ARTICLE 19

Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online

February 2015

Submission

Table of contents

Introduction

ARTICLE 19 welcomes the opportunity to comment on anonymity and encryption for the benefit of the UN Special Rapporteur on Freedom of Expression.

Anonymity and encryption are not new phenomena. The government of Pakistan has long sought to ban the use of encrypted communication, and anonymity equally has long facilitated the expression of controversial ideas, dating back to the Federalist Papers in the US in the late 18th century. However, following the recent Charlie Hebdo attacks, several Western governments have called for measures that would severely curtail the right to freedom of expression and privacy online. The UK Prime Minister David Cameron called for a crackdown on encryption,[1] while the French government is looking into ways to enhance surveillance on the Internet.[2] The protection of anonymity and encryption as a matter of international law is therefore more important than ever.

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and freedom of information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

Given the scope of our mandate, in this submission, ARTICLE 19 seeks to define the concepts of anonymity and encryption, and their implications for the right to freedom of expression in the digital age. We further identify the ways in which anonymity and encryption are protected as a matter of international law. We also outline best practices from around the world as well as problematic laws and practices in relation to those issues. We conclude with recommendations on how best to protect anonymity and encryption.

[1] See ARTICLE 19 *Crackdown on End-to-End Encryption Threatens Free Expression and the Right to Privacy*, January 2015.
[2] Numerama, Manuel Valls annonce une surveillance renforcee sur Internet, 21 janvier 2015

Anonymity

General considerations

Anonymity is a key concept in the protection of freedom of expression as well as privacy. At its simplest, anonymity is merely *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 in a crowd or standing in a queue of strangers. In this way, an activity can be anonymous even though it is also public.

Increasingly, however, various changes in technology have made it possible for information about individuals' daily activities - both public and private - to be collected and stored on a routine basis (e.g. data about the mobile phones and internet usage or the footage from surveillance cameras). In this sense, although individuals may remain anonymous to others, they are increasingly *identifiable* by virtue of the sheer amount of information that is being collected by others, both public bodies and private companies.

In addition to these, there is the increasing number of situations in which individuals are *required* to identify themselves, either as a matter of law (e.g. the need to present an identity card), as a condition of service (when registering to use an online forum) or both (e.g. when buying alcohol). While identification requirements may be a reasonable restriction in many contexts (e.g. crossing a border), each additional requirement represents an encroachment on that well-established sphere of anonymity traditionally enjoyed by private individuals.

In certain contexts - notably voting by means of secret ballots, political speech,[3] artistic expression and the protection of journalistic sources - 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 to just 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.

ARTICLE 19 therefore sets out the existing protection given to anonymity under international and domestic law, and makes recommendations for how it should be further developed.

Anonymity and the law

International standards on anonymity

The right to 'anonymity' has not yet been explicitly recognised as part of the right to freedom of expression under international law. International law has recognised only some aspects of

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

communication which should remain anonymous and undisclosed to others, namely the protection of confidentiality of sources. The UN Human Rights Committee noted in its General Comment no. 34 that:

> States parties should recognize and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose information sources.[4]

Similarly, the Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation (2008) of the four special mandates stated that:

> Normal rules on the protection of confidentiality of journalists' sources of information – including that this should be overridden only by court order on the basis that access to the source is necessary to protect an overriding public interest or private right that cannot be protected by other means - should apply in the context of anti-terrorist actions as at other times.[5]

At the European level, the European Court of Human Rights ('European Court') has recognised that sources or whistleblowers may be deterred from coming forward with important information if their anonymity is not protected.[6] The African Commission on Human and Peoples Rights maintains the protection of sources in Principle XV of its Declaration of Principles on Freedom of Expression in Africa.[7] The Inter-American Commission on Human Rights has adopted the protection of sources as part of its Declaration of Principles on Freedom of Expression.[8]

Outside of the confidentiality of sources, the right to anonymity and anonymous speech has not benefited from strong recognition at the international level. However, the domestic law of some countries has contributed to greater protection being afforded to anonymity.

The protection of anonymity in domestic law

At domestic level, the protection of anonymity has been relatively piecemeal, with some aspects of anonymity being more protected than others.

- **Anonymous speech**: The protection of anonymous speech seems to be limited to countries with a strong tradition of protecting freedom of expression, such as the US, Sweden and Canada.[9] For example, the US Supreme Court has expressly acknowledged on a number of occasions that those who hold unpopular opinions may need the protection of anonymity against whose who strongly disagree with them, whether private parties or the government. The Supreme Court has upheld the right to speak anonymously most notably in several cases:[10]

---

[4] See UN Human Rights Committee, General Comment no. 34, para. 45.
[5] The 2008 Joint Declaration on defamation of religions, and anti-terrorism and anti-extremism legislation.
[6] See *Goodwin v. the United Kingdom*, [GC], no. 17488/90, para.39, 27 March 1996.
[7] See African Commission on Human and Peoples' Rights, ACHPR /Res.62(XXXII)02 (2002).
[8] OAS, *Report on Terrorism and Human Rights*, OEA/Ser.L/V/II.1 16 Doc. 5 rev. 1 corr. (Oct. 22, 2002).
[9] See Article 1 and2, Chapter 10 of the Swedish Fundamental Law on Freedom of Expression makes reference to the right to anonymity; s.14.1 of Canada's Copyright Act gives authors the right to remain anonymous in connection with the publication of their works
[10] See also, *Watchtower v. Vill. of Stratton*, 536 U.S. 150, 166–67 (2002).

- In *Talley v. California*,[11] the Supreme Court found that a city ordinance that proscribed the distribution of pamphlets anonymously was an undue restriction on freedom of expression. Justice Black noted that: "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."

- Similarly, in *McIntyre v Ohio Elections Commission*,[12] the Supreme Court upheld the right to anonymous political speech when it struck down an Ohio statute that required that materials designed to influence voters in an election must be signed. Justice Stevens considered that "the decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." He concluded that under the US "anonymous pamphleteering is not a pernicious, fraudulent practice, but an honourable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority."

- Finally, also worth noting, the Supreme Court upheld the right to read anonymously, free from government interference, in *United States v Rumely*.[13]

- **The confidentiality of sources**: the need to protect the confidentiality of sources has long been recognised in the domestic law of a large number of countries in Central and South America, Europe and Africa.[14]

- **The right to vote anonymously**: in contrast to the relatively limited recognition of the right to anonymous speech around the world, the right to vote anonymously (or 'secret ballot'), is more widely recognised.[15] This is another important example of the way in which the law recognises that anonymity performs an important democratic function.

- **The protection of vulnerable groups**: outside of political expression, the right to anonymity is recognised, in the context of court proceedings, as a means to protect vulnerable groups. In several countries, the courts have a discretionary power to grant anonymity or reporting restrictions orders, in order to prevent the identification of a child or young person involved in criminal proceedings.[16] Such orders may be made, among other things, to enable the subsequent reinsertion of young offenders in society.

  Anonymity orders are not limited to the protection of young people however. They may also be used to protect terrorist suspects or sexual offenders, e.g. from attacks or

---

[11] US Supreme Court, *Talley v. California*, 362 U.S. 60 (1960).
[12] US Supreme Court, McIntyre v Ohio Elections Commission, 514 U.S. 334 (1995).
[13] US Supreme Court, *United States v Rumely*, 345 US 41, 57
[14] Most European countries expressly protect the confidentiality of journalistic sources. In Americas, the constitutions of Brazil, Paraguay, Argentina, and Ecuador provide for explicit source protection; protection is granted in legislation in El Salvador, Peru, Chile, Brazil, Uruguay, Venezuela, and Panama. In Africa, protection is granted in the Mozambique Constitution and Burundi and Angola do so by statute. Japan, Canada, Australia, and New Zealand have established case specific judicial balancing tests to analyze source protection claims.
[15] E.g. in France, Brazil, Japan or Mozambique.
[16] E.g. In the UK, Ss 39 and 49 of the Children and Young Persons Act 1933.

retaliation by their own communities.[17] More controversially, some legal systems allow the courts to grant witness anonymity orders in order to enable witnesses to testify without fear for their life.[18] However, they are available in limited circumstances and subject to certain conditions.[19] These measures are usually seen as a means to protect the right to private life, but can also be a restriction on the right to freedom of expression in certain circumstances.[20]

Online anonymity

The right to online anonymity under international law

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

- The 2013 report of the UN Special Rapporteur highlighted the important relationship between the rights to privacy and freedom of expression in cyberspace.[21] The report also observed that restrictions on anonymity facilitate State communications surveillance and have a chilling effect, dissuading the free expression of information and ideas.[22]

- The relationship between anonymity and the right to freedom of expression was further highlighted in a more recent report on Freedom of Expression and the Internet published by the Inter-American Commission on Human Rights (IACHR) in 2013.[23] Among other things, the IACHR recommended that anonymous platforms should be promoted and that the use of authentication services should be used proportionately.[24]

- Most instruments to have emerged in this area originally came from the Council of Europe or the European Union.[25] 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

---

[17] See e.g. A (Respondent) v British Broadcasting Corporation (Appellant) (Scotland) [2014] UKSC 25.
[18] Under UK law, for example, applications for witness anonymity can be made pre-trial under sections 74 to 85 of the Coroners and Justice Act 2009
[19] For more information, see Crown Prosecution Service Guidance.
[20] E.g. Claire Darwin, Fv G - Anonymity Orders and Extended Reporting Restrictions Orders in the Employment Tribunals, 1 December 2011.
[21] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, 17 April 2013, para 47.
[22] *Ibid.,* paras 48-49.
[23] Special Rapporteur on FOE for the OAS, Freedom of Expression and the Internet, 31 December 2013.
[24] *Ibid.* paras 23; and paras. 133-137.
[25] For instance, in its *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."

> Fundamental Freedoms and other international agreements in the fields of justice and the police.[26]

The European Court has followed this approach in its case-law. It has recognised the importance of anonymity to the right to freedom of expression and privacy. At the same time, it has made it clear that anonymity is not absolute and may be limited for the protection of other legitimate interests, especially the protection of vulnerable groups. In *K.U. v Finland*,[27] 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. The Court considered that anonymity and confidentiality on the Internet must not lead States to refuse to protect the rights of potential victims, especially where vulnerable persons are concerned:[28]

> 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 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.

More recently, the European Court expressed a similar view in *Delfi v Estonia,*[29] 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 that 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.[30] Although the case is currently pending before the Grand Chamber, it points to the urgent need for a strong reaffirmation that the right to anonymity must be protected.

The right to online anonymity under domestic law

Domestic standards on online anonymity are still developing. In several countries, current trends indicate that anonymity may be limited for the purposes of bringing defamation or copyright infringement proceedings, or to enable law enforcement to investigate alleged criminal behaviour. More problematic is the adoption of real-name registration policies in certain countries. While some courts have found that laws requiring real-name registration were an infringement of the right to privacy and freedom of expression, it remains an issue in

---

[26] *Ibid.*
[27] *K.U. v Finland* .(no.2872/02, para. 49, 2 December 2008.
[28] See The European Court of Human Rights, Internet: Case-law of the European Court of Human Rights, 2011.
[29] *Delfi v Estonia,* no.64569/09, 10 October 2013.
[30] See Access, Access intervenes for the right to be anonymous online, June 2014.

countries where the courts are less likely to uphold human rights. What follows is a short summary of the various issues that have arisen in the context of anonymity online:

- **Real-name registration**: laws which require real-name registration are a particularly blunt interference with the rights to freedom of expression and privacy online. They usually enable local law enforcement agencies to track Internet users more easily. Real-name registration laws have been adopted or considered in countries such as **China**[31] and **Russia**.[32] These laws are usually coupled with requirements that internet-users identify themselves in cybercafes, and obligations imposed on cybercafé owners to track and log the online activities of customers, as in **Iran**[33] and **Vietnam**.[34]

  At the same time, many countries do not go as far as requiring real-name registration with social media platforms. In **South Korea**, for instance, the Supreme Court struck down a real-name registration rule.[35] In **Germany**, a court in Schleswig-Holstein went even further, and held that Facebook was in breach of German data protection law by failing to provide users with the option of using pseudonyms.[36]

  Indeed, real-name registration can also be imposed by online news sites and social media platforms such as Facebook. Sometimes a user backlash may lead a company to retract its real-name policy, such as in the case of Google in relation to comments posted on YouTube or Google plus. Moreover, companies may require users to log-in in order to use their service or to connect with a social media account such as Facebook. All these self-regulatory practices have an impact on the right to privacy and freedom of expression.[37]

- **Anonymity and law enforcement:** in most countries, real-name registration laws are not necessary insofar as law enforcement agencies already have powers to require the disclosure of the identity of anonymous Internet users in any event. This is the case, for instance, in countries as varied as **Vietnam**[38] and **the UK**.[39] In other countries, such disclosure may also be ordered by the courts, as in **France**,[40] **Canada**[41] and **the US**.[42]

- **Anonymity and copyright infringement**: the ability of Internet users to gain access to peer-to-peer networks and other file-sharing sites in relative anonymity (e.g. using proxies or Virtual Private Networks) has led copyright holders to demand that Internet Access Providers install Internet filters on their networks. However, such demands have been

---

[31] See Reuters, China to ban online impersonation accounts, enforce real-name registration, 4 February 2015.
[32] In Russia, 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, regulator 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.
[33] See Freedom House, Freedom on the Net report 2014, Iran country report.
[34] See Freedom House, Freedom on the Net report 2014, Vietnam country report.
[35] Wall Street Journal, South Korea Court Knocks Down Real Name Rule, 24 August 2012.
[36] See Guardian, German state fights Facebook over privacy violations, 4 January 2013
[37] 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.
[38] See Freedom House, Vietnam country report, *op.cit.*
[39] See Ss 21 and 22 of the Regulation of Investigatory Powers Act 2000.
[40] See The Verge, Twitter Must Disclose Authors of Anti-Semitic Tweets, French Appeals Court Rules, June 2013.
[41] 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.
[42] See Freedom House, Freedom on the Net report 2014, US country report

rejected by the Court of Justice of the European Union ('**CJEU**') as incompatible with the rights to freedom of expression and privacy.[43] By contrast, copyright holders have generally not encountered significant difficulties in obtaining injunctions requiring the disclosure of the identity of anonymous file-sharers.[44] In **the US,** it appears that the courts have applied a somewhat lower threshold for such disclosure in copyright claims, as compared to defamation lawsuits.[45]

- **Anonymity and defamation online:** in the **US,** some courts have expressly recognised the right to anonymity online. E.g., in *John Doe v 2theMart.com Inc,*[46] Zilly J held that

> The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights.

At the same time, US courts have also recognised that anonymity could be lifted for the purposes of bringing a defamation lawsuit.[47] However, this is subject to the careful scrutiny of the courts, which require 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 with the prima facie case, taking into account the need for disclosure of identity for the case to proceed.[48]

Similar rules apply in the **UK** where anonymity may be lifted by way of a Norwich Pharmacal order.[49] However, the Defamation Act 2013 further limits anonymous speech by encouraging internet intermediaries to remove content posted by anonymous, rather than identifiable, speakers lest they expose themselves to liability. These types of measures may have a significant chilling effect on freedom of expression.

- **Anonymity and the public interest:** in the **UK**, recent case-law indicates that anonymity online may be lifted if there is a sufficiently strong public interest in revealing the identity of an anonymous blogger. In *the Author of a Blog v Times Newspapers Ltd,*[50] the High Court considered that the claimant, an anonymous blogger, did not have a

---

[43] *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.

[44] E.g. Sony Music Entertainment Inc. v Does 1-40, 326 F.Supp. 2d 556 - Dist.Court, SD New York 2004.

[45] Techdirt, Should Anonymity Be Dealt With Differently in Copyright Cases than in Defamation Cases?, 6 September 2011

[46] *John Doe v 2theMart.com Inc.* 140 F Supp 2d 1088 (2001).

[47] See e.g. Dendrite International Inc v John Doe 775 A 2s 758 (2000).

[48] *Ibid.*

[49] E.g. *Smith 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.

[50] *Blog v Times Newspapers Ltd* [2009] EWHC 1358 QB.

reasonable expectation of privacy regarding his personal identification. The Court considered that there was a strong countervailing public interest in revealing the identity of the blogger since he was a serving police officer whose blog posts revealed strong political opinions. It is also worth noting in that case that the identity of the blogger had been discovered by way of *jigsaw identification*, i.e. by piecing together information. Jigsaw identification is an increasingly easy way of discovering someone's identity online, due to the sheer volume of information available.

Anonymity in practice

Given the limits of legal protection of anonymity, many users have turned to technical means of achieving anonymity online. In practice, several initiatives have developed that allow internet users to maintain their anonymity online.[51] This includes the Tor browser, which hides the IP address of Internet users when browsing the Internet,[52] and the https:// protocol, which encrypts communications with some websites.[53] However, even these technical means have been the subject of legal restrictions in some countries. This is the subject of Part 2 of our response.

[51] For an overview of these initiatives, see UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012, pp. 24-26.
[52] For more information about TOR, see EFF, 7 Things You Should Know About TOR, July 2014
[53] 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.

Encryption

General considerations

Encryption has been identified 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'.[54]

Encryption works so that the 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".[55]

Encryption may be achieved in two main different ways, namely 'symmetric' and 'asymmetric' encryption.

- In **symmetric encryption schemes**, the key for encrypting and decrypting the communication is the same. Therefore, both parties must hold the same key in order to communicate. The key is also generally private so that both parties' communications can be kept secret.

- In **asymmetric encryption schemes,** the key for encrypting and decrypting the communication is different. One party publishes an encryption key, which is public for anyone to use and send him or her an encrypted message. Concomitantly, that party holds a private key, only known to him or her, which enables messages received to be decrypted.

Encryption can be used to protect data in transit or in storage: from email, to files, disks and internet connection. At the same time, it is important to bear in mind that 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 also 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".[56] In other words, digital signatures enable recipients of communications to ascertain the identity of the sender of such communications ("authentication"). It also

[54] 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.
[55] *Ibid*. Other forms of keys can include passwords and even biometrics such as fingerprints.
[56] *Ibid*.

prevents the sender from denying the authenticity of the transmitted information. Digital signatures are sometimes certified by a 'Trusted Third Party' ('TTP'), which may be a certification authority (CA) that issues digital certificates. For instance, a CA may certify the ownership of a public key. 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 the identity claimed by another user directly, without the necessity of 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 pre-requisite 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 such activities as online banking, protecting lawyer-client privileged 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.

In order to protect the security of telecommunications systems, various technological standard-setting agencies have developed best practices or 'cybersecurity standards'. This includes, for instance, the information security management standards developed by the International Standards Organisation (ISO).[57] In addition, many countries develop voluntary standards for the protection of information systems.[58] Some standards may also be certified ('cybersecurity certification') by an accredited body for a fee. Cybersecurity is therefore concerned with the protection of the integrity of information systems and preventing technical attacks against them. Encryption is one of the key ways in which cybersecurity can be achieved. While attacks on information systems can take many different forms, from botnets to Distributed Denial of Service Attacks (DDOS), attacks on encryption can be divided into three main types:

- **Brute forcing**: In a brute-force attack, a hacker runs a computer programme, which produces as many password combinations as possible until the code which locks access to the encrypted information is broken.

- **Finding vulnerability**: vulnerabilities may be found in the implementation of the code or in the device on which it is running. Other vulnerabilities may be identified in a client service at different levels (e.g. device, operating systems, application, etc) or at server level. Cryptographers generally agree that the most effective way of detecting such

[57] ISO/IEC 27001 on information security management. Other relevant international organisations include the Internet Engineering Task Force ('IETF') and the World Wide Web Consortium ('W3C').
[58] List of ISO members here.

deficiencies and ensuring strong security of cryptosystems is to open them to scrutiny and peer review.[59]

- **Backdoors**: backdoors are intentional vulnerabilities or security flaws in an encryption system. The key issue with backdoors is that any vulnerability in an information system may be exploited by criminals and law enforcement agencies in equal measure.

In addition, most countries have adopted cybercrime legislation that seeks to criminalise illegitimate access to or interference with computer or information systems.[60] 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 Pakistan, Kenya[61] and Bangladesh[62] among others. At any rate, whereas cybersecurity is generally concerned with the development of technical standards, including encryption, to protect information systems, cybercrime has traditionally been concerned with offences designed to catch computer hackers or anyone unlawfully interfering with information systems.[63] Cybersecurity and cybercrime are thus related but distinct.

Encryption and the law

Despite the vital importance of encryption, intelligence services and law enforcement agencies have long sought to 'crack' encrypted communications and restrict their use, as they see it as an impediment to the protection of national security and the prevention of crime. In the 1990s, encryption was a particularly prominent policy issue, both domestically and internationally.

More recently, there has been renewed interest in cybersecurity with several initiatives being developed by regional bodies such as the African Union[64] or the European Union.[65] Equally, a growing number of countries are prioritising cybersecurity as part of their national security strategy through the creation of national focal points dealing with cybersecurity threats.[66] In the US, the Obama administration has sought the adoption of cybersecurity legislation that would facilitate information sharing between private actors and law enforcement about such threats.[67] However, these efforts are generally centred on the sharing of information between governments and private actors (e.g. banks) about attacks on information security systems and the question of whether such information sharing should be required rather than purely

[59] P. Swire & Kenesa Ahmad, *Encryption and Globalisation,* Colum.Sci & Tech L. Review, Vol XIII, Spring 2012, pp. 416-481 at 432.
[60] See in particular the Council of Europe Cybercrime Convention 2001.
[61] ARTICLE 19, Legal Analysis of Kenya Cybercrime and Computer-Related Crimes Bill 2014 (pending).
[62] International Commission of Jurists, Bangladesh: Information Communication Technology Act Draconian Assault on Free Expression, 20 November 2013.
[63] 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 the way in which these offences are drafted.
[64] African Union Convention on Cyber-Security and Personal Data Protection 2014.
[65] European Commission, Communication on a Cybersecurity Strategy of the European Union - an Open, Safe and Secure Cyberspace, 2013.
[66] E.g. France and Brazil.
[67] E.g. recent initiatives in the US: EFF Statement on President Obama's Cybersecurity Legislative Proposal, 13 January 2015.

voluntary. They generally do not expressly seek to regulate encryption. This does not mean that encryption is not the subject of regulation in many countries.

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 1997 OECD Guidelines on Cryptography policy which identify key issues which its member states should consider when adopting cryptography policies, both nationally and internationally. In particular, the OECD recommended the following basic principles:[68]

  1) Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems;
  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 the 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 co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade. The various policy issues related to the use of cryptographic techniques were explored, which examined.

  In its explanatory report, the OECD noted the fundamental importance of cryptography to the protection of the right to privacy and information security:[69]

  > 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

[68] The full recommendation is available from here.
[69] The report is available from here.

> confidentiality of data, or protecting critical infrastructures, governments may require the use of cryptography of a minimum strength.

- In his 2013 report, the UN Special Rapporteur on freedom of expression established the relationship between freedom of expression, encryption and anonymous communications.[70]

- The Inter-American Commission on Human Rights has made recommendations regarding the protection of anonymous communications and encryption tools, in the 2013 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.[71].

- The 2015 report of the Parliamentary Assembly of the Council of Europe ('PACE') strongly condemned the NSA's efforts to weaken encryption standards and the use of backdoors, in a report on mass surveillance. 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".[72]

It is worth noting that the report seems to signal a more progressive approach by the Council of Europe, moving towards the protection of the rights to privacy and freedom of expression as regards encryption. In a Recommendation Concerning Problems of Criminal Procedure Law Connected with Information states dating from 1995, the Committee of Ministers had recommended to Member States that

> Measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary".[73]

Encryption, trade agreements and cybersecurity

Outside human rights standards, encryption has chiefly been governed by international agreements concerning the regulation of import/exports of dual-use technology goods. It is also relevant to current discussion on cybersecurity and cybercrime, although not always specifically mentioned.

- The **Wassenaar Arrangement** (WA) is a non-binding agreement by a group of 41 nations to maintain export controls on listed items, which fall into two main categories, namely

[70] UN Special Rapporteur on Freedom of Expression, op.cit. para. 89 and 92.
[71] See Inter-American Commission on Human Rights, op. cit. para. 83.
[72] See PACE, Committee on Legal Affairs and Human Rights, Report on Mass Surveillance, AS/Jur (2015) 01, 26 January 2015.
[73] Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995.

'munitions' and 'dual-use goods and technologies'.[74] The latter category includes high level cryptographic products and other technology such as supercomputers and high-level computer security access software that can function in both commercial and military contexts.

Under the Arrangement, participating states agree to adjust their national export control policies to adhere to the WA Control Lists and to follow best practices and guidelines developed under the Arrangement. However, this is discretionary. Participating states also commit to report on transfers and denials of specified controlled items to destinations outside the Arrangement. In addition, the WA facilitates the exchange of information on sensitive dual-use goods and technologies.

Cryptography guidelines were added to the WA in 1998, extending the list of controlled items to include encryption hardware and software cryptography products above 56-bits.[75] However, a wide range of encryption products remain outside the scope of the WA, including items available in the public domain and products when accompanying their user for the user's personal use.[76]

It is also worth noting that like many international agreements, the WA was negotiated as a tool for the promotion of national policies. In particular, the US and UK governments led efforts to promote the key escrow system. However, it was eventually rejected by the other participating countries.

- **The EU** has played an important role in lifting national restrictions on export controls of dual-use technology, including cryptographic products.[77] The key instrument in this regard is Regulation (EC) No 428/2009, which governs the EU export control regime. The Regulation provides for common EU control rules, a common EU control list and harmonised policies for implementation.[78] The Regulation is binding and directly applicable throughout the EU. In addition, EU Member States have a certain discretion in adopting additional measures for implementing some of the Regulation's provisions, e.g. in relation to breaches and applicable penalties.[79]

  In addition, the EU is increasingly seeking to harmonise standards of information security across the Union. In particular, the European Commission's 2013 Communication on Cybersecurity Strategy of the European Union, as well as a proposal for a Directive 'concerning measures to ensure a high common level of network and information security across the Union.[80] The proposal lays down common minimum standards for Network and Information Security (NIS) at a national level. This includes coordinated prevention, detection, mitigation and response mechanisms for cyber security breaches. While

[74] For more information about the Wassenaar Arrangement, see: http://www.wassenaar.org/
[75] See List of Dual-Use Goods and Technologies, Category 5 Part 2 - Information Security, available from here.
[76] Ibid.
[77] See EPIC, *Cryptography & Liberty 2000: An International Survey of Encryption Policy* (2000), p.17. In examining the rationale behind lifting export controls on cryptographic products, the Commission said that "*restricting the use of encryption could well-prevent law-abiding companies and citizens from protecting themselves against criminal attacks*." See EU Commission, Communication on Digital Signatures and Encryption (97)503.
[78] See http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/
[79] Ibid.
[80] For more information about these initiatives, see here.

encryption is not specifically referenced as a tool for prevention, it is vital to the protection of information security.

Nonetheless, the European Commission has come under pressure, in the aftermath of the Charlie Hebdo attacks, from the EU Counter-Terrorism Coordinator to adopt rules granting law enforcement and intelligence agencies lawful access to encrypted communications. In particular, the EU Coordinator suggested that

> The Commission should be invited to explore rules obliging internet and telecommunications companies operating in the EU to provide under certain conditions as set out in the relevant national laws and in full compliance with fundamental rights access of the relevant national authorities to communications (i.e. share encryption keys).[81]

- In 2014, the African Union adopted the African Union Convention on Cyber-Security and Personal Data Protection.[82] The Convention contains a number of obligations incumbent upon data controllers to collect, process and store data confidentially and securely. It also requires Member States to put in place cyber-security strategies, and, where appropriate, institutions with a view to coordinating responses to cyber-security incidents, as well as cooperating with restorative justice and forensic investigations.[83]

  Under the Convention, Member States undertake to impose certain requirements on vendors of ICT products. This includes an obligation to ensure that their goods are tested by independent experts and researchers, and to disclose any vulnerabilities detected together with solutions to their customers.[84] The Convention further requires Member States to criminalise the import and dissemination of hardware or software with backdoors installed in them.[85] More generally, Article 3 of the Convention provides that in adopting legal measures in the area of cyber-security, Member States must ensure that such measures do not infringe the rights of citizens guaranteed by national constitutions and international conventions, especial the African Charter on Human and Peoples' Rights. While the above measures are generally positive, the AU Convention contains a raft of other measures, which are far more concerning. This includes content-based offences, harsher penalties for offences committed online and cooperation between investigating authorities and ISPs to conduct real-time interception of computer data.

Encryption under domestic law

Restrictions on *the use of cryptography (including encryption) come in many different* shapes and forms. They are perhaps best exemplified by the tactics used by the US National Security Agency ('NSA') in the 90s to stifle any debate on cryptography.[86] Generally speaking, they can be divided into the following different types:

- **Control over research, development and dissemination of encryption:** during the "Crypto Wars" in the **US** in the 90s, the NSA sought to restrict public discourse and research on

[81] See Council of the European Union, General Secretariat, Meeting Document, D1035/15, 17 January 2015.
[82] For the full text of the African Union Convention on Cyber-Security and Personal Data Protection, see here.
[83] See Article 25.2.
[84] Article 29 (1) (g).
[85] Article 29 (1) (h).
[86] See Banisar, *op. cit.*

cryptography by limiting funding for academic research in the subject.[87] It also relied on the 1951 Invention Secrecy Act to attempt to classify cryptography products developed by non-government researchers.[88] While we are not aware of similar developments in recent years, they are indicative of the types of measures that might be adopted by governments, intent on restricting public discussion, development and dissemination of encryption techniques.

- **Mandatory technical requirements**: another way in which governments may seek to assert control over information systems is 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 relating to cryptography, telecommunications systems security or information system security. In **the US**, this was achieved by the NSA at the beginning of the Crypto Wars but its control was eventually dismantled by the Computer Security Act 1997. Nonetheless, the NSA worked closely with other government departments and agencies, including the Department of Commerce, the Federal Bureau of Investigation and the Federal Communications Commission to impose further restrictions on cryptography. In particular, they sought the adoption of legislation that would require government approval, or adherence to government encryption criteria, for all encryption products as a condition for use in the US.

  While such proposals were eventually defeated, similar provisions are in place in countries such as India, China or Egypt. For example, in **India**, 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."[89] 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.[90]

  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.[91]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.[92]

  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

[87] *Ibid.*
[88] *Ibid.*
[89] See India Information Technology (Amendment) Act 2008
[90] The Internet Services Guidelines dated 24 August 2007 are available from here.
[91] See Christopher T. Cloutier and Jane Y. Cohen, Casting a Wide Net, China Encryption Restrictions, 2011
[92] *Ibid.*

communications, which enable the armed forces and national security agencies to exercise their powers within the law.

- **Restrictions on end-users:** the regulation of technical specifications is sometimes coupled with restrictions on the use of encryption by end-users. 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.[93] In **India**, the 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.[94] The use of encryption keys of a certain length is also regulated in **Senegal**.[95] 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. In **Pakistan**, the Telecommunications Regulatory Authority ordered all Internet Services Providers to ban all Internet encryption in 2011.[96] 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."[97]

- **Subverting voluntary technical standards:** most countries have standard-setting bodies in place which, among other things, develop voluntary technical standards. In the **US**, technical standards are developed by the National Institute of Standards and Technology ('NIST') - formerly the National Bureau of Standards ('NBS') - following an open process and peer review. Banisar chronicles how as early as 1972, the NSA successfully interfered with the development of the first public government encryption standard - the Data Encryption Standard - by the (then) NBS. The NSA obtained that the key size of a symmetric encryption system be reduced from 128-bit to less than half the size.[98] In 1991, the NSA managed to ensure that NIST would adopt its Digital Signature Standard proposal. When the standard was subsequently released, it was criticised for its lack of privacy protection and for the role of the NSA in designing the algorithm. While we are not aware of similar strategies for weakening encryption standards in other countries, the above example is indicative of the way in which technical standards may subverted in countries where technical requirements are not mandated by law.

  Moreover, it is worth noting that the main US hardware and software companies are under relentless pressure to develop weaker encryption for their products.[99] For instance, the Guardian reported in 2013 that Microsoft had helped the NSA to access encrypted web

---

[93] *Ibid*. For more information on the regulation of encryption in China, see also Freshfields Bruckhaus Deringer.
[94] For more information, see CIS, Encryption Standards and Practices or Peter Swire and Kenesa Ahmad, *op.cit.*
[95] See Article 13 of Law No.2008-41 of 20 August 2008 regarding Cryptology.
[96] See ARTICLE 19, Pakistan: Ban on Internet Encryption A Violation of Freedom of Expression, September 2011
[97] *Ibid.*
[98] Banisar, *op. cit.*
[99] For instance, FBI Director James Comey's called default encryption settings, devices, and networks—including Apple's and Google's new operating systems—a challenge to law enforcement and national security officials: see address at the Brookings Institute, 16 October 2014

chats, emails and cloud storage.[100] In India, the government pressured the Canadian company RIM for access to encrypted messaging. RIM handed over access to individual emails and messaging via Blackberry messenger, as well as supplying metadata, and (after a 4 year standoff with the Indian Government) government files showed that they had received the codes for corporate clients also.[101]

- **The key escrow or trusted party system:** a key escrow system is supposed to achieve strong encryption - and therefore the protection of individuals' privacy and information security - whilst at the same time enabling access to law enforcement and intelligence agencies upon request. 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). 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.[102] 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.[103]

  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'.[104] 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 further below).[105]

  Nonetheless, key escrow systems are currently in place in a few countries, including India (see above), and **Spain**. 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.[106] This provision already existed under the 2003 Telecommunications Law. It is unclear whether this provision has ever been implemented.

- **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. Failure to comply is usually a criminal offence, which is punishable by imprisonment and/or a fine. In **the UK**, for

---

[100] The Guardian, Microsoft handed the NSA access to encrypted messages, 12 July 2013
[101] The Economic Times, Blackberry maker Research in Motion agrees to hand over its encryption keys to India, 2 August 2012
[102] Banisar, *op. cit.*
[103] *Ibid.*
[104] *Ibid.*
[105] *Ibid.*
[106] The Spanish law on telecommunications is available here (in Spanish).

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.[107] 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.[108] Failure to comply is punishable by a fine of 7500 EUR and six-month imprisonment.

While such powers are deeply problematic from the perspective of the right against self-incrimination, they also respect - in principle, at least - the integrity of encryption by enabling individuals to decrypt the protected information themselves rather than disclose the key. They are also generally less intrusive of individuals' privacy than key escrow, since at least the individual knows that his or her privacy is being interfered with. Nonetheless, common problems with mandatory disclosure requirements include the question of whether individuals might be unduly penalised if they do not have access to the keys in their name - either because they are not in possession of the key, never possessed it in the first place, or because they have lost or revoked the key.

- **Import/export controls:** another way in which governments have sought to exert control over encryption is 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. By contrast, the international market demands strong encryption. These divergent interests have been used by governments in the past in order to influence domestic policy. For instance, **the US** used the rules on export controls as a bargaining chip to pressure hardware and software manufacturers into adopting weaker encryption products or the key escrow system at home.[109]

  With the Internet however, these controls have largely been relaxed. For instance, US export controls have been lifted for most products since January 2000.[110] Nonetheless, it appears that several countries, such as **France**[111] or **Senegal**,[112] 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, such as **China**[113] and Ethiopia, continue to impose significant restrictions on the import of computer programmes or equipment that permit cryptography. This is generally because governments are wary of importing products which might have backdoors installed in them or because they wish to retain their domestic surveillance capabilities. In **Ethiopia**, for example, the government recently

---

[107] 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.
[108] The text of the law is available here.
[109] See Banisar, *op. cit.*
[110] See Export Administration Regulation.
[111] See Article 30 of Law no. 2004-575, 21 June 2004 on confidence in the digital economy.
[112] See Article 14 of Law no. 2008-41 of 20 August 2008 on Cryptology.
[113] See Christopher T. Cloutier and Jane Y. Cohen, op. cit.

> 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.[114]

Finally, 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. 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.[115] 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.[116]

[114] See ARTICLE 19, Ethiopia: Legal Analysis of Proclamation on Telecom Fraud Offences, August 2012
[115] 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)
[116] Equipment Interference Code of Practice, Draft for Public Consultation February 2015

Recommendations

Anonymity

Given the vast amount of information collected both by private companies and public bodies about our lives, it is obvious that the rights to privacy, freedom of expression and anonymity online must be more strongly and consistently protected than ever before. Any restriction on anonymity should comply with the three part-test under Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR), namely: (i) have a basis in law, (ii) pursue a legitimate aim as exhaustively enumerated under Article 19 (3) ICCPR; and (iii) be necessary and proportionate in a democratic society.

In ARTICLE 19's view, mandatory real-name registration systems go well beyond what is permissible under international human rights law. At the same time we recognise that online anonymity may be lifted in certain circumstances, including for the prevention of crime and the protection of the rights of others. However, any such restriction on anonymity should be subject to strong procedural safeguards. In particular, as a matter of principle, the mandatory disclosure of 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.

In light of the above, ARTICLE 19 recommends that the UN Special Rapporteur should:

- Explicitly affirm that the right to freedom of expression includes the right to anonymity;
- Elaborate the right to anonymity and hold that it includes the right to anonymous speech, the right to read anonymously, and the right to browse online anonymously.
- Reaffirm that real-name registration systems imposed by governments constitute a violation of the rights to freedom of expression and privacy;
- Recommend that only the courts - rather than law enforcement agencies - should have the power to order that anonymity be lifted.
- Recommend that companies consider the implications of real-name registration policies for freedom of expression and the right to privacy. At a minimum, companies with a real-name registration policy should allow anonymity in appropriate cases.
- Promote the use of tools such as Tor and https:// protocols that allow anonymous 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. Weak encryption standards or 'backdoors' - whether mandatory or otherwise - undermine people's trust in the Internet and constitute a serious interference with fundamental rights.

In ARTICLE 19's view, same as stated above re anonymity, any such interference must strictly comply with the three-part test under Article 19 (3) ICCPR. This means that any restriction on 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 reference to the incredibly 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.[117]

ARTICLE 19 considers that measures such as blanket bans on the use of encryption by end-users, and the installation of back-doors compromising the integrity of private communications software are hopelessly disproportionate and, as such, incapable of justification under international law.

Similarly, ARTICLE 19 believes that the promotion of weak encryption standards and the manipulation of export rules on encryption pose a significant threat to the confidentiality of communications and the right to privacy of Internet users. In addition, such measures can also be understood as undue restrictions on the free expression rights of coders.[118] Given the increasing frequency and severity of cyberattacks on both a national and international level, ARTICLE 19 strongly doubts that weakening encryption standards could ever be a proportionate response.

In light of the above, ARTICLE 19 recommends that the UN Special Rapporteur:

- Affirms that encryption is a basic requirement for the protection of the confidentiality of information and its security and that as such, it is essential to the protection of the right to freedom of expression online;
- Calls on governments
  - to refrain from measures requiring or promoting technical backdoors to be installed in hardware and software encryption products;
  - to repeal laws banning the use of encrypted products, particularly by end-users;
  - to repeal laws requiring government authorisation for the use of encrypted products;
  - to put programmes in place for the promotion of encryption in internet communication;
  - to promote end-to-end encryption as the basic standard for the protection of the right to privacy online;
  - to promote the use of open source software;
  - to invest in open source software to ensure that it is regularly and independently maintained and audited for vulnerabilities;
  - to lift undue import/export restrictions on encryption hardware and software;
- Calls on companies to refrain from weakening technical standards and to roll out the provision of services with strong end-to-end encryption.

---

[117] 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

[118] *Universal City Studios Inc. v. Eric Corley*, 273 F.3d 429 (2d Cir. 2001).The defendant argued that a copyright rule that prevented him from publishing a code that would allow for the decryption of certain films protected by technical protection measures was an unconstitutional limit on his free speech rights. It was ruled that "computer code conveying information is "speech" within the meaning of the 1st Amendment, but that Corley was not justified in disseminating the decryption code, as copyright concerns outweighed his right to free expression in this context.