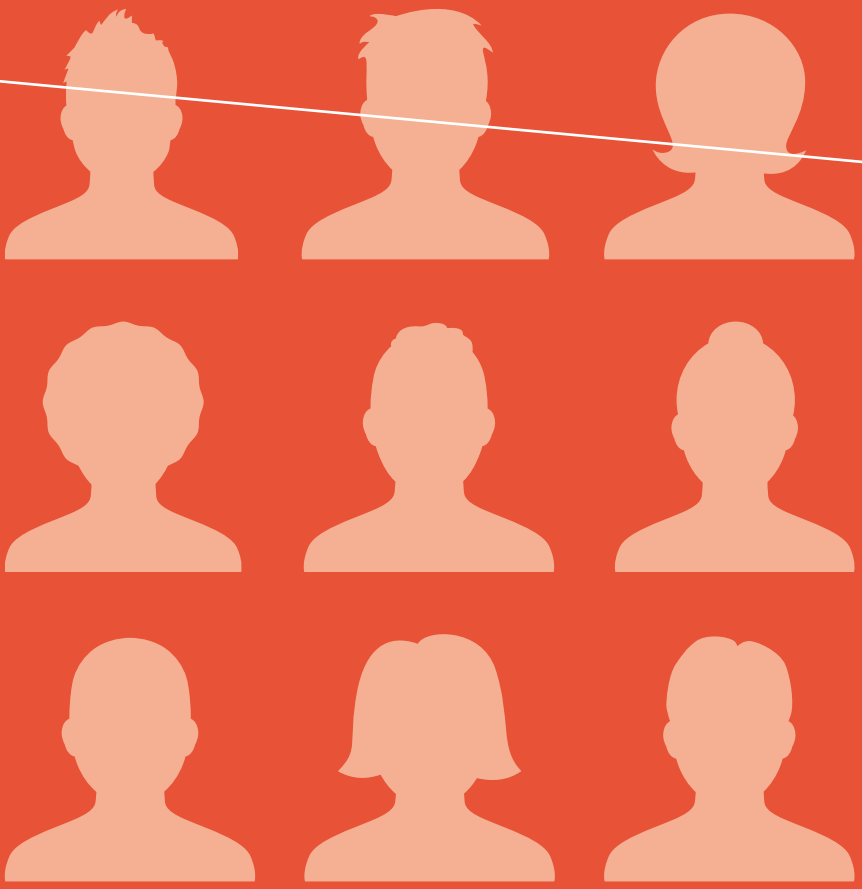
ARTICLE 19



Right to Online Anonymity

June 2015

Policy Brief

ARTICLE 19
Free Word Centre
60 Farringdon Road
London,
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-910793-15-2

The Principles were developed as a part of the Civic Space Initiative financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions here within expressed. ARTICLE 19 bears the sole responsibility for the content of the document.

Executive Summary

Anonymity and encryption are not new phenomena: anonymity has long facilitated the expression of controversial ideas and enabled dissent in many countries of the world; the use of ciphers and codes to protect the privacy of communications has an equally long history.

The protection of anonymity is a vital component in protecting both the right to freedom of expression and the right to privacy. Anonymity allows individuals to express themselves without fear of reprisal, and is especially important in those countries where freedom of expression is heavily censored. It enables whistleblowers to come forward and individuals to disclose their innermost concerns on a variety of issues in internet chat rooms. It also allows users simply to join in with all manner of discussions that they might otherwise avoid.

Governments around the world regularly attempt to restrict anonymity and the use of encryption tools for various reasons, from enabling unlawful activities to facilitating terrorism.

The protection of anonymity and encryption in international law is therefore more important than ever.

In this policy brief, originally developed as a contribution to the report on anonymity and encryption by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ARTICLE 19 seeks to outline the implications of anonymity and encryption for the right to freedom of expression in the digital age. We also identify the ways in which online anonymity and encryption are protected under international law and explore what restrictions to anonymity and encryption tools are compatible with the right to freedom of expression. We conclude with recommendations on how best to protect anonymity and encryption online.

Key recommendations

- States should explicitly recognise in their domestic legislation and practices that the right to freedom of expression includes the right to anonymity;
- States should also recognise the right to anonymous speech, the right to read anonymously, and the right to browse online anonymously;
- States should repeal those laws, regulations and policies requiring real-name registration which are in violation of the rights to freedom of expression and privacy;
- Social media platforms and news sites should not require real-name registration systems, ensuring at the very least that anonymity is a genuine option;
- States should adopt laws, regulations and policies that grant the power to remove the right to anonymity only to courts, rather than law enforcement agencies;
- Any restriction on anonymity and encryption must fully comply with the three-part test of restrictions to freedom of expression and should be subject to strong procedural safeguards;
- States and companies should promote the use of tools such as Tor and https:// protocols that allow encrypted browsing;
- States should recognise in their legislation and practices that encryption is a basic requirement for the protection of the confidentiality and security of information and that, as such, it is essential to the protection of the right to freedom of expression online;
- States should repeal laws or refrain from adopting laws requiring government authorisation for the use of encrypted products;
- States should repeal or refrain from adopting laws requiring the decryption of encrypted data or the disclosure of decryption keys in any circumstances other than by court order;
- States should refrain from adopting measures requiring or promoting technical backdoors to be installed in hardware and/or software encryption products;
- States should lift undue import/export restrictions to encryption hardware and software;
- States should abolish or refrain from adopting key escrow systems;
- Companies should refrain from weakening technical standards and should roll out the provision of services with strong end-to-end encryption;
- States and companies should put programmes in place for the promotion of encryption in internet communication;
- States and companies should promote end-to-end encryption as the basic standard for the protection of the right to privacy online. They should also promote the use of open source software and invest in it so that it is regularly and independently maintained and audited for vulnerabilities.

Table of contents

Introduction

Anonymity and encryption are not new phenomena. Anonymity has long facilitated the expression of controversial ideas and enabled dissent in many countries of the world; the use of ciphers and codes to protect the privacy of communications has an equally long history.

The protection of anonymity is a vital component in protecting both the right to freedom of expression and the right to privacy. Anonymity allows individuals to express themselves without fear of reprisals, and is especially important in those countries where freedom of expression is heavily censored. It enables whistleblowers to come forward and individuals to disclose their innermost concerns on a variety of issues in internet chat rooms. It also allows users simply to join in with all manner of discussions that they might otherwise avoid.

The flipside of anonymity, however, is that it may be used by ill-intentioned individuals to engage in criminal activity or other kinds of wrongdoing, such as online harassment or bullying.

Governments around the world regularly attempt to restrict anonymity and the use of encryption tools for various reasons. For example:

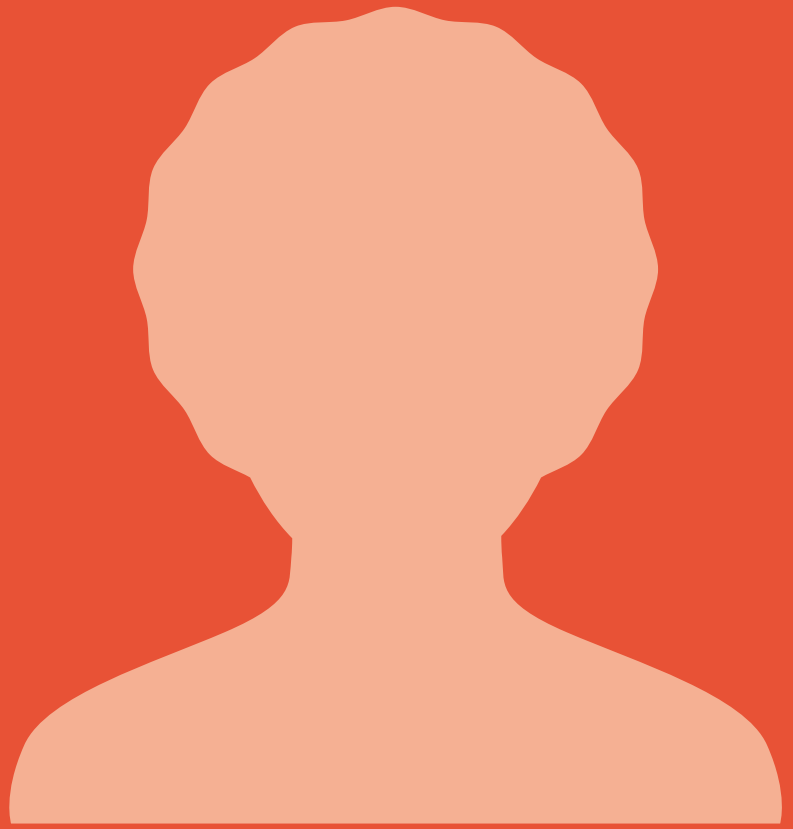
- In China, the government has blocked Virtual Private Networks (VPNs) that allow its citizens to bypass national firewalls.
- In the USA, anonymity has been lambasted as a tool which facilitates unlawful activity.[1]
- Following the *Charlie Hebdo* attacks in January 2015, several Western governments have called for measures that would severely curtail the use of both anonymity and encryption, measures which would – in turn - undermine the right to freedom of expression and privacy online. The UK Prime Minister David Cameron called for a crackdown on encryption,[2] while the French government is looking into ways to enhance surveillance on the internet.[3]

The protection given to anonymity and encryption in law and in practice is therefore more important than ever.

In May 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) released a groundbreaking report on online anonymity and encryption. The report made it clear that attempts by governments to gain backdoor access to people's communications or intentionally weaken encryption standards are a violation of international law. ARTICLE 19 submitted comments to the consultations for this report, and made recommendations about the implications of online anonymity and encryption for the right to freedom of expression in the digital age.[4]

In this policy brief, ARTICLE 19 expands on our original proposal prepared in response to the Special Rapporteur's report. We also identify the ways in which online anonymity and encryption are protected under international law and explore what restrictions to anonymity and encryption tools are compatible with the right to freedom of expression. We conclude by recommending how best to protect anonymity and encryption online.

Section I: Anonymity



Section I: Anonymity

General considerations

Anonymity is a key concept in the protection of freedom of expression as well as the right to privacy. At its simplest, anonymity is *the fact* of not being identified and, in this sense, it is part of the ordinary experience of most people on a daily basis, e.g. walking as part of a crowd or standing in a queue of strangers. In this way, an activity can be anonymous even though it is also public.

In certain contexts - notably voting by means of secret ballots, political speech,[5] artistic expression and the protection of journalistic sources[6] - anonymity has long been recognised as an important safeguard to protect the exercise of fundamental rights. With the rise of digital technologies, however, it has become clear that the importance of anonymity (including pseudonymity) cannot be restricted only to these spheres of activity. In this sense, anonymity not only protects the freedom of individuals to communicate information and ideas that they would otherwise be inhibited or prevented from expressing, but also protects the freedom of individuals to live their lives without unnecessary and undue scrutiny.

The right to online anonymity under international law

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data:

- In May 2015, the Special Rapporteur on FOE published his report on encryption and anonymity in the digital age. The report highlighted the following issues in particular:
  - The Special Rapporteur made it clear that an open and secure internet should be counted among the prerequisites for the enjoyment of freedom of expression today, and must therefore be protected by governments. Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[7]
  - The Special Rappreur highlighted that anonymous speech is necessary for human rights defenders, journalists, and protestors. He noted that any attempt to ban or intercept anonymous communications during protests was an unjustified restriction to the right to freedom of peaceful assembly under the *Universal Declaration of Human Rights* (UDHR) and the *International Covenant on Civil and Political Rights* (ICCPR).[8] He also recommended that legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications
  - He also stressed that restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law. The Special Rapporteur recommended that draft laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. He also emphasised that strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction;[9]

- The Special Rapporteur stated that blanket bans on the individual use of encryption technology disproportionately restrict the right to freedom of expression. He also noted that rules (a) requiring licenses for encryption use; (b) setting weak technical standards for encryption; and (c) controlling the import and export of encryption tools were tantamount to a blanket ban and therefore a disproportionate restriction to freedom of expression;[10]

- The Special Rapporteur also noted that governments' backdoor access to people's communications, key escrow systems (allowing potential third-party access to encryption keys), and the intentional weakening of encryption standards are disproportionate restrictions to the rights to freedom of expression and privacy. In particular, he highlighted that governments proposing backdoor access had not demonstrated that criminal or terrorist use of encryption serves as an insurmountable obstacle to law enforcement objectives. Under international law, states are required to demonstrate, publicly and transparently, that less intrusive means were unavailable or had failed, and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim. Key escrow systems were also deemed to be a threat to the the secure exercise of the right to freedom of expression because of the vulnerabilities inherent in third parties being trusted to keep encryption keys secure, or being required to hand them over to others;[11]

- The Special Rapporteur also found that blanket prohibitions on anonymity online and compulsory real-name or SIM card registration go well beyond what is permissible under international law; he noted that because anonymity facilitates opinion and expression in significant ways online, states should protect it and, in general, not restrict the technologies that make it possible.[12]

- The report further acknowledges the role of corporate actors in protecting and promoting strong encryption standards. In particular, companies are invited to consider how their own policies restrict encryption and anonymity.

- The 2013 report of the Special Rapporteur on FOE highlighted the important relationship between the rights to privacy and freedom of expression in cyberspace.[13] The report also observed that restrictions to anonymity facilitate states' communications surveillance and have a chilling effect on the free expression of information and ideas.[14]

- Several instruments to have emerged in this area came originally from the Council of Europe and the European Union.[15] For example, the Committee of Ministers of the Council of Europe adopted the *Declaration on freedom of communication on the Internet* in May 2003. Principle 7 on anonymity provides that:

  > 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. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.16

- In its jurisprudence, the European Court of Human Rights (European Court) has recognised the importance of anonymity to the rights to freedom of expression and privacy. At the same time, the Court has been clear that anonymity is not absolute and may be limited for the protection of other legitimate interests, especially the protection of vulnerable groups. Specifically, it stated that anonymity and confidentiality on the internet must not lead states to refuse to protect the rights of potential victims, especially where vulnerable people are concerned:[17]

  > Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.[18]

The European Court expressed a similar view in the case of *Delfi v Estonia*[19] when it noted that it was:

> [M]indful, in this context, of the importance of the wishes of Internet users not to disclose their identity in exercising their freedom of expression. At the same time, the spread of the Internet and the possibility – or for some purposes the danger – that information once made public will remain public and circulate forever, calls for caution.

The European Court took the view that by allowing comments by non-registered users, an online news platform must have assumed a certain responsibility for these comments. This aspect of the decision of the European Court has attracted widespread criticism, as many fear this could lead to the end of user-generated comments or the adoption of real-name registration policies and laws across the Council of Europe region.[20] A review of the decision is pending before the Grand Chamber as of May 2015.

– The relationship between anonymity and the right to freedom of expression was further highlighted in a more recent report published by the Inter-American Commission on Human Rights (IACHR) in 2013, *Freedom of Expression and the Internet*.[21] Among other things, the IACHR recommended that anonymous platforms should be promoted and the use of authentication services used proportionately.[22]

Anonymity in practice

Given the limited nature of the legal protection of anonymity, many users have turned to technical methods to achieve anonymity online. In practice, several initiatives have developed that allow internet users to maintain their anonymity online.[23] These include the Tor browser, which hides the IP address of internet users when browsing online,[24] and the https:// protocol, which encrypts communications with some websites.[25] However, even these technical tools have been restricted by law in some countries.

Section II: Encryption

Section II: Encryption

General considerations

Encryption has been defined as:

> The process of encoding or 'scrambling' the content of any data or voice communication with an algorithm and a randomly selected variable associated with the algorithm, known as a 'key'.[26]

Encryption means that information can only be decrypted by the intended recipient of the communication who holds the key. In most cases, the key is essentially "a string of numbers; the longer the key, the stronger the security."[27]

Encryption can be used to protect data in transit or in storage and includes emails, files, disks and internet connections. However, although encryption generally protects the confidentiality of the message or content data, it does not necessarily hide the IP addresses of either the sender or the recipient (metadata) *vis-a-vis* third parties, although IP addresses may also be hidden using other technologies such as the TOR browser. In this sense, encryption alone does not guarantee anonymity since internet users remain traceable and therefore potentially identifiable.

Equally, encryption can be used to verify the authenticity and integrity of communications, e.g. through the use of digital signatures. A digital signature is "a cryptographically based assurance that a particular document was created or transmitted by a given person."[28] Digital signatures are sometimes certified by a 'Trusted Third Party' ('TTP'), which may be a certification authority (CA) that issues digital certificates. In practice, however, TTPs are only as trustworthy as their weakest link. For this reason, end-to-end encryption mechanisms are generally preferable since they allow a user to verify directly the identity claimed by another user, without any need for a TTP, who then cannot access the data relating to the communication. In other words, end-to-end encryption is a more secure form of encryption.

Encryption as a prerequisite for secure communications online

Encryption is a fundamental feature of the internet. Without the authentication techniques derived from encryption, secure online transactions would be impossible. Without encryption itself, the electronic communications of every individual, as well as every private company and government agency, would be open to inspection and abuse. For this reason, encryption is used on a daily basis for information and activities such as online banking, privileged lawyer-client communication, medical data, tax records, and major infrastructure such as electric grids or power plants. It is particularly important for human rights defenders, whistleblowers, journalists and activists who are often the subject of surveillance by intelligence or law enforcement agencies.

Encryption is closely related to cyber security, which is generally concerned with the development of technical standards, including encryption, to protect information systems. In this sense, cyber security is related to but distinct from cybercrime, which has traditionally been used to describe offences committed by anyone unlawfully interfering with information systems.[29] Most countries have adopted cybercrime legislation that seeks to criminalise illegitimate access to or interference with computer or information systems.[30] A significant problem with cybercrime legislation, however, is that it tends to provide for content-based offences, such as online defamation or blasphemy. Examples of such legislation can be found in a number of countries including Pakistan, Kenya and Bangladesh.

Encryption under international law

Internationally, the protection of a 'right to encryption' has so far been limited. It has traditionally been linked to the protection of the right to privacy and personal data rather than freedom of expression.

- A key instrument in this regard is the 2015 report of the Special Rapporteur on FOE, outlined in the previous section. Moreover, in his 2013 report, the Special Rapporteur on FOE first established the relationship between freedom of expression, encryption and anonymous communications.[33]

- The 1997 Organisation for Economic Co-operation and Development (OECD) *Guidelines on Cryptography Policy* identify key issues for its member states to consider when adopting cryptography policies, both nationally and internationally. In particular, the OECD recommended the following basic principles:[34]

  1) Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems;[35]

  2) Users should have a right to choose any cryptographic method, subject to applicable law;

  3) Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments;

  4) Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at national and international level;

  5) The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods;

  6) National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible;

  7) Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated;

  8) Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

In its explanatory report, the OECD noted the fundamental importance of cryptography to the protection of the right to privacy and information security:

> The respect of privacy and the confidentiality of personal information are important values in a democratic society. However, privacy is now at greater risk because in the emerging information and communications infrastructure neither open networks, nor many types of private networks, were designed with confidentiality of communications and storage of data in mind. However, cryptography forms the basis for a new generation of privacy enhancing technologies. The use of effective cryptography in a network environment can help protect the privacy of personal information and the secrecy of confidential information. The failure to use cryptography in an environment where data is not completely secure can put a number of interests at risk, including public safety and national security. In some cases, such as where national law calls for maintaining the confidentiality of data, or protecting critical infrastructures, governments may require the use of cryptography of a minimum strength.[36]

- The Inter-American Commission on Human Rights made recommendations regarding the protection of anonymous communications and encryption tools on it's report on *Freedom of Expression and the Internet 2013*, where it stated that:

  > The prohibition of the use of circumvention tools to legitimately protect the right to anonymous communication or for the legitimate use of a person's property shall not be considered a legitimate copyright protection measure.

- In 2012, the Committee of Ministers of the Council of Europe (COE) recommended that COE member states engage with the private sector to:

  > Ensure that the most appropriate security measures are applied to protect personal data against unlawful access by third parties. This should include measures for the end-to-end encryption of communication between the user and the social networking services website.[37]

– The 2015 report of the Parliamentary Assembly of the Council of Europe (PACE) on mass surveillance strongly condemned the National Security Agency (NSA)'s efforts to weaken encryption standards and the use of backdoors. The report concluded that:

> The creation of "backdoors" or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited; all institutions and businesses holding personal data should be held to apply the most effective security measures available.[38]

Encryption is also relevant to other rights, including the right to avoid self-incrimination and the right to a fair trial. Measures such as the compulsory handover of decryption keys may impinge on the right to avoid self-incrimination.

The jurisprudence of the European Court and some domestic courts establishes that the right against self-incrimination is not absolute[39] and that it may only be brought into play as the result of an act of testimony, as opposed to the production of pre-existing documents or materials.[40] There are significant differences in the approach of the courts, however, when it comes to the question of whether decryption keys are more analogous to physical keys[41] (pre-existing material) as opposed to a safe code (testimonial).[42] Although the European Court has yet to rule specifically on the compulsory handover of decryption keys, current jurisprudence indicates that the European Court would focus on the question of whether the trial as a whole was fair, with regard to any public interest in the investigation and prosecution of the crime at issue, the nature and degree of the compulsion, the type of information sought and how it was used in court.[43]

Finally, encryption has chiefly been governed by international agreements concerning the regulation of the import/export of dual-use technology goods, such as the *Wassenaar Arrangement*.[44]

Moreover, the Internet Engineering Task Force (IETF) have repeatedly emphasised the importance of encryption and recommended that it should be encouraged and available for all.[45] In the 2014 statement, the IETF also made clear that "the use of encryption defends against pervasive monitoring and other passive attacks."[46]

Section III: Restrictions on Anonymity and Encryption

Section III: Restrictions on Anonymity and Encryption

Anonymity

Given the vast amount of information collected by both private companies and public bodies about our lives, it is obvious that the rights to privacy, freedom of expression and anonymity online must now be more strongly and consistently protected than ever before. To begin with, the right to anonymity should be expressly recognised as a key component of the right to freedom of expression.

ARTICLE 19's position
In ARTICLE 19's view, for the right to freedom of expression to be meaningful in the digital age, it must necessarily contain the right to anonymity, including the right to anonymous speech, the right to read anonymously, and the right to browse online anonymously.

This is consistent with the best practice established in several countries[47] where the right to anonymous speech, the right to read anonymously and, more generally, the right to online anonymity have been recognised. It is also in line with the purpose of data protection law, which seeks to protect individuals from being identified as a result of personal data processing by automated computer systems.

Furthermore, any restriction to anonymity should comply with the three-part test under Article 19 (3) of the *International Covenant on Civil and Political Rights* (ICCPR), namely that it should:

- Be prescribed by the law: restrictions have to be precise and clearly stipulated in accordance with the principle of the rule of law. This means that vague or broadly worded restrictions, or restrictions that leave excessive discretion to executive authorities, are incompatible with the right to freedom of expression;

- Pursue a legitimate aim, as explicitly enumerated in Article 19 para 3 of the ICCPR, namely respect of the rights or reputations of others, and the protection of national security or public order (*ordre public*), public health or morals. The list of aims is an exhaustive one and thus any interference which does not pursue one of those aims violates Article 19;

- Be necessary and proportionate to aims pursued.[48] The word "necessary" means that there must be a "pressing social need" for the interference;[49] that the reasons given by the state to justify the interference must be "relevant and sufficient" and that the state must demonstrate that the interference is proportionate to the aim pursued.[50]

In the following sections, ARTICLE 19 outlines the main types of restrictions that arise in the context of anonymity online, along with the approach that we consider to be appropriate for such restrictions.

ARTICLE 19's recommendations:
- States should explicitly recognise in their domestic legislation and practices that the right to freedom of expression includes the right to anonymity;

- States should also explicitly recognise the right to anonymous speech, the right to read anonymously, and the right to browse online anonymously.

Real-name registration

Real-name registration laws have recently been adopted or considered in several countries.[51] They usually enable local law enforcement agencies to track internet users more easily. ARTICLE 19 finds that these laws are a particularly blunt interference with the rights to freedom of expression and privacy online. These laws are usually coupled with requirements that internet users identify themselves in cybercafés, and obligations for cybercafé owners to track and log the online activities of customers.[52]

ARTICLE 19's position

In ARTICLE 19's view, mandatory real-name registration systems go well beyond what is permissible under international human rights law and should be abolished:[53]

- As noted earlier, anonymity has been key in facilitating freedom of expression online. It is an intrinsic part of the culture and function of the internet. It has enabled people to express controversial opinions that they might not otherwise have shared in the offline world. Mandatory real-name registration schemes have a chilling effect on freedom of expression as individuals feel afraid to exercise their right to freedom of expression. For example, they might be less likely to come forward with embarrassing information about powerful individuals for fear of costly litigation or punishment.

- Real-name registration systems also encourage the collection of information which could easily be abused by the authorities and become a tool of repression, leading to the persecution and harassment of individuals on the basis of their expression. In many countries, criticising the government is illegal and only the anonymous posting of such information online can ensure that those who post it are not at risk of reprisal.[54]

- The requirements of real-name registration are ineffective in practice, as individuals can always use other technical means and security tools like en-cryption, VPNs, or anonymous internet navigation to preserve their anonymity.

- Anonymity is not limited to the internet and still exists in 'real life'. For example, individuals may send anonymous letters, make anonymous phone calls, or distribute leaflets and other publications anonymously. Although the internet makes it much easier and less expensive to reach large numbers of people, any requirement for real-name identification would restrict internet communication more than many other everyday forms of communication (e.g. postal services are not required to authenticate the return addresses of letters with harmful content; real-name identification is also not required for telephone calls.)

Equally, ARTICLE 19 believes that, as a general principle, social media platforms and news sites should not require the use of real-name registration systems.

- Although companies are not bound by the requirements of international human rights law as a matter of strict legal form, ARTICLE 19 believes that they nonetheless have a duty to respect human rights in line with the *Ruggie Principles on Business & Human Rights*.[55]

- The use of real-name registration by social media platforms and news sites as a prerequisite to using their services can have a negative impact on the rights to privacy and freedom of expression, particularly for minority or vulnerable groups, who might be prevented from asserting their sense of identity.[56]

- Whilst real-name policies are usually presented as an effective tool against internet trolling, fostering a culture of mutual respect between internet users, the disadvantages of real-name policies outweigh their benefits. In particular, anonymity is vital to protect children, victims of crime, individuals from minority groups and other vulnerable groups from being targeted by criminals or other malevolent third parties who may abuse real-name policies. In this sense, anonymity is as much about online safety as self-expression.

– Real-name registration or a requirement to provide identification of some sort (when registering with a service, such as an email account) also raises serious concerns over data protection, given that many such systems require users to provide a considerable amount of sensitive personal data as a means to verify their identity.[57]

ARTICLE 19's recommendations:

– States should repeal laws, regulations and policies requiring real-name registration that violate the rights to freedom of expression and privacy.

– Social media platforms and news sites should not require the use of real-name registration systems. At the very least, internet companies should ensure anonymity remains a genuine option.

Access to personal data and disclosure of identity

Access by law enforcement

In most countries, real-name registration laws are not necessary, given that law enforcement agencies already have the power to require the disclosure of the identity of anonymous internet users.[58]

ARTICLE 19's position

ARTICLE 19 recognises that online anonymity is not absolute and may be lifted in certain limited circumstances, in strict compliance with the international standards on freedom of expression under the three-part test outlined above. Any such lifting of anonymity should be subject to strong procedural safeguards. In particular, as a matter of principle, the mandatory disclosure of an individual's online identity should only be ordered by the courts, which are best placed to properly balance the right to anonymous expression with other interests.[59]

Moreover, there should be a higher threshold if the individual in question is engaged in journalistic activity. In such a situation, the court would have to examine the impact on the right to freedom of expression and whether there was a higher public interest in disclosure.

Law enforcement agencies should only have the power to access individuals' personal data without a court order in cases of emergency, for example because of an imminent and specific risk of harm to a particular individual.

Access by third parties

ARTICLE 19 also recognises that anonymity may be legitimately lifted for the purpose of bringing civil proceedings (such as defamation or other private actions), but this must be subject to strong procedural safeguards.

ARTICLE 19's position
In this respect, ARTICLE 19 highlights that as a matter of principle, the courts are best placed to properly balance the right to anonymous expression with other interests and to therefore order the mandatory disclosure of an individual's online identity if necessary. This is consistent with best practice in countries where the courts have recognised that anonymity could be lifted in specific cases, subject to the careful scrutiny of the courts.[60] In cases of defamation, for example, this requires that a number of conditions be fulfilled, including notice to the anonymous poster, details of the allegedly defamatory statements, evidence of a *prima facie* case against the anonymous poster, and the balance between the right to anonymous speech and the prima facie case, taking into account the need for disclosure of identity in order for the case to proceed.[61]

Other measures

ARTICLE 19 opposes measures that limit anonymous speech by encouraging internet intermediaries to remove content posted by anonymous, rather than identifiable, speakers lest they expose themselves to liability.[62] In our view, such measures have a chilling effect on freedom of expression and should not be adopted.

Equally, internet filters that would enable copyright holders to track internet users who use peer-to-peer networks and other file-sharing sites in relative anonymity (e.g. using proxies or VPNs) are incompatible with the rights to freedom of expression and privacy and should be prohibited.[63]

ARTICLE 19's recommendations:

- States should adopt laws, regulations and policies that grant powers to order the lifting of anonymity only to the courts - rather than to law enforcement agencies;
- Any restriction on anonymity must fully comply with the three-part test for restrictions to freedom of expression and should be subject to strong procedural safeguards;
- States and companies should promote the use of tools such as Tor and https:// protocols that allow encrypted browsing.

Encryption

Encryption is essential to ensuring the security of information, the integrity of communications and the right to privacy online. It is also a vital tool for the protection of freedom of expression on the internet as well as the circumvention of surveillance and censorship. As noted in the Report of the Special Rapporteur on FOE, weak encryption standards or backdoors - whether mandatory or otherwise - undermine people's trust in the internet and constitute a serious interference with fundamental rights.

Restrictions on the use of cryptography (including encryption) come in many different shapes and forms. Generally speaking, they can be divided into the following different types.

Restrictions imposed on end-users

A number of governments provide for outright bans or significant restrictions on the use of encryption by end-users (e.g. China,[64] India,[65] Senegal,[66] Egypt[67] or Pakistan[68]).

ARTICLE 19's position
ARTICLE 19 believes that restrictions to the use of encrypted products by users are a clear violation of the right to privacy and freedom of expression. As noted earlier, encryption is vital to protect the confidentiality of communications and personal data. Prohibiting the use of encryption is akin to preventing individuals from putting locks on their doors or curtains on their windows. As such, it is a disproportionate restriction to the rights to privacy and free expression and can never be justified.

In ARTICLE 19's view, any interference with encryption standards must strictly comply with the three-part test under Article 19 (3) of the ICCPR. This means that any restriction to encryption must be prescribed by law, pursue a legitimate aim and be necessary and proportionate to that aim. In the first instance, the necessity of any such measures must be assessed by referring to the broad range of surveillance powers already available to intelligence agencies and law enforcement bodies, powers which have already been widely criticised as both unnecessary and overbroad.[69]

ARTICLE 19's recommendations:

- States should recognise in their legislation and practices that encryption is a basic requirement for the protection of the confidentiality of information and its security and that, as such, it is essential for the protection of the right to freedom of expression online;

- Any restrictions to encryption must comply strictly with the three-part test under Article 19 (3) of the ICCPR and be subject to procedural guarantees under due process;

- States should repeal or refrain from adopting laws requiring government authorisation for the use of encrypted products;

- States should repeal or refrain from adopting laws requiring the decryption of encrypted data or the disclosure of decryption keys in any circumstances other than by court order.

Mandatory technical requirements

Several governments also seek to assert control over information systems by giving a government agency, usually linked to the Ministry of Defence, Ministry of Interior or Ministry of Transport, overall authority to review and approve all standards, techniques, systems and equipment (e.g. India,[70] China[71] and Egypt[72]).

ARTICLE 19's position

ARTICLE 19 considers that measures such as technical specifications mandated by governments in order to weaken encryption standards, along with the installation of backdoors compromising the integrity of private communications software, are disproportionate and, as such, incapable of justification under international law. In ARTICLE 19's view:

- Such measures are equivalent to requiring locksmiths to produce weak door locks and deadbolts in order to facilitate governments' access to private homes. Such intrusion of privacy is both unacceptable and dangerous;

- Far from making it easier for law enforcement to catch criminals, the adoption of weak encryption standards is instead more likely to facilitate increased criminal activity;

- Moreover, given the growing frequency and severity of cyber-attacks at both national and international level, it is seriously doubtful that weakening encryption standards could ever be a proportionate response.

ARTICLE 19's recommendations:

- States should refrain from adopting measures requiring or promoting technical backdoors to be installed in hardware and/or software encryption products.

Import/export controls

Governments have also sought to exert control over encryption through import/export controls. In particular, governments have traditionally been reluctant to export strong encryption products for fear that this might undermine the capabilities of their intelligence agencies to spy on foreign targets. Yet the international market demands strong encryption. In the past these divergent interests have been used by governments to influence domestic policy. For instance, the USA used rules on export controls as a bargaining chip to pressurise hardware and software manufacturers into adopting weaker encryption products or the key escrow system at home.[73]

With the internet however, these controls have largely been relaxed.[74] Nonetheless, it appears that several countries (e.g. France[75] and Senegal[76]) retain export controls over certain categories of hardware and software that enable encryption. This usually concerns products other than those that guarantee authentication or the protection of the integrity of information systems, as well as dual-use goods. Moreover, the export of some categories of encryption products, particularly those with military use, remain affected to some extent by the Wassenaar Arrangement (see above).

Finally, some countries (e.g. China[77] and Ethiopia), continue to impose significant restrictions on the import of any computer programmes or equipment that permit cryptography. This is because governments are generally wary of importing products that might have backdoors installed or because the governments wish to retain their domestic surveillance capabilities.[78]

ARTICLE 19's position
ARTICLE 19 believes that the application of import/export controls to encryption products is a disproportionate restriction to the rights to freedom of expression and privacy. Such measures pose a serious threat to the confidentiality of users' communications by making them more vulnerable to domestic or foreign surveillance. In countries where it is an offence to criticise government policies and officials, this exposes journalists, human rights defenders, activists or other vulnerable groups to further risk of reprisals.

ARTICLE 19's recommendations:
– States should lift undue import/export restrictions from encryption hardware and software.

The key escrow or trusted party system
In a key escrow system, long encryption keys are permitted but users are required to store their keys with government agencies or a 'trusted third party" (usually authorised by the government or with government ties).[79]

Although efforts to have a key escrow system adopted internationally have been unsuccessful, key escrow systems are currently in place in several countries (e.g. India and Spain[80]).

ARTICLE 19's position
ARTICLE 19 believes that key escrow systems are a disproportionate restriction to the rights to privacy and freedom of expression. Key escrow systems are equivalent to giving government the keys to a person's house. While variations on the key escrow system with court authorisation may seem appealing, such systems are expensive to implement and also provide ultimately weak protection of privacy since protection is only as strong as its weakest link. The more entities and individuals that are involved, the more likely they are to be subject to indirect pressure by government and others.

ARTICLE 19's recommendations:
– States should abolish or refrain from adopting key escrow systems.

Mandatory disclosure of encryption keys
In some countries, as an alternative to key escrow systems, law enforcement agencies or courts can require the disclosure of encryption keys, or order the decryption of encrypted data from a person who is suspected of committing a crime or, in some countries, a third party. Failure to comply is usually a criminal offence, which is punishable by imprisonment and/or a fine.[81]

ARTICLE 19's position
Given that law enforcement bodies or intelligence agencies may, in an exceptional case, require the power to order the disclosure of a relevant key or decryption of communications, ARTICLE 19 considers that the least intrusive means would be to require the respective body to obtain a court order requiring the individual in question to provide the agency with the information in decrypted format.

In ARTICLE 19's view, the disclosure of a decryption key would almost inevitably entail a disproportionate restriction to the right to privacy since the key would potentially reveal private information well beyond the intended purpose for the mandatory disclosure of the key.

While decryption orders may be permissible in exceptional cases, no court should make such an order unless it is satisfied that the interference with the individual's rights to privacy and free expression is both necessary in the circumstances and proportionate. Law enforcement agencies should be required to establish that the individual in question is reasonably suspected of involvement in serious criminality. Furthermore, a court should only grant the order for specific communications rather than for all encrypted files on a computer.

In making a decryption order, the court should address itself to the question of whether the use of such compulsory powers would be in violation of the right to avoid self-incrimination, i.e. that the use of the material obtained as a result of the exercise of such powers would have an adverse effect on the fairness of subsequent criminal proceedings.

Finally, in order to ensure that any mandatory powers to decrypt communications are not abused, any such decryption should only take place in the presence of an independent lawyer or data protection authority.

In all cases, trial judges should exercise their discretion in excluding evidence obtained as a result of these compulsory powers to require the disclosure of encryption keys or the decryption of information if the admission of such evidence would have an adverse effect on the fairness of the proceedings. In particular, should decrypted information be obtained unlawfully and in breach of the right to privacy, trial judges should, in our view, rule that the information obtained as a result of the disclosure is inadmissible.

However, if the order has been made lawfully and the person refuses to comply with the order, they may be subject to the appropriate sanctions for contempt of court. At the same time, if the failure to disclose encryption keys is criminalised, ARTICLE 19 believes that any such offence should, as a minimum, acknowledge defences such as lack of knowledge or possession of the key.

Other surveillance powers

It should be noted that in circumstances where law enforcement and intelligence agencies have been unable to obtain greater powers to either crack encryption or seek the disclosure of encryption keys, they have generally asked for other surveillance powers.[82]

ARTICLE 19's position

ARTICLE 19 believes that the use of hacking by government officials is, in general, a clear violation of the rights to privacy and free expression, given that it involves access to private information without permission or notification, and is in breach of the integrity of the target's own security measures. Unlike search warrants where the individual would at least be notified that their home or office was being searched, hacking generally takes place without a person's knowledge. It is the equivalent of the police breaking into someone's home.

Given the obvious intrusiveness of such a measure, it should only be authorised by a judge in the most exceptional circumstances and must be subject to strict conditions. In particular, hacking should only be available for the most serious offences and as a last resort, once other, less intrusive methods have already been exhausted.

ARTICLE 19's recommendations:

- Companies should refrain from weakening technical standards and should roll out the provision of services with strong end-to-end encryption;
- States and companies should put programmes in place to promote encryption in internet communications;
- States and companies should promote end-to-end encryption as the basic standard for the protection of the right to privacy online. They should also promote the use of open source software and invest in open source software to ensure that it is regularly and independently maintained and audited for vulnerabilities.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at international and regional level, and for their implementation in domestic legal systems. ARTICLE 19 has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information, and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes each year a number of legal analyses, and comments on legislative proposals and existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our legal materials available at **http://www.article19.org/resources.php/legal**.

If you would like to discuss this policy brief further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at **legal@article19.org**.

This policy brief is wholly financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions herein expressed. ARTICLE 19 bears the sole responsibility for the content of the document.

References

1. See, for example, A Report of the US President's Working Group on Unlawful Conduct on the Internet ***The electronic frontier: the challenge of unlawful conduct involving the use of the Internet***, March 2001; which states "[i]ndividuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections."

2. See ARTICLE 19 ***Crackdown on End-to-End Encryption Threatens Free Expression and the Right to Privacy***, January 2015.

3. Numerama, Manuel Valls annonce une surveillance renforcée sur Internet, 21 janvier 2015

4. See, ARTICLE 19, **ARTICLE 19 to UN Watchdog: Online Anonymity and Encryption Must Be Protected**, contribution to the UN Special Rapporteur on Freedom of Expression's call for comments on anonymity and encryption to his 2015 thematic report to the Human Rights Council, February 2015.

5. E.g. Lord Neuberger, the President of the UK Supreme Court, What's in a name? Privacy and anonymous speech on the Internet, 30 September 2014; Lord Neuberger noted that the real identity of Junius, a famous English anonymous political writer in the late 18thC, remained unknown to this day.

6. See Human Rights Committee, **General Comment no. 34**, para. 45; the 2008 Joint Declaration on defamation of religions, and anti-terrorism and anti-extremism legislation; ***Goodwin v. the United Kingdom***, [GC], no. 17488/90, para.39, 27 March 1996; African Commission on Human and Peoples' Rights (ACHPR), **ACHPR /Res.62(XXXII)02** (2002); OAS, ***Report on Terrorism and Human Rights***, OEA/Ser.L/V/II.1 16 Doc. 5 rev. 1 corr. (Oct. 22, 2002).

7. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye**, A/HRC/29/32, 29 May 2015 (the 2015 Report of the SR on FOE), paras 12,16 and 56.

8. *Ibid.*, para 53.

9. *Ibid.*, paras 31-35.

10. *Ibid.*, paras 40-41.

11. *Ibid.*, paras 36, 42-44.

12. *Ibid.*, paras 49-51.

13. UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, 17 April 2013 (the 2013 Report of the SR on FOE), para 47.

14. *Ibid.*, paras 48-49.

15. For instance, in **Recommendation No.R (99)5 for the Protection of Privacy on the Internet (1999)**, the Committee of Ministers of the Council of Europe noted that there was a "need to develop techniques which permit the anonymity of data subjects and the confidentiality of the information exchanged on information highways while respecting the rights and freedoms of others and the values of a democratic society."

16. *Ibid.*

17. European Court, *K.U. v Finland*, Appl. No.2872/02, 2 December 2008, para. 49. The European Court found that Finland violated the right to private life because it had failed to put in place a legislative framework that would allow the courts or law enforcement agencies to require the disclosure of the identity of ISPs customers for the purposes of criminal investigation.

18. European Court, **Internet: Case-law of the European Court of Human Rights**, 2011.

19. European Court, ***Delfi v Estonia***, App. No.64569/09, 10 October 2013.

20. See Access, **Access intervenes for the right to be anonymous online**, June 2014.

21. Special Rapporteur on FOE for the OAS, **Freedom of Expression and the Internet**, 31 December 2013.

22. *Ibid.* paras 23; and paras. 133-137.

23. For an overview of these initiatives, see **UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012**, pp. 24-26.

24. For more information about TOR, see EFF, **7 Things You Should Know About TOR**, July 2014

25. See EFF's initiative, HTTPS everywhere: **https://www.eff.org/HTTPS-EVERYWHERE**; https// protects the confidentiality of communications, it does not provide anonymity as such.

26. D. Banisar, *Stopping Science: the Case of Cryptography, Health Matrix*, Vol 9:253, 1999. For the purposes of this paper, 'encryption' refers to electronic encryption. However, the same general principles apply to analogue forms of encryption also.

27. *Ibid.* Other forms of keys can include passwords and even biometrics such as fingerprints.
28. *Ibid.*

29. This in itself raises a series of other issues, which go beyond the scope of the present paper. Suffice to note that computer offences can prevent security research depending on how these offences are drafted.

30. See in particular the Council of Europe Cybercrime Convention, 2001.

31. ARTICLE 19, **Legal Analysis of Kenya Cybercrime and Computer-Related Crimes Bill 2014** (pending).

32. International Commission of Jurists, **Bangladesh: Information Communication Technology Act Draconian Assault on Free Expression**, 20 November 2013.

33. The 2013 Report of the SR on FOE, *op.cit.* paras 89 and 92.

34. The full recommendation is available from **here**.

35. The report is available from **here**.

36. See Inter-American Commission on Human Rights, *op. cit.* para. 83.

37. See **Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services**, 2012

38. See PACE, Committee on Legal Affairs and Human Rights, **Report on Mass Surveillance**, AS/Jur (2015) 01, 26 January 2015.

39. European Court, *Murray v. the UK*, (1996) 22 EHRR 29, at para. 45; Stott v Brown, [2000] UKPC D3; *Doe v. United States,* 487 U.S. 201, 219.

40. European Court, *Saunders v UK*, App.No. 19187/91, [GC], 17 December 1996; USA, *Fisher v US*, 425 US 391.

41. In the UK, encryption keys are generally regarded as physical keys, see R v S &A [2008] EWCA Crim 2177

42. In the US, the mandatory disclosure of encryption keys is generally regarded as testimony subject to a number of exceptions, see *inter alia, Doe v. United States*, 487 U.S. 201, 219 Justice Stevens dissenting.

43. *Ibid.*

44. The **Wassenaar Arrangement**; See also Regulation (EC) No 428/2009, which governs the EU export control regime

45. See IETF, **RFC 1984** of 1996, **RFC 2804** of 2000 or **RFC 3365** of 2002.

46. See IETF, **RFC 7435** of December 2014.

47. See, US Supreme Court, ***Talley v. California***, 362 U.S. 60 (1960); US Supreme Court, ***McIntyre v Ohio Elections Commission***, 514 U.S. 334 (1995), US Supreme Court, ***United States v Rumely*, 345 US 41, 57**; *John Doe v 2theMart.com Inc.* 140 F Supp 2d 1088 (2001); see also Supreme Court of Canada, ***R v Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212**.

48. E.g. *Rafael Marques de Morais v. Angola, Communication* No. 1128/2002, 18 April 2005, para. 6.8

49. E.g., *Hrico v. Slovakia*, 27 July 2004, Application No. 41498/99, para. 40.

50. See, e.g. HR Committee, *Rafael Marques de Morais v. Angola*, para 6.8.The HR Committee has stated that "the requirement of necessity implies an element of proportionality, in the sense that the scope of the restriction imposed on freedom of expression must be proportional to the value which the restriction serves to protect.

51. E.g. in China, see Reuters, **China to ban online impersonation accounts, enforce real-name registration**, 4 February 2015; or in Russia where bloggers in "3,000 visitors" category must register with the state media regulation agency, using real names and personal details. If they fail to do this, the regulators may instruct providers or administrators of relevant sites to provide the names and contacts to the authorities. Failure to register or to provide contact information is punishable by administrative fines: see HRW, **Russia: Veto Law to Restrict Online Freedom**, May 2014.

52. For example in Iran, see Freedom House, **Freedom on the Net report 2014, Iran country report**; or in Vietnam, see Freedom House, Freedom on the Net report 2014, Vietnam country report.

53. See ARTICLE 19, **Right to Blog** (2013) at pp. 17-18.

54. *C.f.*, **Recommendation CM/Rec (2011)7 on the new notion of media states** that "arrangements may be needed to authorise the use of pseudonyms (for example in social networks) in cases where disclosure of identity might attract retaliation (for example as a consequence of political or human rights activism)."

55. The **Guiding Principles on Business and Human Rights**, Office of the UN High Commissioner for Human Rights, 2011.

56. For example, members of the queer community such as The Sisters of Perpetual Indulgence have protested that Facebook's real-name policy denies them the ability to assert their sense of identity. See Huffington Post, ***Facebook Still Forcing LGBT People and Others to 'Authenticate' their Identities***, 27 March 2015; for recommendations on best practices, see K.A. Heatherly, A. L. Fargo & J.A. Martin, Anonymous Online Comments: the Law and Best Media Practices from Around the World, October 2014, p. 14.

57. See Facebook, **What type of ID does Facebook accept?**

58. This is the case, for instance, in countries as varied as Vietnam, see Freedom House, Vietnam country report, op.cit.; or the UK, see Ss 21 and 22 of the Regulation of Investigatory Powers Act 2000.

59. This is the case, for instance, in countries such as France, see The Verge, **Twitter Must Disclose Authors of Anti-Semitic Tweets, French Appeals Court Rules**, June 2013; Canada, see e.g. See **R v Spencer 2014 SCC 43** in which the Canadian Supreme Court held that a warrant was required for ISPs to disclose subscriber information in an investigation concerning child pornography; or the US, see F**reedom House, *Freedom on the Net report 2014*, US country report**.

60. See e.g. USA, *Dendrite International Inc v John Doe* 775 A 2s 758 (2000).

61. *Ibid*. See also in the UK, *mith v ADVFN Ltd* [2008] EWHC 1797 (QB), *Sheffield Wednesday v Hargreaves* [2007] EWHC 2375 (QB) and *Jane Clift v Martin Clarke* [2011] EWHC 1164. The UK courts have declined to grant Norwich Pharmacal orders where it would be disproportionate and unjustifiably intrusive to make an order for the disclosure of the identities of a user who had posted messages that were not defamatory, barely defamatory or little more than abusive.

62. E.g. the UK Defamation Act 2013.

63. ***Case C-70/10 Scarlet Extended SA v Societe belge des auteurs compositeurs et editeurs (SABAM)*** (24 November 2011); the ECJ found that blanket web filtering systems installed by ISPs to prevent illegal file sharing on peer-to-peer networks was incompatible with fundamental rights. The ruling was strongly reaffirmed in ***Case C-360/10 Sabam v Netlog*** (16 February 2012) which raised the same question in relation to social networks.

64. In China, Chinese end-users may use government approved encrypted products made in China without a licence but such products are only available through authorised channels; for more information on the regulation of encryption in China, see also **Freshfields Bruckhaus Deringer**.

65. In India, tthe Guidelines provide that individuals or organisations are only permitted to use encryption up to 40 bit key length without permission from the Licensor (i.e. the DOT). The use of a stronger encryption key, by contrast, must be authorised. The decryption key, split in two parts must be deposited with the Licensor; see CIS, **Encryption Standards and Practices** or Peter Swire and Kenesa Ahmad, op.cit.

66. The use of encryption keys of a certain length is also regulated in Senegal, see Article 13 of **Law No.2008-41 of 20 August 2008 regarding Cryptology**.

67. In Egypt, Article 64 of the TRL 2003 bans the encryption of personal communications without the consent of the authorities and gives telecommunication operators the right to collect accurate information and data about their users.

68. In 2011, the Pakistan Telecommunications Regulatory Authority ordered all Internet Services Providers to ban all Internet encryption in 2011; see ARTICLE 19, Pakistan: **Ban on Internet Encryption A Violation of Freedom of Expression**, September 2011. The orders were seemingly based on Section 54 the Pakistan Telecommunication (Re-Organisation) Act 1996, which allows the federal government to authorise any person or persons to intercept calls and messages, or to trace calls through any telecommunication system in "the interest of national security or in the apprehension of any offence."

69. Pen America, **Global Chilling: The Effect of Mass Surveillance on International Writers**, 5 January 2015; HRW, **With Liberty to Monitor All: How Large Scale US Surveillance is harming Journalism, Law and American Democracy**, July 2014.

70. In India, for example, section 84A of Information Technology (Amendment) Act, 2008 provides that "the Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption;" see India **Information Technology (Amendment) Act 2008**. Moreover, the Guidelines developed by the Department of Telecommunications ('DOT') in 2007 for the grant of licences for operating Internet services provide that the use of bulk encryption by licensees is not permitted; see The **Internet Services Guidelines**, 24 August 2007.

71. In China, encryption is a policy matter under tight government control. Under the Regulations for the Administration of Commercial Encryption 1999, the manufacture, use, import or export of encryption products is subject to government approval. For instance, encrypted products may only be manufactured by government-approved firms, which are only authorised to produce certain types and categories of encryption products. see Christopher T. Cloutier and Jane Y. Cohen, **Casting a Wide Net, China Encryption Restrictions**, 2011.

72. In Egypt, Article 13(8) of the **Telecommunication Regulation Law** 2003 provides that the National Telecommunication Regulatory Authority approves specifications and technical standards of telecommunication equipment. It also sets the rules and procedures regulating their import, sale and use. Moreover, Article 64 further mandates telecommunications operators to provide all technical equipment, systems, software and communications, which enable the armed forces and national security agencies to exercise their powers within the law.

73. See Banisar, *op. cit.*

74. For instance, US export controls have been lifted for most products since January 2000; see **Export Administration Regulation**.

75. See Article 30 of Law no. 2004-575, 21 June 2004 on confidence in the digital economy.

76. See Article 14 of Law no. 2008-41 of 20 August 2008 on Cryptology.

77. See Christopher T. Cloutier and Jane Y. Cohen, op. cit.

78. In Ethiopia, for example, the government recently enacted Proclamation no. 761/2012 on Telecom Fraud Offences, which criminalises the manufacture, assembly, import or offers for sale of any telecommunications equipment without a permit from the Ministry of Information and Communication Technology Development. Sentences of between 10 and 15 years imprisonment and fines from Birr 100,000 to Birr 150,000 are available. Furthermore, under Section 3 (3), the Ministry has the power to prescribe the types of technologies that will not require permits, and set their technical standards; see ARTICLE 19, **Ethiopia: Legal Analysis of Proclamation on Telecom Fraud Offences**, August 2012.

79. In the US, key escrow and the so-called Clipper Chip were central battlegrounds during the Crypto Wars. In 1993, the US government requested manufacturers of communications hardware which incorporated encryption to install a chip developed by the NSA, the Clipper Chip. The encryption key in communication devices would be split up and handed over to two government agencies that would disclose them to law enforcement and intelligence agencies where needed. However, the system attracted widespread criticism both on account of the NSA involvement in the process and the fact that the government would hold the keys. In a subsequent proposal, the government provided incentives for software companies to develop programmes whose encryption keys would be held in databases run by independent entities or "trusted third parties." Each entity would hold one part of the key, and would disclose it upon presentation of a court order by law enforcement and intelligence agencies. This initiative was equally unsuccessful and the US government failed in its efforts to have a key escrow system adopted internationally. See, Banisar, op. cit.

80. In Spain, Article 43 of **Law on Telecommunications 2014** provides that encryption may be used to protect the confidentiality of communications but that its use may be subject to certain conditions. In particular, an obligation may be imposed to provide algorithms or encryption procedures to government agencies in accordance with the law. This provision already existed under the 2003 Telecommunications Law. It is unclear whether this provision has ever been implemented.

81. In the UK, for instance, failure to comply with a court order requiring disclosure is punishable on indictment by 5 years imprisonment in a national security or child indecency case or two years in any other case; see **Part III of the Regulation of Investigatory Powers Act 2000**. For a detailed analysis of the encryption provisions in RIPA, see JUSTICE, **Freedom From Suspicion: Surveillance Reform for a Digital Age** (2011), pp 120-132. In France, under Article 36 of **Law no. 2004-575, 21 June 2004 on Confidence in the Digital Economy**, disclosure of encryption keys must be authorised by a judge. Failure to comply is punishable by a fine of 7500 EUR and six-month imprisonment.

82. For instance, in 2012, the government of the Netherlands considered a Bill that would have allowed law enforcement and intelligence agencies to remotely interfere with computer systems, including the deletion of data and the installation of malware; see Bits of Freedom, **Dutch Proposal to search and destroy foreign computers**, 18 October 2012; see also Law on Intelligence and Security 2002 (**Wet op de inlichtingen- en veiligheidsdiensten 2002**). Similarly, the UK government recently published a Code of Practice for public consultation which would allow interference with any equipment producing electromagnetic, acoustic and other emissions, as well as communications content and data; see **Equipment Interference Code of Practice**, Draft for Public Consultation February 2015.

DEFENDING FREEDOM OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org