Submission to the Office of the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression on Encryption and Anonymity in Digital Communications

February 2015

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Background[1]

The spread of the Internet has provided a great boon to freedom of expression, giving ordinary citizens the power to address a global audience in the millions and bringing enormous amounts of information into every household with an Internet connection. A number of factors facilitate the incredible sharing of information that takes place over the World Wide Web but this is driven at least in part by the intimacy of the medium. Communicating from the safety and security of one's home lends a sense of privacy to online expression, which is reinforced by the facelessness of online interactions. These qualities help facilitate the candour and openness that have become characteristic of online speech and grant users the freedom to pursue secret tastes or interests, and express unfiltered opinions, on all things great and trivial without fear of what their family or social circle might think.

While online interactions might feel private, the reality is rather different. The Internet is the most heavily monitored medium of expression in history, where nearly every article read, every comment made and every piece of information obtained or shared is tracked, processed and collated on a massive scale by a variety of both State and non-State actors. This unprecedented level of monitoring is facilitated in part by the nature of the medium itself – which centralises the flow of information and gives it a permanence which never applied to phone conversations or even hand-written correspondence – and partly by the rapid advancement in computing power and information storage capacity which has coincided with the Internet's spread. The impact of this tracking is a general erosion of privacy as more aspects of peoples' lives move online, and what were once transient and relatively anonymous activities now leave identifiable digital trails.

Awareness of the extent of monitoring taking place online was brought into the public eye in a dramatic fashion by Edward Snowden's disclosures in 2013 of a massive surveillance apparatus led by the United States' National Security Agency (NSA) and operated with the collaboration of allied governments around the world.[2] In the aftermath of the Snowden revelations, digital mass surveillance programmes were widely condemned as a human rights violation, including by the UN High Commissioner for Human Rights,[3] the Parliamentary Assembly of the Council of

[2] It is important to note that this is only one of a number of intrusive surveillance networks in place around the world.

[3] Opening Remarks to the Expert Seminar: The right to privacy in the digital age, 24 February 2014. Available at: www.ohchr.org/AR/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=A.

Europe[4] and in a Joint Declaration by the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Organization of American States Special Rapporteur on Freedom of Expression.[5] However, others have spoken out in defence of the data collection efforts. In a digital world, the programmes' proponents argue, law enforcement must be equipped with the tools to track online communications.[6] They argue that widespread surveillance is necessary to guarantee safety and security in a world of disbursed and shifting threats, and that sophisticated and geographically diverse enemies make it impossible to know where important communications will originate, necessitating a broad surveillance net.

Since the Snowden revelations, the debate over mass surveillance has been further complicated by the growing proliferation of tools designed to protect privacy, including to facilitate anonymous communication. Anonymisation tools come in many different forms, which vary widely in their usability and efficacy.

The most popular anonymisation tool is Tor, the usage of which doubled in the initial two months after the Snowden revelations.[7] Tor is usually deployed through a specialised web browser, which enables users to surf the web via the Tor network. It uses multi-layered encryption, as well as thousands of distributed relay points, to mask both the content of traffic and the identity of its origin. The degree of protection Tor offers is difficult to know with any certainty, since intelligence authorities and hackers are obviously not forthcoming about the extent of their capabilities and in any case there is an ongoing "arms-race" between the forces seeking to bolster privacy tools and those seeking to crack them. However, the Snowden files suggest that the NSA was at that time unable to hack it. Crucially, Tor's design is meant to ensure that its creators themselves are unable to access this information, and there is no (known) backdoor.

Revelations of the scope of the NSA-led surveillance activities also led to a spike in the use of encryption. In early 2013, encrypted traffic accounted for 2.29% of peak hour traffic in North America, 1.47% in Europe and 1.8% in Latin America. As of May 2014, those proportions had risen to 3.8%, 6.1% and 10.37%, respectively.[8] Even more significantly, some United States-based technology companies, the reputations of which suffered as the public learned about their complicity in the

[4] Luke Harding, "Mass surveillance is fundamental threat to human rights, says European report", *The Guardian*, 26 January 2015. Available at: http://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe.
[5] Adopted 21 June 2013. Available at: www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.
[6] Dianne Feinstein, "The NSA's Watchfulness Protects America", *Wall Street Journal*, 13 October 2013. Available at: www.wsj.com/articles/SB10001424052702304520704579125950862794052.
[7] Tim Sampson, "Tor usage doubles after Snowden's surveillance revelations", The Daily Dot, 28 August 2013. Available at: www.dailydot.com/politics/tor-usage-doubles-snowden-nsa-prism/.
[8] Klint Finley, "Encrypted Web Traffic More Than Doubles After NSA Revelations", Wired, 16 May 2014. Available at: www.wired.com/2014/05/sandvine-report/.

surveillance efforts, have announced plans to encrypt all user information by default, placing it off limits even to the companies themselves.[9] As with anonymisation tools, it is difficult to know for certain how effective encryption is at hiding the content of communications. Tech companies claim that the move to encrypting user information would render them incapable of complying with future law enforcement requests for access. The fact that law enforcement officials are complaining vociferously about the plans[10] suggests that, at the very least, it would make surveillance significantly more difficult, although it is worth noting that encryption on its own does not shield users' metadata, which itself can be highly revealing.

While privacy advocates have welcomed increased use of anonymisation and encryption tools, governments and law enforcement authorities have protested. For example, Tor has been accused of facilitating the sharing of child pornography.[11] Moreover, some governments and law enforcement authorities have labelled encryption-by-default as dangerous, and have even threatened to pass legislation forcing companies to create backdoors for law enforcement access.[12]

Generally, the human rights and tech communities reacted very negatively to the NSA-led mass surveillance programmes, and are keenly aware of the importance of privacy, anonymity and encryption to maintaining the vibrancy of online speech. However, it is clear that arguments from the security establishment cannot simply be dismissed out of hand. It is clear that digital surveillance is an essential tool for any modern law enforcement or national security authority. Strong encryption and anonymisation tools make it much more difficult for these authorities to monitor the communications of criminals and security threats, hindering their legitimate operations.

The question of how to balance user privacy, particularly through encryption and anonymisation tools, against legitimate law enforcement needs is of critical importance to free speech in the digital era. This Submission, developed by the Centre for Law and Democracy (CLD) in response to a call for input by the Office of the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, explores the implications of this debate for freedom of

[9] Joe Miller, "Google and Apple to introduce default encryption", BBC, 19 September 2014. Available at: www.bbc.com/news/technology-29276955.
[10] Russell Brandom, "FBI director blasts Apple and Google for offering encryption, The Verge, 25 September 2014. Available at: www.theverge.com/2014/9/25/6845261/fbi-director-blasts-apple-and-google-for-offering-encryption.
[11] Andy Greenberg, "No, Department of Justice, 80 Percent of Tor Traffic Is Not Child Porn", Wired, 28 January 2015. Available at: www.wired.com/2015/01/department-justice-80-percent-tor-traffic-child-porn/.
[12] Will Oremus, "Obama Wants Tech Companies to Install Backdoors for Government Spying", 19 January 2015. Available at: www.slate.com/blogs/future_tense/2015/01/19/obama_wants_backdoors_in_encrypted_messaging_to_allow_government_spying.html.

expression, and identifies five key principles which should guide future policymaking in this area.

Privacy, Anonymity and Freedom of Expression

There is a rich history of anonymity facilitating free speech. Anonymous pamphleteering has long been a potent force in political discourse. A notable example was Thomas Paine's *Common Sense*, published in early 1776 to encourage the people of the Thirteen Colonies (soon to become the United States of America) to declare their independence from Great Britain. It played a significant role in rousing popular support for the coming revolution and was highly incendiary in nature, not to mention legally treasonous, making the decision by Paine to leave his name off of it understandable. Thomas Robert Malthus' *An Essay on the Principle of Population*, the first book to highlight the dangers of overpopulation, was also originally published anonymously. Malthus later revealed himself as the author of the controversial work and, it is worth noting, was thereafter subjected to intense personal attacks. Many ideas which are now widely accepted began as fringe, or even offensive, concepts. Anonymity can be central to allowing these ideas to be aired. In 1995, the United States Supreme Court, holding that the right to anonymous speech was constitutionally protected, noted: "Anonymity is a shield from the tyranny of the majority."[13]

The right of journalists to work with anonymous sources, and the importance of laws allowing them to keep their sources confidential, is also firmly entrenched in international law. As the European Court of Human Rights stated in the case of *Goodwin v. the United Kingdom*:

> Protection of journalistic sources is one of the basic conditions for press freedom.... Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest.[14]

Journalists' experiences in recent years provide some evidence of the importance of confidential sources. According to report by Human Rights Watch in collaboration with the American Civil Liberties Union, United States' government officials have become increasingly cagey about sharing information with journalists since

[13] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). Available at: supreme.justia.com/cases/federal/us/514/334/case.pdf.
[14] 27 March 1996, Application no. 17488/90, para. 39.

Snowden revealed the extent of surveillance taking place.[15] The same study indicated that awareness about the surveillance programmes has increased pressure on journalists and lawyers, with many having adopted costly, time-consuming and elaborate communication safeguards aimed at minimising the risk of interception.

Anonymity can also be particularly important in facilitating whistleblowing, in order to protect individuals who expose malfeasance or corruption by public authorities or other powerful interests against reprisals. Many governments, and even some businesses, go out of their way to facilitate anonymous disclosures, in the hopes of stopping harmful or illegal behaviour.[16]

Anonymous speech can also help facilitate discussion about embarrassing or personally sensitive topics. Mental health crisis centres, sexual health resource centres and reporting mechanisms for child abuse need to allow for anonymous communications for obvious reasons. The potential for embarrassment or social stigma, with its concomitant chill on speech, can even extend to relatively mundane topics. An individual who feels technologically challenged may be reluctant to seek information publicly about what they fear is a simple technical problem.

In addition to these specific instances where anonymity facilitates speech, there is a growing consensus about the broader importance of privacy and anonymity to freedom of expression, particularly in an online context. For example, the Council of Europe's *Declaration on Freedom of Communication on the Internet* states that:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas (…) States should respect the will of users of the Internet not to disclose their identity.[17]

Control over one's communications, including over who has access to them, is a key element of expression. Studies have shown that perceptions of control lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.[18]

---

[15] Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, July 2014. Available at: www.hrw.org/reports/2014/07/28/liberty-monitor-all-0.

[16] See, for example, the anonymity policy of the United States' Securities and Exchange Commission, available at: http://www.secwhistleblowerprogram.org/SEC-Whistleblower/anonymity/anonymity-provisions/, and the anonymous reporting mechanisms established by TD, a Canadian bank, available at: http://www.td.com/about-tdbfg/corporate-governance/tdbfg-whistleblower-hotline/whistleblower.jsp.

[17] Council of Europe, *Declaration on Freedom of Communication on the Internet*, Principle 7 (2003). Available at: www.coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf.

[18] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 *European Journal of Information Systems* (2013), p. 300. Available at: www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.

The nexus between privacy and freedom of expression was noted by Frank La Rue in 2013, during his tenure as the UN Special Rapporteur on Freedom of Opinion and Expression:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy… Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.[19]

The connection between privacy and freedom of expression was also noted in a 2014 report by the Office of the United Nations High Commissioner for Human Rights, which explicitly warned of the dangers posed by mass surveillance to these and other human rights:

> While the mandate for the present report focused on the right to privacy, it should be underscored that other rights also may be affected by mass surveillance, the interception of digital communications and the collection of personal data. These include the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media… Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.[20]

Once it is understood that the use of anonymisation and encryption tools to protect digital speech engages freedom of expression and privacy issues, it follows that restrictions on the use of such tools, or measures to limit the effectiveness of such tools, must pass muster as restrictions on these rights. The Centre for Law and Democracy recognises that, in a digital world, law enforcement and intelligence authorities have a legitimate need to carry out surveillance online. Law enforcement has had the power to listen to a suspect's telephone conversations or read a suspect's mail for decades, and this is a power that should naturally carry over into the digital realm. However, these powers have been subject to stringent procedural safeguards and analogous safeguards need to be applied in a digital context.

Under international law, any intrusions into freedom of expression must be justified according to the three-part test for restrictions on freedom of expression as set out in Article 19(3) of the *International Covenant on Civil and Political Rights*.[21] This

[19] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, UN Doc. A/HRC/23/40, para. 79.
[20] Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, UN doc, A/HRC/27/37, para. 14-20.
[21] UN General Assembly Resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976. For a fuller elaboration of how the three-part test works, see: www.law-democracy.org/live/wp-content/uploads/2015/02/foe-briefingnotes-2.pdf.

requires restrictions to be provided for by law, to serve one of the legitimate aims listed in that article, which include national security and public order, and to be 'necessary' to protect that aim. The necessity part of the test is complex, and would be where the balancing between law enforcement and free speech interest in relation to the use of anonymisation and encryption tools would largely need to take place.

The technological complexity of anonymisation and encryption tools, as well as the capacity of law enforcement authorities to pierce those tools, significantly complicates the debate, as does the fact that the technologies are evolving at a very rapid pace. However, under international law it is up to the State to justify any interference with freedom of expression pursuant to the three-part test. It is clear that mere allegations of national security needs are not enough, and that States much provide specific evidence about how, on balance, any restriction on freedom of expression serves the larger public interest.

Key Principles on Anonymity and Encryption

The relationship between surveillance, freedom of expression, security, privacy, anonymity and technology is complex and continually evolving. However, it is possible at this point to identify a few key principles which are of cardinal importance to guaranteeing freedom of expression online and which should guide future discussions on these issues.

1. **States should respect robust principles of transparency regarding their activities in relation to anonymity and encryption based on the right to information and the fact that secrecy in this area impacts on the human rights to freedom of expression and privacy.**

Discussions around online privacy and anonymity and the proper extent of State surveillance efforts need to take place in public. In the immediate aftermath of the Snowden disclosures, even the United States government said that it "welcomed" the opportunity to engage in a broad public debate over the appropriateness of its mass surveillance programmes, no doubt as a way to try to bolster its credibility.[22]

Balancing fundamental human rights, like freedom of expression and privacy, against national security, is a difficult and important challenge even for more democratic States. It is absolutely vital that the public be adequately informed about policies governing and the extent of surveillance being carried out in order to facilitate robust debate around this issue.

[22] Dan Roberts, "White House 'welcomes media interest' in Prism", *The Guardian*, 9 June 2013. Available at: www.theguardian.com/world/2013/jun/09/prism-security-media-response.

The need for disclosure of information which would not directly undermine the objectives of surveillance activities flows from the right to information (RTI), a human right which is derived from the right to freedom of expression.[23] Core RTI principles establish a presumption in favour of the release of all information held by public authorities. As organs of the State, security and intelligence authorities should be subject to RTI obligations. RTI principles also establish that information should be made public unless this would pose a risk of harm to a protected interest, which would include public order and national security. Importantly, however, where the overall public interest is served by disclosure, the information should still be released even if this poses a risk of harm to security. In the context of surveillance activities, given that they undermine respect for human rights such as freedom of expression and privacy, there will always be a strong public interest argument in favour of openness.

The need for transparency in rules governing national security, and a good overview of the minimum categories of information that should be disclosed, is reflected in the *Tshwane Principles on National Security and the Right to Information*,[24] the leading international statement in this area. The Principles were drafted by a broad coalition of civil society and academic and other experts and have been endorsed by the four special international mandates on freedom of expression (at the UN, the OAS, the OSCE and the ACHPR), as well as the UN Special Rapporteur on Counter-Terrorism and Human Rights. Principle 10E of the Tshwane Principles states:

> (1) The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.
> (2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.
> (3) In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.
> (4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.
> (5) The high presumptions in favor of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.

[23] See *Claude Reyes and Others v. Chile,* 19 September 2006, Series C, No. 151 (Inter-American Court of Human Rights), *Társaság A Szabadságjogokért v. Hungary*, 14 April 2009, Application no. 37374/05 (European Court of Human Rights) and UN Human Rights Committee, General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 18.

[24] Available at: http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

The Joint Declaration by the two special international mandates on freedom of expression on Surveillance Programs and their Impact on Freedom of Expression also addresses the issue of transparency, stating, in paragraph 12:

> ... states should, at the very least, make public information regarding the regulatory framework of surveillance programs; the entities in charge of their implementation and oversight; the procedures for authorizing, choosing targets, and using the data collected; and the use of these techniques, including aggregate information on their scope.[25]

The categories of information listed in these statements include the legal and policy framework within which surveillance takes place, statistical or aggregated data about the operations of surveillance authorities such as their total number of targets, the bodies or authorities which are empowered to conduct surveillance and information about the structure, hierarchy and decision-making apparatuses of these organisations, and information about any illegal or abusive surveillance practices that have been carried out. CLD also believes that individuals who have been subject to surveillance should be notified of this fact as soon as possible, which will normally be as soon as such notification will not undermine the purpose of the surveillance.

To supplement official openness about digital surveillance, it is important to support organisations and individuals who lever greater openness about this issue. An important aspect of this is that States put in place strong whistleblower protection legislation which applies broadly to both the private and public sectors, including security and intelligence authorities. It is also important that support is provided to organisations which report on how digital surveillance is being carried out, although it may be a bit unrealistic to expect this to be provided by the very governments which are the target of such reporting.

2. There should be adequate oversight of digital surveillance, including of the authorities that carry it out.

Proper oversight is necessary wherever State power is exercised and this is particularly important where there is a risk that human rights may be negatively impacted. As Navi Pillay, the UN High Commissioner for Human Rights, put it: "[I]nternal safeguards without independent, external monitoring are ineffective against the abuse of surveillance methods."[26]

Surveillance, almost by definition, takes place in secret. Although there is a paramount need for transparency about these processes, as described above, there

[25] Adopted 21 June 2013. Available at: www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.
[26] Opening Remarks to the Expert Seminar: The right to privacy in the digital age, 24 February 2014. Available at: www.ohchr.org/AR/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=A.

will inevitably be limits on what information can be made public. States' laws and policies governing surveillance should always be public, and this also applies to general interpretations of those laws and policies. However, there is a need for independent oversight of how the regulatory framework for surveillance is implemented by law enforcement and intelligence authorities.

Paragraphs 8 and 9 of the Joint Declaration of the special international mandates notes, in part:

> The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged… The collection of this information shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.

Similarly, Principle 31 of the Tshwanee Principles states:

> States should establish, if they have not already done so, independent oversight bodies to oversee security sector entities, including their operations, regulations, policies, finances, and administration. Such oversight bodies should be institutionally, operationally, and financially independent from the institutions they are mandated to oversee.

Different States handle this task through a variety of mechanisms which can include courts, parliamentary oversight bodies, specialised administrative oversight bodies and civil society groups. Given the important implications of surveillance for freedom of expression and privacy, and the need for such measures to be established by law if they are to meet international standards governing restrictions on these rights, some degree of judicial oversight will always be necessary, for example to challenge alleged breaches of the rules after they have happened.

Given that some of the core goals of oversight include promoting respect for the rules, accountability, transparency and public engagement, ultimate accountability to elected representatives will be a key element of an effective oversight system.

At the same time, these bodies cannot conduct oversight activities on a regular basis and, for this to happen, it is imperative that the system also include one or more specialised administrative oversight bodies. Protecting the independence of these bodies from both intelligence authorities and the executive is clearly crucial if they are to be effective in conducting oversight, and this idea is reflected in both the Joint Declaration and the Tshwanee Principles.

If oversight is the purview of multiple bodies, there is a risk of compartmentalisation undermining effectiveness. Often, the sum total of a surveillance system can be far more invasive when considered as a whole as opposed to being broken down into component parts. This can be mitigated by

having responsibility divided along thematic lines rather than having each authority monitored by a different oversight body. Ideally, however, one central body would have overall responsibility for oversight of the whole system.

3. Actual surveillance activities should be limited and targeted and represent an appropriate balance between security needs and the rights to freedom of expression and privacy.

One of the most difficult issues in relation to digital surveillance is how to ensure an appropriate balance between security needs and freedom of expression and privacy in relation to the basic approach towards surveillance. The Snowden revelations shocked people around the world by revealing official data collection being undertaken on a massive scale, far more than most people had previously imagined. There is little doubt that many people found the secrecy in which these activities were being conducted to be particularly problematical, but their very scale, and their essentially indiscriminate nature, were also the subject of widespread criticism.

An indiscriminate approach, whereby intelligence or law enforcement authorities collect information about as many targets as possible, without any regard to the relevance of the information or its importance to law enforcement or national security investigations, as opposed to targets being individually selected and approved through judicial oversight, is highly problematical from the perspective of international human rights law.

One of the claims made to justify this approach was that the information was simply being stored, and would only be accessed where this was justified in the public interest. Systems which separate the collection and inspection functions, where collection takes place automatically and indiscriminately but judicial authorisation is sought before the collected information is examined, remain highly problematical. The very act of collecting and storing information undermines the integrity of communication processes, including because it creates a perception among all users that they are being watched, thereby inhibiting free, full and candid expression.

CLD has, in the past, condemned data retention schemes, which require private Internet intermediaries to retain information about their users for a particular period of time.[27] A prominent data retention scheme, based on the European Union's Data Retention Directive, was invalidated by the European Court of Justice (ECJ) in April 2014 on the ground that it was incompatible with the privacy and data protection provisions of the Charter of Fundamental Rights of the European Union.[28] A problem with these schemes, beyond the general fact that they create a sense

[27] See Analysis of the European Union's 2006 Data Retention Directive, available at: : http://www.law-democracy.org/live/european-union-data-retention-directive-not-justifiable/.
[28] Case C-293/12. Available at: curia.europa.eu/juris/documents.jsf?num=C-293/12.

among users that they are being monitored, is the risk that the databases in which the information is held can be hacked. For example, in July 2012, when the Australian government announced that it was considering proposals to require Australian ISPs to retain user data, the Anonymous hacker network responded by promptly breaking into the database of a major ISP.[29]

At the same time, the benefits of such broad data collection for law enforcement and intelligence authorities is obvious. There is certainly merit to their arguments about the dynamism of online communications and the distributed nature of their targets, which presents a challenge to traditional methods of surveillance authorisation.

Any widespread system of data collection for potential surveillance purposes would be extremely difficult to justify given the profound implications it would inevitably have for freedom of expression and privacy. And, as with any measure which restricts these rights, the onus would be on the government to justify the system. At the same time, more thought needs to be given to whether a system along these lines could be designed which did incorporate adequate safeguards against abuse, and which provided a balance between security needs and these rights.

4. Structural measures which weaken anonymisation and encryption tools represent serious restrictions on freedom of expression and privacy and are legitimate only where justified in accordance with international standards for limitations on those rights, taking into account the wider importance of these tools to the overall integrity of online communications and our shared interest in a secure web.

Among the more troubling activities which the NSA is alleged to have carried out is its deliberate attempts to weaken encryption standards, a move which would place the security of transactions and communications across the Internet at risk.

Modern encryption mechanisms tend to rely heavily on random number generators. If the random number generator can be compromised, the encryption tool can also be compromised. Around the world, many software and hardware developers rely the National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce, to determine which random number generating systems are secure.[30] By statute, the NIST is required to consult with the

[29] Joel Falconer, "Anonymous hacks Australian ISP AAPT to demonstrate data retention problems", *The Next Web*, 26 July 2012. Available at: thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems/.

[30] Tony Wu, Justin Chung, James Yamat, Jessica Richman, "The ethics (or not) of Massive Government Surveillance". Available at: mcs.stanford.edu/people/eroberts/cs201/projects/ethics-of-surveillance/tech_encryptionbackdoors.html.

NSA as part of this process,[31] and there have been allegations that the NSA has abused this to deliberately weaken cryptographic standards.[32]

From a freedom of expression perspective, it is very difficult to justify any policy which structurally undermine anonymisation and encryption tools. The motivation for security authorities to seek to do this is obvious, since strong encryption systems are an effective tool for cyber-criminals or terrorists to avoid detection and capture. However, building backdoors or other weaknesses into the security systems of commonly used devices or deliberately inserting weak algorithms into encryption software poses serious risks to the integrity of these devices and systems.

A serious problem with backdoors is that they significantly undermine the overall security of the products they are built into. It is a common refrain among the tech community that once a backdoor is built it is impossible to control who goes through it. This was highlighted in a presentation by Jacob Appelbaum, a security researcher with access to the files leaked by Edward Snowden, on 30 December 2013, in which he indicated that two security researchers present in the audience had independently discovered a backdoor that the NSA had ordered to be built into certain computer systems.[33] Appelbaum noted that, for every security researcher whose work is focused on finding and correcting vulnerabilities, there are hundreds of full time hackers with rather less noble intentions who are seeking to find security holes.

This is not the say that a requirement to backdoor software is necessarily illegitimate. Ultimately, that depends on the specific security impact of the backdoor, which must be weighed against the implications in terms of freedom of expression and privacy to determine where, on balance, the public interest lies. As with many such issues, this balancing is complicated by the complex and rapidly shifting technological environment. However, any measure which significantly undermined the security of a product which was widely used would be very difficult to justify.

In considering a requirement to build backdoors into software or services, it is also worth noting that different States have radically different understandings of what makes a legitimate surveillance target. Thomas Paine, the anonymous pamphleteer, was a hero of the American Revolution but a traitor as far as the British Crown was concerned. If major tech companies introduce backdoors into their products, with a mechanism for States to request access, China's list of targets will presumably include prominent dissidents like Ai Weiwei.[34] Edward Snowden has claimed that the NSA's list of targets included human rights organisations, such as Amnesty

[31] See 44 U.S.C. 35.3543(a)(3).
[32] Nicole Perlroth, "Government Announces Steps to Restore Confidence on Encryption Standards", *New York Times*, 10 September 2013. Available at: bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/.
[33] Full presentation available at: www.youtube.com/watch?v=vILAlhwUgIU.
[34] See "Ai Weiwei: Absent friend", *The Economist*, 9 April 2014. Available at: www.economist.com/blogs/prospero/2014/04/ai-weiwei.

International and Human Rights Watch.[35] The huge temptation for States, democratic and despotic alike, to abuse their surveillance capabilities to target legitimate opposition voices is a strong argument against backdoors.

While the legitimacy of backdoors cannot be ruled out altogether, alternatives which can be applied in a more targeted way are vastly preferable. It is worth noting that, as early as 2001, law enforcement authorities were developing avenues for getting around the use of encryption. A report from that year described a programme known as "magic lantern", malware that installs keylogging software, which records each key as it is struck, tracking information as it is created.[36] These devices can be installed physically, for example with a USB stick, but they can also be blended with ordinary web traffic and streamed onto a target machine or installed by posing as an open wifi connection.[37] If law enforcement and intelligence authorities consider that these methods are insufficient to enable them to do their jobs effectively, the burden lies on them to make this case convincingly and to demonstrate clearly why more general measures, which may weaken security for everyone, are needed.

5. The sale of intrusive digital surveillance technologies should be subject to a requirement to obtain an export licence, which should be denied where there is a likelihood that the technologies will be used to carry out human rights abuses.

As noted above, most countries carry out digital surveillance in one form or another. Among repressive States, the Internet's utility as a mechanism for surveillance has made it a key tool for monitoring and stifling democratic dissent. The very nature of the Internet lends itself to this use but highly sophisticated technology is required to conduct surveillance. The best-funded intelligence and law enforcement authorities tend to develop this technology internally but most countries, particularly in the developing world, lack the resources and technical capacity to do so. As a result, private companies play a key role in facilitating the digital surveillance that repressive governments carry out. Overwhelmingly, these companies are based in Europe and North America.

For example, Trovicor, which manufactures the most widely used online surveillance system in the world, is based in Germany and was formerly a subsidiary of Nokia Siemens. A company brochure dated 2007 stated that its monitoring

[35] Luke Harding, "Edward Snowden: US government spied on human rights workers", *The Guardian*, 8 April 2014. Available at: www.theguardian.com/world/2014/apr/08/edwards-snowden-us-government-spied-human-rights-workers.
[36] Bob Sullivan, "FBI software cracks encryption wall", NBC News, 20 November 2001. Available at: www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/.
[37] Cora Currier and Morgan Marquis-Boire, "Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide, The Intercept, 30 October 2014. Available at: https://firstlook.org/theintercept/2014/10/30/hacking-team/.

systems had been installed in 60 countries, including Syria, Yemen, Egypt, Bahrain and Iran.[38] In 2009, due to pressure following Iran's violent crackdown on protestors, Nokia Siemens sold Trovicor. However, the company continues to work with the Iranian government under its new owners, the German-based Perusa Partners Fund.[39]

Blue Coat, which is based in the United States, is a major supplier of DPI systems. Although their products can be used for legitimate network management functions, they can also be used to intercept and analyse traffic. A study by Citizen Lab found indications that these systems were being used in Egypt, Kuwait, Qatar, Saudi Arabia, the United Arab Emirates, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey and Venezuela.[40]

Another widely used surveillance technology is the FinFisher Suite sold by Gamma International, a company based in the United Kingdom. This product is more targeted, and operates through malicious software installed on a particular machine. A study by Citizen Lab found evidence that FinFisher is being used in Australia, Austria, Bahrain, Bangladesh, Brunei, Bulgaria, Canada, Czech Republic, Estonia, Ethiopia, Germany, Hungary, India, Indonesia, Japan, Latvia, Lithuania, Macedonia, Malaysia, Mexico, Mongolia, Netherlands, Nigeria, Pakistan, Panama, Qatar, Romania, Serbia, Singapore, South Africa, Turkey, Turkmenistan, United Arab Emirates, the United Kingdom, the United States and Vietnam.[41]

It is worth noting that the abusive use of these technologies can extend across borders. For example, in 2014, it was reported that the Ethiopian government used equipment manufactured by Hacking Team, an Italian company, to attack critical journalists based in the United States.[42]

Network surveillance tools like these have legitimate law enforcement uses when they are employed by democratic States and subjected to appropriate procedural safeguards. However, they have also become a central tool for repressing democratic dissent and facilitating human rights abuses by repressive States. The international community has an obligation to ensure that, as far as possible,

[38] Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens", *Bloomberg*, 22 August 2011. Available at: www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.
[39] Andy Greenberg, "Nokia Siemens Denies Lingering Ties To Iran Surveillance", *Forbes*, 15 October 2010. Available at: www.forbes.com/sites/andygreenberg/2010/10/15/nokia-siemens-denies-lingering-ties-to-iran-surveillance/.
[40] See: citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf.
[41] See: citizenlab.org/2013/04/for-their-eyes-only-2/.
[42] Craig Timberg, "Foreign regimes use spyware against journalists, even in U.S.", *The Washington Post*, 12 February 2014. Available at: http://www.washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-journalists-even-in-us/2014/02/12/9501a20e-9043-11e3-84e1-27626c5ef5fb_story.html.

powerful surveillance tools are kept out of the hands of States that are likely to abuse them.

A useful model in this regard could be the *Arms Trade Treaty*,[43] which has been signed by 130 States and ratified by 61. That treaty places an obligation on States which are aware of a substantial risk that arms intended to be exported to another country might contribute to serious human rights abuses to stop the export.[44] An analogous procedure could probably be developed for the export of surveillance equipment to countries known to abuse these technologies. There would, to be sure, be some challenges in setting up and applying such a system. There would be a threshold issue of how serious the risk and nature of the human rights abuse would need to be and there would be implementation challenges because it is far more difficult to track whether a country is spying on its citizens than whether it is shooting them. Nonetheless, there are some mechanisms in place which require State approval for the export of surveillance technologies.[45] Some effort should be given to developing models for such a system.

Beyond export controls, attention needs to be focused on the increasingly important role that private intermediaries play in relation to digital communications. Major tech companies' decisions to collaborate with or resist State efforts to track users are an important part of this debate. This Submission has focused on State actions, but user privacy depends in fundamental ways on the private actors who design both anonymisation and encryption tools, as well as technologies designed to pierce through them. More thought needs to be given to the unprecedented power that private actors have over online speech and what that means for freedom of expression as a whole.

[43] UN General Assembly Resolution 234B(LXVII) of 2 April 2013, in force 24 December 2014. Available at: www.un.org/disarmament/ATT/.
[44] See www.amnesty.org/en/campaigns/control-arms.
[45] Kenneth Page, "Huge transparency win forces Switzerland to disclose surveillance exports data", IFEX, 14 January 2015. Available at: www.ifex.org/international/2015/01/14/swiss_government_reveal/.