Remembrance of Data Passed: A Study of Data Sanitization Practices", IEEE Privacy and Security, January/February 2003 (describing the results of buying and examining the contents of large numbers of used hard drives, including massive quantities of sensitive personal data).

<sup>102</sup> For instance, in the United States, the otherwise strict data breach notification rules surrounding health information are set aside if the compromised data is encrypted. See 74 Fed. Reg. 19006 (Apr. 27, 2009).

<sup>103</sup> See Bert-Jap Koops (2013), *Crypto Law Survey*. Retrieved February 9, 2015, from <http://cryptolaw.org/> (listing known export, import, and domestic use controls on encryption).



threatening to ban or block their products and services. From 2010 to 2013, for instance, Canadian mobile manufacturer BlackBerry was involved in public confrontations with (at least) the governments of Saudi Arabia, the United Arab Emirates, and India, which objected to the BlackBerry service's use of strong encryption terminating in Canada, and suggested that the use of the firm's products might be banned in their territories.<sup>104</sup> The manufacturer responded by agreeing to deliver a solution that would grant governments access to spy on non-enterprise users.<sup>105</sup>

The United States at one time required government licenses for each and every copy of encryption software exported, including via Internet download to users outside of the United States (or via open publication online in a forum that foreigners could access). Based in a tradition of viewing cryptographic technology as military rather than civilian, the original regulations treated encryption devices or software with a key length of more than 40 bits as a "munition," and their export was controlled alongside the export of physical weapons. The result was absurd. Software developed in the United States was commonly produced in "US" and "International" versions, with the International version stripped of strong encryption. Users were presented with a choice: did they want a version of the software that supported only 40-bit encryption (breakable in hours or minutes on today's PCs), or did they want the full 128-bit capable version? The "strong" version was only available if the user checked a box asserting that they lived in the United States or Canada. The ineffectual restriction was a function of the fact that at the time there were no accurate mechanisms to verify an Internet user's location.

---

<sup>104</sup> See, e.g., BBC News (2010), *Two Gulf States to Ban Some BlackBerry Functions*. Retrieved February 9, 2015, from <http://www.bbc.com/news/world-middle-east-10830485>.

<sup>105</sup> See Wired News (2013), *BlackBerry gives Indian government ability to intercept messages*, retrieved February 9, 2015, from <http://www.wired.co.uk/news/archive/2013-07/11/blackberry-india>

The United States' restrictions on cryptography lead to ridiculous results (a checkbox to verify whether the user was in the United States, for example—or different rules applied to the export of precisely the same cryptographic code on a floppy disk or in a printed book), but utterly failed to stop the spread of strong encryption.

The United States eventually reversed what amounted to a pervasive ban on the export of strong encryption—after significant industry and civil society opposition, as well a lawsuit by Professor Daniel J. Bernstein, represented by the Electronic Frontier Foundation.<sup>106</sup> But governments haven't stopped trying to stop the spread of information, and export regulations remain a favorite method.

Currently, however, we see the United Kingdom leading a new effort, not only against the export of encryption, but against its very development and use by the public. UK Prime Minister Cameron, supported by U.S. President Obama, for example has called for technology companies to maintain “very clear front doors” in their software whereby law enforcement—when armed with appropriate legal process—could access the content of any and all messages.<sup>107</sup>

While there has been no formal proposal in the UK or the U.S., Prime Minister Cameron's statement implies that his government believes developers of communication tools should be mandated to ensure that the content of their messages must always be accessible to third parties (here, law enforcement). As described above however, the security of encryption is provided specifically

---

<sup>106</sup> For a wide-ranging account of the defeat of the U.S. government's anti-encryption policies in the 1990s, see Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (New York: Viking Penguin, 2001).

<sup>107</sup> The White House Office of the Press Secretary (2015). *Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference*. Retrieved February 6, 2015, from <http://www.whitehouse.gov/the-press-office/2015/01/18/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint->

because it prevents third parties from accessing the encrypted content. Any encryption scheme in which it is possible for someone other than the intended recipient to access the message includes a fundamental weakness that tends in practice to help *every* attacker.<sup>108</sup>

Computer security expert Steven Bellovin has explained some of the reasons why back doors weaken security generally. First, it's hard to secure communications properly even between two parties. Cryptography with a back door adds a third party, requiring a more complex protocol, and as Bellovin puts it: "Many previous attempts to add such features have resulted in new, easily exploited security flaws rather than better law enforcement access<sup>109</sup>." Bellovin further notes:

Complexity in the protocols isn't the only problem; protocols require computer programs to implement them, and more complex code generally creates more exploitable bugs. In the most notorious incident of this type, a cell phone switch in Greece was hacked by an unknown party. The so-called 'lawful intercept' mechanisms in the switch—that is, the features designed to permit the police to wiretap calls easily—was abused by the attacker to monitor at least a hundred cell phones, up to and including the prime minister's. This attack would not have been possible if the vendor hadn't written the lawful intercept code.

---

<sup>108</sup> For contemporary critiques of U.S. law enforcement complaints about encryption products, particularly Apple's full-disk encryption software, see Jeremy Gillula (2014), *Even a Golden Key Can Be Stolen by Thieves: The Simple Facts of Apple's Encryption Decision*. Retrieved February 9, 2015, from <https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision>; Kevin Poulsen (2014), *Apple's iPhone Encryption is a Godsend, Even if Cops Hate It*, Wired. Retrieved February 9, 2015, from <http://www.wired.com/2014/10/golden-key/>; Chris Coyne (2014), *The Horror of a Secure Golden Key*, Retrieved February 9, 2015, from <https://keybase.io/blog/2014-10-08/the-horror-of-a-secure-golden-key> (each responding to law enforcement criticisms of Apple on disk encryption and highlighting the security risks created by back doors in encryption systems).

<sup>109</sup> Steve Bellovin (2010). *The Worm and the Wiretap*, SMBlog. Retrieved February 6, 2015, from <http://www.cs.columbia.edu/~smb/blog//2010-10/2010-10-16.html>

More recently, as security researcher Susan Landau explained,<sup>110</sup>

“an IBM researcher found that a Cisco wiretapping architecture designed to accommodate law-enforcement requirements—a system already in use by major carriers—had numerous security holes in its design.<sup>111</sup> This would have made it easy to break into the communications network and surreptitiously wiretap private communications.”

The same is true for Google, which had its "compliance" technologies hacked by China.<sup>112</sup>

This isn't just a problem for the average individual, or even for the millions of companies that need secure communications. Government agencies around the world currently use many commercial products — the same ones they want to force to have a back door. Law enforcement will not be able to ensure that others will not be able to access the same back doors that they themselves use.

Furthermore, users who want strong encryption will be able to get it — from the many places in the world where encryption is offered for sale and for free. In 1996, the United States National Research Council published a study called "Cryptography's Role in Securing the Information Society," nicknamed CRISIS.<sup>113</sup> The National Research Council observed:

Products using unescrowed encryption are in use today by millions of users, and such products are available from many

---

<sup>110</sup> Susan Landau (2010), *Moving Rapidly Backwards on Security*, Huffington Post. Retrieved February 6, 2015, from [http://www.huffingtonpost.com/susan-landau/moving-rapidly-backwards-\\_b\\_760667.html](http://www.huffingtonpost.com/susan-landau/moving-rapidly-backwards-_b_760667.html)

<sup>111</sup> Tom Cross (2010), *Exploiting Lawful Intercept to Wiretap the Internet*. Retrieved February 6, 2015, from <https://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html#Cross>

<sup>112</sup> Bruce Schneier (2010), *U.S. Enables Chinese Hacking of Google*. Retrieved February 6, 2015, from <http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html>

<sup>113</sup> Kenneth W. Dam and Herbert S. Lin (1996). *Cryptography's Role in Securing The Information Society*. Retrieved February 6, 2015 from [http://www.nap.edu/openbook.php?record\\_id=5131](http://www.nap.edu/openbook.php?record_id=5131)

difficult-to-censor Internet sites abroad. Users could pre-encrypt their data, using whatever means were available, before their data were accepted by an escrowed encryption device or system. Users could store their data on remote computers, accessible through the click of a mouse but otherwise unknown to anyone but the data owner, such practices could occur quite legally even with a ban on the use of unescrowed encryption. Knowledge of strong encryption techniques is available from official U.S. government publications and other sources worldwide, and experts understanding how to use such knowledge might well be in high demand from criminal elements.<sup>114</sup>

None of that has changed. And of course, more encryption technology is far more readily available today than it was in 1996; it's a basic feature of operating systems, computer programming languages, computer network protocols, and is routinely taught in university curricula all over the world. So unless governments want to mandate that users are forbidden to run anything that is not government approved on their devices, their efforts to stop malicious actors from getting hold of encryption tools will be of extremely questionable efficacy.

In addition, in order to ensure that no "untappable" technology exists, what Prime Minister Cameron appears to propose would amount to a technology mandate and a draconian regulatory framework. The implications of this for innovation are dire. Could Mark Zuckerberg have built Facebook in his dorm room if he'd had to build in surveillance capabilities before launch in order to avoid government fines? Would the original Skype have ever happened if it had been forced to include an artificial bottleneck to allow government easy access to all of your peer-to-peer communications? This has especially serious implications for the open source community and small innovators. Some open source developers have already taken a stand against building back doors into software.

---

<sup>114</sup> CRISIS report at 303. "Escrowed" encryption here refers to a set of systems promoted by the administration of U.S. President Bill Clinton, in which someone other than an end-user—an "escrow agent"—maintains a spare copy of the user's decryption keys or other technical data that would allow the user's messages to be decrypted.

<sup>115</sup> And any additional mandates on service providers would require them to spend a vast amount of money making their technologies compliant with the new rules. Of course, there can be no real question about who will foot the bill: the providers will pass those costs onto their customers.

## Defending the Right to Encrypt

Despite there being similar proposals to ban secure, end-to-end encryption since at least 1995,<sup>116</sup> governments around the world have entirely failed to present evidence that encryption actually causes a problem for law enforcement. In 2010, the New York Times reported that the government officials pushing for this have only come up with a few examples (and it is not clear that all of the examples actually involve encryption) and no real facts that would allow independent investigation or confirmation.<sup>117</sup>

Both individuals and government agencies rely on strong encryption in their daily activities.<sup>118</sup> Moreover, human rights activists, journalists, refugees, bloggers, and whistle-blowers 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

---

<sup>115</sup> Zooko O'Whielacronx (2010), *Statement on Backdoors*. Retrieved February 6, 2015, from <http://tahoe-lafs.org/pipermail/tahoe-dev/2010-October/005353.html>

<sup>116</sup> Cindy Cohn (2014). *EFF Response to FBI Director Comey's Speech on Encryption*, Electronic Frontier Foundation. Retrieved February 6, 2015, from <https://www.eff.org/deeplinks/2014/10/eff-response-fbi-director-comeys-speech-encryption>

<sup>117</sup> Charlie Savage (2010). *U.S. Tries to Make It Easier to Wiretap the Internet*, New York Times. Retrieved February 6, 2015, from <http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all>

<sup>118</sup> See e.g. *Tor project*. Retrieved February 6, 2015, from <http://www.torproject.org/about/torusers.html.en>

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

## III. Conclusion

We respectfully recommend the Special Rapporteur:

- Reaffirm that every individual has the right to freedom of expression, which includes the right to speak, read, and communicate anonymously;
- Establish that anonymity must not be restricted *a priori* (including legal prohibitions on anonymous speech, anonymity tools, or businesses and service providers that provide anonymous services);
- Assert that strong anonymity—provided for by privacy-protective technology, private sector best practices, and robust legal safeguards—is vital to some of the core societal benefits of anonymity, including situations where powerful actors (including those wielding state power) might otherwise determine the identity of the speaker;
- Affirm that the compelled disclosure of anonymous speakers must only occur once a legally defined offense has been committed. And in all cases, the rights of an online speaker should be considered and respected by judicial process before identifying that individual in response to a request to do so;
- Recognize the freedom to use encryption technology and to publish and distribute encryption technologies and research;
- Reiterate the dangers of prohibitions on encryption and the mandatory inclusion of “back doors” in secure software and equipment;
- Recommend that Internet intermediaries should not block or limit the transmission of encrypted communications, and
- Recommend that Internet service providers be encouraged to design systems for end-to-end encryption.



